CRISSP Privacy Policy

Overview

Unless authorised by the client or by law, client information collected for inclusion in CRISSP must be used only for the purpose for which it was collected or a related (in some cases directly related) purpose that is within the individual's reasonable expectations. Information handling must take place in accordance with the Information Privacy Principles (IPPs) contained in the *Information Privacy Act 2000* (IPA) or the Health Privacy Principles (HPPs) contained in the *Health Records Act 2001* (HRA).

Depending on whether personal or health information is collected, NGOs will need to comply with the requirements of the IPA or the HRA, or both. The CRISSP Privacy Policy is *generic*; it is designed to address the requirements of either the IPA or the HRA. On the whole it does not refer specifically to the IPA or the HRA. In those cases where the IPA or the HRA may require a different approach, the policy explicitly refers to the relevant legislation or privacy principle.

The policy also contains references to NGOs' existing privacy policies. Each NGO using CRISSP is already subject to privacy legislation and as part of its compliance regime would have a purpose-built privacy policy. The CRISSP Privacy Policy will operate alongside the existing policy, sometimes supplementing it, at other times updating or changing it. Each NGO will need to assess the CRISSP Privacy Policy and make changes to its existing privacy policy accordingly.

In particular, NGOs must ensure that any privacy materials prepared for internal or external distribution are *consistent* with the requirements of the CRISSP Privacy Policy.

1 – Collection

The collection principles are designed to limit the collection of personal or health information to that which is necessary for organisations to carry out their legitimate functions and activities. Good collection practices are the key to ensuring that the handling of information takes place in a privacy-compliant way. A key aim of the collection principles is to clearly establish the *purpose(s)* of collection.

1.1 Personal or health information may only be collected for inclusion in CRISSP if it is necessary for NGOs to carry out their functions and activities.

Commentary

The primary NGO functions and activities supported by CRISSP are:

- to carry out community care and welfare functions and activities;
- to provide coordinated services to meet the needs of clients;
- to provide information about an NGO, DHS or related service requested by members of the community; and
- for planning, funding, monitoring and evaluating the services provided by NGOs.

Information collected by NGOs from clients and members of the public and held in CRISSP must be limited to what is necessary to undertake these functions and activities.

1.2 Personal or health information must be collected in a way that is lawful and fair and is not unreasonably intrusive

Commentary

It is the responsibility of each NGO using CRISSP to ensure that individual privacy procedures address the need to collect information fairly, lawfully and in a manner that is not unreasonably intrusive. This must be based on current practice that, in turn, will be in accordance with each NGO's existing privacy policy.

1.3 Where personal or health information is collected directly from an individual for inclusion in CRISSP, NGOs must take reasonable steps to provide individuals with a CRISSP Privacy Notice. This must be done at or before the time of collection (or as soon as practicable after).

Commentary

All new clients must be provided with a CRISSP Privacy Notice. A privacy notice ensures that clients are made aware of relevant information about the collection and handling of their information. At a minimum, the CRISSP Privacy Notice must provide information about the name of the organisation (NGO) and how to contact it, and that clients may request access to the information held about them. It must also explain the purposes for which information is collected, any law that requires it to be collected, how it will be handled and the consequences to the individual if the information is not provided. A model CRISSP Privacy Notice has been drafted for use by CRISSP NGOs. (See Appendix.)

Where possible, the CRISSP Privacy Notice must be provided to the client at the point his or her information is collected. This CRISSP Privacy Notice specifically addresses relevant privacy issues including the information to be shared via the CCL.

The CRISSP Privacy Notice may be incorporated into NGOs' existing privacy statements or vice versa. At a minimum, NGOs must ensure that any existing statements are aligned with the content of the model CRISSP Privacy Notice.

CRISSP itself provides a cue for compliance with this requirement by means of a tick box located at the point at which personal or health information would be collected and recorded in CRISSP. NGOs must tick this box to record that the CRISSP Privacy Notice has been provided to the client.

If it is not possible to provide the notice at the point at which the information is initially collected (for example, collection of information takes place under emergency conditions), CRISSP will continue to provide prompts to workers to provide the notice via their daily task list until the item is closed.

CRISSP NGOs must ensure that workers understand and comply with these notification requirements.

1.4 CRISSP information must be collected directly from an individual where it is reasonable and practicable to do so.

Commentary

While privacy legislation prefers direct collection from the individual, information may be collected from a third party where it is both necessary and it is not reasonable and practicable to collect it directly from the client. What is reasonable

and practicable will depend of the circumstances in which an organisation collects information.

For example, Child Protection Placement & Support is usually initiated through a referral containing relevant personal information from DHS to an NGO. In this case it is not reasonable and practicable for an NGO providing Child Protection Placement & Support services to collect information directly from the individual.

1.5 Where personal or health information is collected from a third party for inclusion in CRISSP, NGOs must take reasonable steps to ensure that the individual has been provided with relevant information about the collection and handling of the information. This must be done at or before the time of collection (or as soon as practicable after).

Commentary

If information is collected from a third party for inclusion in CRISSP, reasonable steps must be taken to inform the client of the items covered by 1.3 (unless doing so would pose a serious risk to the life or health of any individual or would involve the disclosure of health information given in confidence). This is consistent with current privacy requirements.

Clients do not need to be informed about the collection of their information from a third party if doing so would pose a serious risk to the life or health of any individual. It is also not necessary to notify the person if this would frustrate a law enforcement activity or involve the disclosure of health information given in confidence.

Reasonable steps will depend upon the circumstances and it is likely that NGOs' current practices in compliance with this sub-principle will be adequate. For example, when DHS issues a child protection placement and support referral, 'reasonable steps' on the part of the NGO would mean ensuring that DHS has a suitable privacy regime in place.

1.6 Wherever possible, sensitive information and health information must only be collected with the consent of the client or his/her authorised representative. Otherwise, it may only be collected as provided for by law.

Commentary

Unless otherwise provided for by law, client or authorised representative consent is required whether the personal or health information is collected from the client or from a third party. Consent to collect sensitive information and health information may be express or implied. The fact that consent has been obtained and/or a CCL consent form has been signed should be recorded in each instance.

Express or implied consent

If a client or his/her authorised representative is informed about the likely uses and disclosures of the health or sensitive information within CRISSP and agrees to provide it for those purposes, consent to collect the information can be implied. Where health and/or sensitive information is to be collected from a third party, eg. a doctor or another health service provider, it is recommended that where possible consent is express and recorded in writing, as the third party is likely to require evidence that the client has consented prior to releasing the information.

What is sensitive and health information?

The Information Privacy Act requires consent for the collection of "sensitive information", about an individual's racial or ethnic origin, political opinions or affiliations, religious beliefs or affiliations, philosophical beliefs, membership of a

professional or trade association or trade union, sexual preferences or practices, or criminal record.

The Health Records Act requires consent for the collection of a person's "health information", including any information about their physical, mental or psychological health, about any disability they have or about health services they receive or are seeking.

Much of the information collected to provide Disability Services and Early Childhood Intervention Services is health information. Implied or express consent will be required for NGOs working in these areas to collect client health information except where otherwise authorised by law to collect information without consent or where the collection is necessary to lessen or prevent a serious threat to an individual's life, health, safety or welfare.

Child Protection Placement & Support and Juvenile Justice collect both health information and sensitive information. NGOs working in these areas may collect health and sensitive information without consent for CRISSP where authorised by law.

1.7 When health information is given in confidence, this must be noted in CRISSP.

Commentary

The HRA contains additional requirements in relation to confidentiality and health information. When acting as a health service provider and given health information in confidence by a third party (other than a health service provider in relation to the provision of health services to the individual), the provider must confirm that the information is confidential, record only relevant information and take reasonable steps to ensure the information is accurate, not misleading and recorded as confidential.

2 - Use & Disclosure

2.1 Personal and health information may only be used and disclosed for the primary purpose of collection or for a secondary purpose as provided for under IPP 2 or HPP 2.

Commentary

The privacy principles provide that information may be used for the primary purpose for which it was collected. Once the primary purpose has been identified and any consent requirements met, it is not necessary to obtain the client's consent to use/disclose the information for that purpose.

The primary purpose is the purpose that was explained to, and/or understood by, the individual at the time of collection. For example, if a client provides contact details to a receptionist for the purpose of making an appointment with a caseworker, it is understood by the individual that the receptionist will pass those details on to the caseworker.

Other purposes are known as 'secondary' purposes. The use and disclosure principles outline the circumstances under which personal/health information may be used for a secondary purpose. The secondary purposes for which information handled in CRISSP is likely to be used will fall within one of eight identified exceptions although some of these exceptions (eg. serious and imminent threats, law enforcement, ASIO/ASIS) will be rare in practical terms and will require action from a nominated employee. The permitted exceptions are:

- Where the secondary purpose is related to the primary purpose (in the case of sensitive and health information *directly* related) and it is within the individual's reasonable expectations;
- Where the individual has consented to the secondary purpose;
- For research/statistical purposes where the results will not be published in an identifiable form and it is impracticable for the organisation to seek the individual's consent and, in the case of disclosure, the organisation reasonably believes that the recipient will not disclose the information;
- Where the secondary purpose involves a serious and imminent threat to an individual or a serious threat to public health, safety or welfare;
- Where the secondary purpose involves the investigation of unlawful activity;
- Where the secondary purpose is required or authorised by or under law;
- Where the secondary purpose is for law enforcement purposes; or
- Where the secondary purpose involves ASIO/ASIS.

If a proposed secondary use/disclosure is not authorised under another law or otherwise provided for in an exception, information cannot be used/disclosed without breaching the privacy legislation. If a secondary purpose is known in advance, individuals should be provided with notice.

3 – Data Quality

3.1 NGOs must take reasonable steps to make sure that CRISSP information is accurate, complete and up to date.

Commentary

A key objective of CRISSP is to improve data quality, including ensuring that information is accurate, complete and up to date. In this sense, implementation of CRISSP supports compliance with the data quality principles.

The need to ensure that client information held in CRISSP is accurate, complete, up to date and relevant to NGO functions and activities has been addressed through CRISSP functionality and design. The Integrated Client Application Management Centre (ICAMC) will also assist with data quality issues once CRISSP is operational.

The data quality principles extend beyond CRISSP. NGOs retain primary responsibility for ensuring that general data quality requirements are met and that existing privacy practices are appropriate.

4 – Data Security

4.1 NGOs must take reasonable steps to protect the information held on CRISSP from misuse and loss and from unauthorised access, modification or disclosure.

Commentary

CRISSP data will be stored securely within DHS' e-Business portal and will be subject to a range of robust security measures.

NGOs primary security responsibilities include: the nomination and maintenance of authorised users; ensuring security at their sites; and data quality.

Additionally, only authorised NGO staff may have access to CRISSP, and access is on a 'need to know' basis.
Upon logon to CRISSP, users are required to agree to a set of conditions about the use of CRISSP including security.

NGO staff access to client information must be reviewed in the following circumstances:

- on appointment to an NGO
- on change of role within an NGO
- upon exit from an NGO

CRISSP will be monitored to detect any unauthorised access attempts, multiple unsuccessful logons and inactive system users. NGOs must take appropriate action where necessary in response to audit reports provided by ICAMC.

CRISSP will be able to encrypt information as necessary for security purposes.

4.2 NGOs must take reasonable steps to destroy or permanently de-identify information on CRISSP if it is no longer needed for any purpose.

Commentary

CRISSP will comply with existing NGO policies and procedures regarding the retention and disposal of information. Particular care needs to be taken in relation to destruction of electronic information.

5 – Openness

5.1 NGOs must develop clearly expressed policies on CRISSP's management of information and make them available to anyone who asks for them.

Commentary

The CRISSP Privacy Guidelines document describes the ways in which personal and health information is managed within CRISSP and it may be made available to anyone who asks for it. The CRISSP Privacy Guidelines should be integrated with each NGO's current privacy policy.

5.2 Upon request, NGOs must take reasonable steps to let people know, generally, what sort of information is held on CRISSP, for what purposes, and how it collects and handles that information.

Commentary

On the whole, this requirement will be dealt with via the CRISSP Privacy Notice. NGOs should be prepared to provide further information as required.

6 – Access and correction

6.1 NGOs must enable individuals to seek access to, and correct, their own information.

Commentary

The access and correction processes developed for CRISSP should be consistent with NGOs' current practices in relation to IPP 6 and HPP 6, in accordance with the relevant privacy legislation.

Where it is appropriate to do so, client access/correction requests should be dealt with informally.

Personal and health information held by NGOs will not be subject to the *Freedom of Information Act 1986* unless this is a term of the Service Agreement.

7 – Unique Identifiers

7.1 The assigning of unique identifiers to clients and cases within CRISSP may only occur where it is necessary for NGOs to carry out their functions efficiently.

Commentary

The Common Client Layer links together identifiers assigned to cases and clients of NGOs providing DHS-funded community services as well as DHS Juvenile Justice, Child Protection, Disability Services, Early Childhood Intervention Services and Housing. This allows a 'single view' of a common client to authorised users and as permitted by law. The use of identifiers also aims to minimise the duplication of data.

Identifiers are generated by and internal to the Integrated Client and Case Management Systems (ICCMS), including CRISSP. They are necessary for ICCMS – including CRISSP – to do its business, and are not disclosed for other purposes.

8 – Anonymity

8.1 Wherever practicable, individuals must be given the option to remain anonymous in their dealings with NGOs and information must not be entered into CRISSP unless it is necessary.

Commentary

On the whole, NGOs will support the anonymity of individuals they interact with. For example, an individual's contact details will not be collected for inclusion in CRISSP when a general inquiry about the NGO's services is made**.**

However, the bulk of the services provided by NGOs are such that personally identifying information is usually required in order *to receive* the service. In practical terms, this means that the anonymity principle will have limited impact on CRISSP, which is a client and case management system designed to manage personal/health information.

9 – Transborder data flows

9.1 CRISSP client information may only be transferred outside of Victoria under specific circumstances.

Commentary

All CRISSP information is held in Victoria. As a result, there are no general issues to deal with in relation to IPP 9 and HPP 9.

In all other circumstances, CRISSP information may only be transferred outside of Victoria as provided for in the privacy legislation and consistent with NGOs' current privacy policies. These include:

- where the NGO believes that the recipient protects privacy under standards similar to the Information Privacy Principles (for personal information) and Health Privacy Principles (for health information);
- Where the client or his/her authorised representative consents;
- As required or authorised by law; or
- Where necessary for the performance of a contract between an NGO and the client or a third party in specified circumstances.

Under the *Health Records Act*, an organisation may also transfer health information outside Victoria where:

- The transfer is for the benefit of the individual;
- It is impracticable to obtain the consent of the individual; and;
- if it were practicable to obtain that consent, the individual would be more likely to give it.

Complaints

Victorian privacy legislation provides that individuals may complain if they believe that their information privacy has been breached by an organisation covered by a Victorian privacy law. NGOs must ensure that they have processes in place to manage all privacy complaints in an open, accountable and fair way.

Any privacy complaints arising through CRISSP should be managed in accordance with each NGO's existing complaints process. Complaints should be referred to a relevant contact immediately to ensure legislative timeframes are met. Under the CRISSP Heads of Agreement, NGOs are required to notify DHS as soon as practicable of any CRISSP privacy breach.

NGOs must provide individuals with notice regarding their right to make a privacy complaint, including their capacity to make a complaint to the Victorian Privacy Commissioner and the Victorian Health Services Commissioner.