



## Management Support Unit (MSU)



### Information Sheet No 17 Privacy – Knowledge and Practice

The purpose of this information sheet is to outline the provisions of the Federal and State privacy legislation, the principles that underpin these provisions and to provide practical guidelines to assist NGOs to meet these provisions.

#### **What is Privacy?**

Privacy can be defined as the right to exercise control over one's personal information or a set of conditions necessary to protect our individual dignity and autonomy (*Office of the NSW Privacy Commissioner, Lawlink NSW*).

Privacy can have various meanings. It may refer to physical privacy such as searching bags or using DNA samples, information privacy (the way in which governments or organisations deal with our personal information such as age, sexual preference, religion and so on) or freedom from excessive surveillance - our right to go about our daily lives without our actions being monitored in person or on camera.

Personal information is any information or opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. It includes but is not confined to an individual's name, address, physical information such as birthmarks or fingerprints, a photograph or image of a person and any body samples.

Privacy regulations can be breached even if the person is not named – if a person can be identified through other details, this is known as 'constructive identification'. Personal information does not include information about a person who has been dead for 30 years or more. Health information is a special type of personal information and refers to the physical or mental health or disability of an individual.

## Why do NGOs keep records?

Community organisations may keep records for a number of reasons including:

- Commonwealth and State laws

These may include forms such as asset and membership registers, financial information and taxation records.

- Funding agreements

These may record expenditure on specific projects.

- Quality standards

These may include the results of interventions or client feedback surveys to demonstrate efficacy of a project.

- The organisation's specific purposes.

These may include client, funding or meeting records.

## Privacy Legislation

There are three main laws protecting the privacy of individuals:

### 1. Privacy Act 1998 (Commonwealth)

This law sets privacy standards for dealing with personal information and is administered by the Office of the Federal Privacy Officer. It applies to both Commonwealth Government agencies and the private sector throughout Australia.

### 2. Privacy and Personal Information Protection Act 1998 (NSW)

This act also sets privacy standards for dealing with personal information for NSW State and Local Government agencies. It is administered by Privacy NSW.

### 3. Health Records and Information Privacy Act 2002 (NSW)

This act sets privacy standards that are specific to dealing with health information. It applies to NSW State and Local Government agencies

and private sector individuals and organisations throughout NSW. It is administered by Privacy NSW.

There are other laws that impact on specialist areas relating to privacy such as privacy of communications or bodily privacy and disclosure of a person's criminal record (*Refer to Privacy NSW, Lawlink*).

## **Principles underpinning Privacy Laws**

Both State and Federal legislation contains principles to be followed to protect the privacy of individuals. The National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000, the Privacy and Personal Information Act 1998 (or PPIP) and Health Records and Information Privacy Act 2002 provide Information Protection Principles which describe the legal obligations of organisations when they collect, store, use and disclose personal information.

While there is some variation between the different legislation and NGOs may not be subject to all the requirements, the principles outlined below provide guidelines for agency practice and cover the collection, storage, access, use and disclosure of information.

As the legislation is very specific, particularly in relation to health services, it is essential for organisations to obtain independent legal advice and not rely solely on these guidelines if they have any privacy concerns.

## **Collection**

The collection of information must be:

1. **Lawful** - The information must be collected for a lawful purpose. It must be directly related to the agency's activities and necessary for that purpose.
2. **Direct** - The individual must give the information directly, unless consent has been given for a different collection process. Parents and guardians can give consent for minors.
3. **Open** - The agency has to inform the individual that information is being collected, why it is being collected and who will be storing and using it.
4. **Relevant** - The agency must ensure that the information is relevant, accurate, up-to-date and not excessive. The collection should not intrude unreasonably into the individual's affairs. The organisation must not collect personal information unless it is necessary for one or more of its functions and activities.

## Storage

5. **Secure** - Information must be stored securely, not kept longer than necessary and disposed of appropriately. It should be protected from unauthorised access, use or disclosure.

## Access

6. **Transparent** - The agency must provide the individual with enough details about what personal information they are storing, why they are storing it and the individuals rights to access the information.
7. **Accessible** - The agency must allow the individual to access personal information without unreasonable delay or expense.
8. **Correct** - The agency must allow the individual to update, correct or amend their personal information where necessary. The organisation must take reasonable steps to ensure that the personal information it collects uses or discloses is accurate, complete and up to date.

## Accuracy and Use

9. **Accurate** - Agencies must make sure personal information is accurate before using it.
10. **Limited** - Agencies can only use information for the purpose for which it was collected, for a directly related purpose or for a purpose to which the person concerned has consented. It can also be used without consent to deal with a serious and imminent threat to anyone's safety.

## Disclosure

11. **Restricted or limited** - The agency can only disclose an individual's information with consent or if the individual was told at the time the information was collected that it would be disclosed. The agency may also disclose information if it is for a related purpose and they do not think the individual would object. Information can also be used without consent in order to deal with a serious and imminent threat to any person's health and safety. Additional directives apply if the information is being given to a third party for the purposes of direct marketing or in cases where the organisation reasonably believes that disclosure is necessary for the purposes of law enforcement.
12. **Safeguarded** - The agency cannot disclose sensitive personal information without consent – for example information about an

© 2008

**NCOSS Management Support Unit (MSU)**

66 Albion St, Surry Hills NSW 2010

phone: 02 9211 2599 ext 127 fax: 02 9281 1968

email: [msu@ncoss.org.au](mailto:msu@ncoss.org.au) web: [www.ncoss.org.au/msu](http://www.ncoss.org.au/msu)

individual's ethnic or racial origin, political, religions or philosophical beliefs, health or sexual activities or trade union membership. Sensitive information may only be disclosed in order to deal with a serious and imminent threat to any person's health and safety.

In the case of the Health Records and Information Privacy Act 2002 there are additional principles relating to identifiers and anonymity, transfer of health information and linkage. The following websites are helpful in this regard:

[www.privacy.gov.au/faqs/hf/index.html](http://www.privacy.gov.au/faqs/hf/index.html)

[www.privacy.gov.au/health/index.html](http://www.privacy.gov.au/health/index.html)

[www.privacy.gov.au/health/pubs/index.html](http://www.privacy.gov.au/health/pubs/index.html)

[www.privacy.gov.au/business/infosh/index.html](http://www.privacy.gov.au/business/infosh/index.html)

The following information sheets related to health privacy are available on the Office of the Privacy Commissioner website and intended to assist private sector health service providers in fulfilling a range of obligations under the Privacy Act 1988 relating to use, disclosure and individual access to health information:

Denial of access to health information due to a serious threat to life or health  
([www.privacy.gov.au/publications/IS21\\_08.html](http://www.privacy.gov.au/publications/IS21_08.html))

Fees for access to health information under the Privacy Act  
([www.privacy.gov.au/publications/IS22\\_08.html](http://www.privacy.gov.au/publications/IS22_08.html) )

Use and disclosure of health information for management, funding and monitoring of a health service ([www.privacy.gov.au/publications/IS23\\_08.html](http://www.privacy.gov.au/publications/IS23_08.html) )

Disclosure of health information and impaired capacity  
([www.privacy.gov.au/publications/IS24\\_08.html](http://www.privacy.gov.au/publications/IS24_08.html))

Sharing health information to provide a health service  
([www.privacy.gov.au/publications/IS25\\_08.html](http://www.privacy.gov.au/publications/IS25_08.html) )

## **How to Protect Other People's Personal Information**

In order to assist your organisation to uphold the provisions of the privacy legislation, it is helpful to take note of the following ten steps (adapted from *Don't Leave Privacy to Chance*, Office of the Australian Government Privacy Commissioner, refer [www.privacy.gov.au/publications/](http://www.privacy.gov.au/publications/) ).

**1. Only collect information that is necessary.**

Make sure individuals know what personal information your organisation collects and for what purpose. Think carefully about whether each piece of information is necessary in general and in each specific instance. For example it is important to ensure that proper guidelines are followed in collecting information about a potential employee's criminal history – the nature of the job and the nature of the conviction are relevant factors. For minor offences or convictions that are older than ten years may be removed from the record.

**2. Do not collect personal information about an individual just because you think the information may come in handy later.**

You should only collect information that is necessary at the time it is collected. If the need arises later, collect the information then.

**3. Tell people what you are going to do with the personal information you collect about them.**

It is important to tell individuals why you want to collect information, how you plan to use it and whether you intend to disclose it. You should provide details on how they can contact you and how they can gain access to their information.

**4. Consider whether you should be using personal information for a particular purpose.**

Organisations often begin to use information for a purpose other than the one for which it was collected. Unless you have consent from the individual or authorisation under the law you should generally only use the information if it is related to the original purpose for which the data was collected and within the reasonable expectations of the individual.

**5. Consider whether you need to disclose personal information.**

Consider whether it is essential for you to disclose information to another organisation or to a third party. It is best practice to obtain consent for disclosure but the Privacy legislation does allow for disclosure in some circumstances.

**6. If people ask, give them access to personal information you hold about them.**

Organisations have a general duty to provide individuals with access to their personal information. It is wise to be open and responsive to such requests. If you do not wish to provide access, you need to give reasons, consistent with the Privacy Act. Agencies should be aware of their obligations under the Freedom of Information Act 1988 which also provides some grounds for denying access to information.

#### **7. Keep personal information secure.**

It is of critical importance that you keep personal information safe and secure from unauthorised access, modification, disclosure, misuse or loss. The steps you take should be in proportion to the sensitivity of the data you are holding. Steps to be taken include IT security such as locking mechanisms if a workstation is not used for ten minutes (requiring the authorised worker to log in again), installing firewalls, cookie removers and anti-virus scanners on systems; allowing file access to staff on a 'need to know' basis and training staff in privacy procedures. It is important to review safety procedures from time to time.

#### **8. Don't keep information you no longer need or are no longer required to retain.**

If you no longer need information and are not compelled by law to retain it, then destroy it by shredding or pulping paper, placing files in a security garbage bin or securely deleting any electronic records, ensuring that they cannot be retrieved.

#### **9. Keep personal information accurate and up to date.**

It is important to ensure that information is updated as soon as it comes to hand and that these changes are noted by relevant staff members.

#### **10. Consider making someone in your organisation responsible for privacy.**

It is useful to have one person responsible for privacy so that the issue does not go onto the 'backburner'. This person takes responsibility for dealing with any grievances or complaints and could also be responsible for privacy training within the organisation.

The Federal Office of the Privacy Commissioner provides a list of trainers on their website <http://www.privacy.gov.au/>

## **Policy**

It is important to ensure that your organisation has a privacy policy. A good record keeping policy is essential to enable NGOs to comply with quality standards which require employees to understand the processes used in collecting, using, storing and sharing client data. Therefore the policy needs to include both a general statement of intent as well as specific procedures that safeguard privacy.

The policy should identify whether information is classified as open access or personal information, with separate procedures for the two types of information. The policy also needs to refer to the ways in which information security is assured, such as safe combinations, security keys and passwords.

It is also important to ensure that somebody is delegated responsibility for policy implementation.

## **Useful Resources and References**

### **Office of the NSW Privacy Commissioner:**

[www.lawlink.nsw.gov.au/lawlink/privacynsw/ll\\_pnsw.nsf/pages/PNSW\\_nswprivacy\\_laws](http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_nswprivacy_laws)

[www.lawlink.nsw.gov.au/privacynsw](http://www.lawlink.nsw.gov.au/privacynsw)

[www.privacy.gov.au/business/infosh/index.html](http://www.privacy.gov.au/business/infosh/index.html)

### **National privacy principles**

<http://tfiledown.qut.edu.au/download.asp?rNum=2623092&pNum=2623088&fac=bus&OLTWebSiteID=DYO&CFID=14104901&CFTOKEN=60644328>

### **Guidelines to National Privacy Principles (NPPs)**

[http://privacy.gov.au/publications/nppgl\\_01.html](http://privacy.gov.au/publications/nppgl_01.html)

© 2008

**NCOSS Management Support Unit (MSU)**

66 Albion St, Surry Hills NSW 2010

**phone:** 02 9211 2599 ext 127 **fax:** 02 9281 1968

**email:** [msu@ncoss.org.au](mailto:msu@ncoss.org.au) **web:** [www.ncoss.org.au/msu](http://www.ncoss.org.au/msu)

## **Record keeping in NGOs**

<http://ltfiledown.qut.edu.au/download.asp?rNum=2623089&pNum=2623088&fac=bus&OLTWebSiteID=DYO&CFID=14104901&CFTOKEN=60644328>

## **Information security policy**

<http://ltfiledown.qut.edu.au/download.asp?rNum=2638388&pNum=2623088&fac=bus&OLTWebSiteID=DYO&CFID=14104901&CFTOKEN=60644328>

## **Australian Government: Office of the Privacy Commission –Ten Steps to Protecting Other People’s Information:**

[www.privacy.gov.au/publications/ten\\_steps/ten\\_steps\\_org.pdf](http://www.privacy.gov.au/publications/ten_steps/ten_steps_org.pdf)

## **NCOSS Forum Report, 2002, Electronic Health Records and NSW Health Privacy Laws**

[www.ncoss.org.au/bookshelf/index.html](http://www.ncoss.org.au/bookshelf/index.html)

## **Standards Australia – Records Management (AS ISO 15489.1-2002 – Records Management)**

[www.standards.org.au/](http://www.standards.org.au/)

## **Application of the 10 National Privacy Principles (NPP) and information about exemptions from these provisions**

[www.privacy.gov.au/business/infosh/index.html](http://www.privacy.gov.au/business/infosh/index.html)

## **For guidelines on privacy policy refer:**

[www.privacy.gov.au/policy/index.html](http://www.privacy.gov.au/policy/index.html)

## **Ten steps to develop a multi-layered privacy notice – Where can I find more information?**

[www.privacy.gov.au/policy/privacy\\_policy.html](http://www.privacy.gov.au/policy/privacy_policy.html)

© 2008

**NCOSS Management Support Unit (MSU)**  
66 Albion St, Surry Hills NSW 2010  
**phone:** 02 9211 2599 ext 127 **fax:** 02 9281 1968  
**email:** [msu@ncoss.org.au](mailto:msu@ncoss.org.au) **web:** [www.ncoss.org.au/msu](http://www.ncoss.org.au/msu)