Checklist 4: How do we meet our privacy obligations?

Information for organisations delivering human services in New South Wales

This fact sheet covers:

- What is a privacy policy?
- Does your organisation need a privacy policy?
- What types of information do privacy laws cover?
- What should your privacy policy say?
- How can your organisation make sure its privacy policy complies with privacy laws and the Human Services Agreement?

This checklist is part of the Guide to the Human Services Agreement (Guide). The Guide provides information on organisations' key legal obligations under the Human Services Agreement. The Guide includes a suite of resources to help organisations meet their obligations.

Caution

The information contained in this document is intended as a guide only and is not legal advice. Interpreting contract terms is complex. If your organisation has a legal problem you should talk to a lawyer before making a decision about what to do. Refer to our webpage on legal advice to see if your organisation may be eligible for free legal advice.

This checklist has been prepared on the basis of the Agreement for Funding of Services – Standard Terms dated 16 October 2019 (**Standard Terms**) and Agreement for Funding of Services – Schedule dated 31 March 2017 (**Schedule**), published on the BuyNSW website (together referred to as the **Human Services Agreement** or **Agreement**).

If the terms on which your Human Services Agreement is based have been amended, please review the information in this document carefully to make sure they are consistent where necessary.

Note: organisations funded by the Department of Communities and Justice

The Department of Communities and Justice (**DCJ**) has added supplementary conditions to the standard form Schedule. The most recent DCJ Schedule, dated 16 October 2019 is available on the DCJ website.

This factsheet has not been amended to take into account the DCJ Schedule. If your organisation uses the DCJ Schedule, refer to Not-for-profit Law's fact sheet on the DCJ's supplementary conditions to understand how the DCJ conditions apply to your organisation's obligations under the Agreement. For example, the DCJ Schedule has a direct impact on organisations privacy obligations under the Agreement.

Tip

Read this checklist with the Human Services Agreement and the Guide at hand for reference. Clauses that we refer to in this document will be the clauses in the Standard Terms (unless we state otherwise).

What is a privacy policy?

A privacy policy sets out how your organisation will manage personal information, including:

- the types of personal, health and sensitive information your organisation collects
- how information is collected and stored
- the circumstances when you will disclose personal, health or sensitive information to someone else, and
- how a person can correct information your organisation holds or lodge a complaint about its handling

Does your organisation need a privacy policy?

Yes.

Under the Standard Terms your organisation has agreed to comply with privacy laws as if it were the relevant NSW government agency (clause 18.1(a)).

This means that your organisation must comply with the following Acts, as if it were a 'public sector agency':

- *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**), which creates the Information Privacy Principles (**IPPs**)
- *Health Records and Information Privacy Act 2002* (NSW) (**HRIP Act**), which creates the Health Privacy Principles (**HPPs**), and
- *Privacy Act 1988* (Cth) (**Privacy Act**), which creates the Australian Privacy Principles (**APPs**)

(together referred to as the **Privacy Laws**).

Under section 33 of the PPIP Act, the NSW government agency (and therefore your organisation) is required to prepare and implement a privacy policy.

APP 1 of the Privacy Act provides that your organisation must:

- have a clearly-expressed, up-to-date privacy policy, and
- make this policy available as soon as is practically possible (for example, on your website).

If anyone asks you for the policy, you must give them a copy (for example, by posting it to them).

Handling personal information in a lawful, transparent and respectful way is an important part of building trust with the people your organisation provides services to as well as partner organisations.

Caution

Failure to comply with the Privacy Laws could amount to a breach of the Standard Terms or the Privacy Laws, and could result in financial or legal penalties.

What types of information do Privacy Laws cover?

- **Personal information:** Any information that identifies a person, including for example, their name, address, photographs, fingerprints.
- **Health information:** Information or opinions about a person's physical and mental health, disability, health preferences, use of health services, bodily donations and genetics.
- **Sensitive information:** Any information about a person's race, ethnicity, political, religious or philosophical beliefs, professional or trade association membership, sexual preferences or practices, criminal record, credit information and health or biometric information.

What should your privacy policy say?

- **Under the IPPs:** Your privacy policy must outline how your organisation will collect, use, disclose, secure and provide access to the personal, sensitive and health information it holds. All NSW government contractors and their sub-contractors must make sure their privacy policy complies with the matters set out in checklists 1 and 2 (see below).
- **Under the APPs:** Your privacy policy should outline how your organisation will manage a data breach, including how your organisation will comply with mandatory data breach notification obligations. Organisations must make sure their privacy policy complies with checklists 1 and 2 (and also checklist 3 if your organisation is a health service provider under the HRIP Act) (see below).
- **Under the HPP:** If your organisation is also a health service provider, or is an organisation that collects, uses or holds health information, then it must ensure its privacy policy complies with the matters set out in checklists 1, 2 and 3 (see below).

Tips for privacy policies

- Don't copy text from another organisation's policy, because the text might:
  - not be relevant to your organisation's practices
  - be prepared according to laws from different states or countries from those that apply to you
  - not cover requirements you're obliged to meet, or
  - be protected by copyright.
- Keep it easy to read. Draft your privacy policy in plain, easy-to-understand language to help your clients and staff understand the policy and avoid potential legal ambiguity.
- Keep it updated. The ways your organisation collects and uses personal information can change, and so do technology and laws. Review your privacy policy regularly to make sure it reflects your current practices and obligations.
- Keep it easy to access. The best place for your privacy policy is on your website, with a clearly visible link and an easily downloadable resource. It's also a good idea to keep a hard copy in your office.

How can your organisation make sure its privacy policy complies with Privacy Laws and the Human Services Agreement?

Tip: How to use the checklists

Checklists 1 and 2 are compulsory and apply to ALL organisations providing services under the Human Services Agreement.

Checklists 1, 2 and 3 are compulsory and apply to certain organisations (ie. health service providers).

Review your privacy policy against the checklists that apply to make sure your policy meets your organisation's legal obligations.

The checklists summarise the key points that your privacy policy should cover. Instead of copying the list word-for-word, adapt each point so that it specifically addresses how your organisation will handle personal, health and sensitive information.

Tip

Complying with the security requirements in clause 25 is one way your organisation can add an additional layer of safety towards meeting your privacy law obligations.

Checklist 1: Applies to ALL organisations (based on obligations under the IPPs)

Things your privacy policy should cover	Relevant IPP	Explanation	Reviewed ☑
How your organisation will collect personal information	IPP 1 – Lawful	Your organisation can only collect a person's personal information for a lawful purpose. It must be required for the organisation's activities	☐
	IPP 1 – Lawful	Your organisation can't collect personal information by unlawful means	☐
	IPP 2 – Direct	Only collect information directly from the person that the information relates to, or their parent or guardian if authorised	☐
	IPP 3 – Open	Take steps to make sure the person is aware the information is being collected, why it's being collected, and who will be using it and storing it. Tell the person how to access their personal information and how to make sure it is correct	☐
	IPP 4 – Relevant	Make sure information collected is relevant, accurate, up-to-date, complete, and not excessive	☐

Things your privacy policy should cover	Relevant IPP	Explanation	Reviewed ☑
Explain how your organisation will store personal information	IPP 5 – Secure	Store information securely. Don't keep it longer than needed and dispose of it securely	☐
Explain how the individual can access their information	IPP 6 – Transparent	Provide the person with details about the personal information your organisation is storing, the reasons why you are storing it and how they can access it to make sure it is correct	☐
	IPP 7 – Accessible	Allow access to the person's personal information in a reasonable time and make sure access isn't costly	☐
	IPP 8 – Correct	Allow the person to update, correct or amend their personal information	☐
Explain how your organisation will use information	IPP 9 – Accurate	Make sure information is correct and relevant before using it	☐
	IPP 10 – Limited	Only use a person's personal information for the reason the organisation collected it	☐
Explain when and how your organisation will disclose personal information to a third party	IPP 11 – Restricted	Only release a person's information to a third party if they consent to its release, if they reasonably would not object to its disclosure, or if the information is needed to deal with a serious risk of harm	☐
	IPP 12 – Safeguarded	Don't disclose sensitive information such as racial, ethnic, political, religious, sexual activity or trade union membership without the person's consent	☐
Explain that your organisation is obliged to disclose a person's personal information in certain circumstances	N/A	Tell people that the personal information the organisation collects may be disclosed to the applicable NSW government agency for the following purposes: • NSW government agency audits or assessments of the organisation's compliance with the Human Services Agreement (clause 18.2(b)), or • if the NSW government agency requests information so that it can comply with its obligations under the *Government Information (Public Access) Act 2009* (NSW) (clause 19.3 of the Human Services Agreement)	☐
	N/A	Explain that your organisation is obliged to notify the applicable NSW government agency immediately if it has reasonable grounds to believe there has been a breach of the Privacy Laws in connection with the organisation's delivery of the Services under the Human Services Agreement (clause 18.2(a) of the Human Services Agreement)	☐
	N/A	Outline that because your organisation receives funding from the NSW government agency, it must comply with any direction from the NSW government	☐

Things your privacy policy should cover	Relevant IPP	Explanation	Reviewed ☑
		agency in respect to compliance with the Privacy Laws (clause 18.1 of the Human Services Agreement)	

Checklist 2: Applies to ALL organisations (based on obligations under the APPs)

Things your privacy policy should cover	Relevant APP	Explanation	Reviewed ☑
Explain that your organisation will only collect sensitive information in certain circumstances	APP 3 – Collection APP 5 – Notification	Sensitive information can only be collected with consent, or where permitted by law. If collecting sensitive information, make sure you have consent for such collection, use or disclosure	☐
Provide individuals with a right to anonymity	APP 2 – Anonymity	Individuals must have the option of not identifying themselves, or of using a pseudonym (where lawful and practical)	☐
Explain if and how information will be transferred across borders	APP 8 – Cross-border disclosure	Before your organisation discloses personal information to an overseas recipient, it must take steps to make sure the overseas recipient is subject to similar privacy laws	☐
Prepare a Data Breach Response Plan	APP 11 – Security	Your organisation must prepare a Data Breach Response Plan that clearly sets out the steps to take and the people responsible for responding to a data breach	☐
Explain your organisation's mandatory data breach notification obligations	N/A	If your organisation suspects that an 'eligible data breach' has occurred, and there is a real risk of serious harm to the person as a result of the breach, your organisation is required to notify both the person affected and the Office of the Australian Information Commissioner as soon as possible by completing a Data Breach Notification Statement	☐

Tip

If you believe a data breach has occurred, you should get legal advice about whether the mandatory data breach notification obligations apply. Penalties apply for organisations that don't comply with the mandatory data breach notification regime.

Checklist 3: Applies to Health Service Providers and organisations that collect, hold and use health information (based on obligations under the HPPs)

Things your privacy policy should cover	Relevant HPP	Explanation	Reviewed ☑
Outline how your organisation will collect personal information	HPP 3 – Direct	Only collect information directly from the person that the information relates to, unless it is unreasonable or impractical to do so – making sure to check any guidelines issued by the Privacy Commissioner on collection	☐
Explain that your organisation can make appropriate amendments to health information held on an individual	HPP 8 – Correct	At the request of a person, make appropriate amendments (whether by way of corrections, deletions or additions) to make sure the health information is accurate, relevant, up-to-date, complete and not misleading Private Sector health providers (ie. non-public sector agencies earning over $3million a year) should refer to sections 33-37b of the HRIP Act which sets out specific obligations in relation to amendment or addition to records	☐
Explain your organisation will only disclose an individual's health information in limited circumstances	HPP 10 and HPP 11 – Limited	Only disclose a person's health information for the reason it was collected, otherwise get a separate consent from the person	☐
State that you will only use ID numbers in certain circumstances	HPP 12 – Unidentified	Only give a person an ID number if it's reasonably necessary	☐
Explain that individuals have a right to anonymity where possible	HPP 13 – Anonymous	Give a person the option to provide their information anonymously where practical	☐
Explain that your organisation will only transfer health information outside NSW in certain circumstances	HPP 14 – Controlled	Only transfer health information outside NSW in accordance with the procedure set out in HPP 14 which includes: • making sure the person consents to the transfer • the other party who is receiving the information is required to follow privacy obligations similar to those under the HPPs, and • your organisation reasonably believes the transfer is necessary to lessen or prevent a serious threat to public health or safety	☐
Explain that your organisation is only authorised to use health record linkage systems in certain circumstances	HPP 15 – Authorised	Only use health records linkage systems (such as MyHealth Record) with consent	☐

Other things to think about

Issue	Explanation	Reviewed ☑
Cloud storage	If your organisation uses internet (or cloud) based storage systems, it must take reasonable steps to make sure third party storage providers comply with the Privacy Laws. If your provider breaches those laws, your organisation may be accountable for those breaches	☐
Privacy audit	Consider conducting a quarterly audit to determine what types of information your organisation collects, uses and discloses and update your privacy policy accordingly	☐
Privacy officer	Appoint a person in your organisation to be responsible for its privacy compliance	☐

Caution

The above checklists are not exhaustive, and if in doubt, you should seek legal advice about your privacy policy.

Resources

Not-for-profit Law resources

Not-for-profit Law has developed a Guide to the Human Services Agreement which includes a fact sheet, a template sub-contract agreement, and a range of checklists which should be read together. See Not-for-profit Law's page on Government Funding Agreements:

- Fact sheet - Human Services Agreement: Department of Communities and Justice Supplementary Conditions
- Fact sheet – Human Services Agreement: Important clauses
- Checklist 1 – How do we meet our notification obligations?
- Checklist 2 – How do we meet our reporting obligations?
- Checklist 3 – How do we practically comply with the Human Services Agreement?
- Checklist 4 – How do we meet our privacy obligations?
- Checklist 5 – How do we meet our intellectual property obligations?
- Checklist 6 – What are our obligations when engaging Personnel?
- Checklist 7 – What records and registers do we need to keep?
- Checklist 8 – Things to consider before entering into a sub-contract agreement
- Template Sub-contract Agreement

In addition, we have resources on the following related topic:

- Privacy and the notifiable data breaches scheme

Other related resources

- BuyNSW website Office of the Australian Information Commissioner
- The Information and Privacy Commission, New South Wales

Legislation

- *Health Records and Information Privacy Act 2002* (NSW)
- *Government Information (Public Access) Act 2009* (NSW)
- *Privacy and Personal Information Protection Act 1998* (NSW)
- *Privacy Act 1988* (Cth)

This resource was developed with financial support from the NSW Department of Finance, Services & Innovation.