Department of Communities and Justice
Factsheet on the privacy obligations of Targeted Earlier Intervention service providers

Introduction

This information sheet will assist Targeted Earlier Intervention (TEI) service providers to comply with their privacy obligations under:

- Privacy and Personal Information Protection Act 1998 NSW (PPIP Act)
- Health Records and Information Privacy Act 2002 (HRIP Act)
- Privacy Act 1988

Clause 18 of the Human Services Agreement – Standard Terms includes your obligation to comply with this legislation.

This information sheet will broadly cover:

- What is personal and health information?
- Collection personal information and Privacy Notices
- Use and disclosure of personal and health information
- Obtaining consent
- The security of information

TEI service providers should use this information to inform their organisations privacy policy and to ensure their practices for collecting, using and disclosing client's personal and health information is lawful.

The information provided is a guide only.

For more information, please refer to the Information and Privacy Commission's Fact sheets, Guidelines and Resources page at https://www.ipc.nsw.gov.au/privacy/agencies/resources and the relevant legislation.

What is personal and health information?

Personal information:

- information about an individual that can be used to identify them. For example, their first and last name, their street-level address.
- an opinion about an individual that can be used to identify them. For example, case notes about a client that could be used to identify an individual.

Health information:

- personal information that is information or an opinion about the physical or mental health or a disability of an individual (e.g. notes from a counselling session)

- an individual's express wishes about the future provision of health services to him/her (e.g. a client askes to speak with a psychologist to manage to their mental health)
- a health service provided, or to be provided, to an individual (e.g. a client needs to see a psychologist to manage their depression).
- other personal information collected to provide, or in providing, a health service (e.g. this individual has high blood pressure and takes insulin to manage their diabetes)
- other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances
- other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual
- healthcare identifiers (e.g. Medicare number)

Collecting personal or health information

Collection

When you collect personal and/or health information from clients, you must ensure:

- the information is collected lawfully (e.g. unlawful collection would be recording someone during a phone call without their permission)
- the information collected is for purposes related to the functions and activities of their service (i.e. only collect information you need to provide your service)
- the information collected is reasonably necessary for that purpose
- the information collected is not excessive, is accurate, up to date and complete
- the collection does not unreasonably intrude into the personal affairs of the individual
- the information is collected directly from the person it is about, unless:
    - the person has authorised for the information to be collected from someone else (e.g. carer)
    - the individual is under the age of 16 years. The information has been provided by a parent or guardian.

Privacy Notice

A privacy notice is a one-way communication. It simply states: "this is what is going to happen with your personal or health information".

A privacy notice must be given to your clients when you collect personal or health information from them (or as soon as reasonably possible after).

Your privacy notice should be written in clear language the client can understand. It should also be truthful and not misleading.

When you collect personal or health information from clients they should be made aware of the following:

- that information is being collected from them
- why the information is collected
- how the information will be used
- who the information is for (e.g. your organisation)
- who the information may be shared with and why
- if the information they provide is required by law or voluntary
- any consequences for the client if information is not provided (e.g. you may not be able to refer them for additional support)
- their right to access and correct information
- the name and address of your organisation for any queries they may have
- the name and address of any organisation who may also hold the information

This list is not exhaustive. You should tailor your privacy notice to meet the needs of your organisation and to cover any elements that are specific to your operating context.

Using and Disclosing Personal or Health Information

As a general rule, information must not be used or disclosed other than for the purpose for which it was collected.

The terms ‘use’ and ‘disclosure’ are not defined in privacy legislation, however case law has developed to give them different meanings under the Act. In general:

Use

To use information means to handle personal or health information collected from a client. For example, using a client’s personal or health information to organise a referral.

You can only use a client’s personal or health information if:

- The proposed use is consistent with the purpose for which it was collected
- The proposed secondary use is directly related to the purpose of collection
- The individual has consented for their personal or health information to be used for that purpose
- It is necessary to prevent or lessen a serious and imminent threat to life or health of a person

Disclosure

To 'disclose' information means to give personal or health information collected by your organisation to a person or body outside your organisation.

For example, your organisation may pass on client details to another organisation to organise a referral.

Your organisation may also disclose personal information to a school or a parent, or to the police if you need to report abuse.

When considering whether a disclosure is permitted by privacy legislation check whether:

- The disclosure is directly related to the purpose for which the information was collected
- The individual has been made aware that information of that kind is usually disclosed (e.g. your privacy notice clearly indicates that information of this kind may be disclosed in certain circumstances)
- The disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of a person.

Disclosure of any information held by your organisation may also be subject to secrecy provisions in specific legislation (e.g. *Crimes Administration of Sentences Act 1999* or *the Children Detention Centres Act 1987*).

NOTE: The privacy principles only apply to 'personal information'. That is information that can use to identify a client, e.g. a client's name or address. These privacy principles do NOT apply to de-identified information. That is, information that cannot be used to identify an individual.

You must exercise caution when using or disclosing personal or health information. If you are not sure, always seek legal advice. See the Information and Privacy Commission NSW website for more information.

Consent

Your organisation must obtain client consent to collect, use and disclose client's personal information. This will help ensure your data collection practices are lawful.

In order for consent to be valid it must be:

Voluntary	The client must be free to exercise genuine choice to provide or withhold consent. They must be free to say no, and still receive the service. They must also be free to say yes, but change their mind at any time.
Informed	The client must be properly and clearly informed about how their personal information with be handled, so they can decide whether to give consent. If your organisation provides incorrect or misleading information, the client's consent could be invalid.

Specific	Consent must be precise and as specific as possible. Your consent form should include a request for each use and disclosure of their personal information. For example: - I consent for [service provider name] to collect and store personal or health information about me - I consent for [service provider name] to share my personal or health information with relevant agencies to provide me with support - I consent for my personal or health information to be stored in the Data Exchange - I consent to participate in follow up research, surveys or evaluation
Current	You must not assume that consent given in particular circumstances applies indefinitely. Good practice is to check in with your clients to make sure they have not changed their mind about consent. Make it clear that a client is entitled to change their mind and revoke their consent later on.
Given by a person with the capacity to give it	A person has capacity to give consent if: - they understand the general nature and effect of how their personal information will be used and disclosed - they can communicate their consent Issues that could affect a client's capacity to consent include: - age - physical or mental disability - temporary incapacity (e.g. psychotic episode, in severe distress) - limited understanding of English

Refer to the Information and Privacy Commission's Fact Sheet - Consent and Bundled Consent for more information.

Security of information

You must always take reasonable steps to ensure the personal and health information you hold is secure. The precautions you take to ensure the security of information will vary depending on the sensitivity of the information and the possibility of adverse consequences for an individual if the information is lost or disclosed.

When dealing with personal or health information, you need to consider the following:

- **Physical Security**: What form does the information take? Where is the personal and health information held? For example, are they paper or electronic records? Are they stored in locked cabinets?

- **ICT Security**: How is the information protected from unauthorised access? For example, is it password protected or stored electronically with access restrictions?
- **Access Security:** Who is authorised to access the information? Is access restricted by role, work unit and is access audited?
- **Governance, culture and training**: Do staff receive regular training in privacy obligations? Are they aware of security policies, privacy management plan and the privacy policy?
- **Data breaches**: Are staff aware of their obligations when faced with a data breach?
- **Sensitive information**: Is sensitive information, such as psychology reports subject to increased security safeguards?
- **De-identification**: how and when is client information de-identified?
- **Destruction**: How and when are documents containing personal information destroyed? is there a relevant disposal authority?

Early identification of privacy risks

It is important to consider any privacy risks related to your data collection and storage practices.

Considering privacy obligations early can eliminate or minimise the risk of unlawful disclosures or breaches of privacy.

It is also important to consider the relevant legislation with respect to:

- the privacy compliance obligations
- data breach notification
- any audit responsibilities

If in doubt, please seek legal advice.

You could talk to the legal team within your organisation or Justice Connect to request a referral for assistance.

Data breach – who to notify?

A data breach can be caused by various things, e.g. through malware or hacking, human or technical errors, a lack of training, a loss of a record, or emails being sent to the wrong recipients.

See Data Breach Guidance for NSW Agencies for more information.

In the event of a data breach, you must follow your organisations internal protocols and notify the Legal Branch of DCJ by emailing infoandprivacy@justice.nsw.gov.au.

Practical tips to protect personal and health information

- Be Proactive – Develop clear practices, procedures and training around the secure storage and handling of information.
- Put privacy on the agenda – conduct regular training on privacy and discuss privacy risks/concerns at staff meetings.
- Seek Advice – contact the Legal Branch of DCJ promptly if you identify a data breach or a risk of a data breach: infoandprivacy@justice.nsw.gov.au.

For more information, please refer to our website:
https://www.justice.nsw.gov.au/Pages/privacy.aspx.