EMERGENCE

OUR STORIES IN THE NEXT DECADE

Confidentiality, privacy and data protection

20 May 2021

Acknowledgement of Country

We acknowledge the Traditional Owners of the lands across Australia.

We pay deep respect to Elders past, present and emerging and any Aboriginal or Torres Strait Islander persons who are joining this webinar today.

We acknowledge Aboriginal and Torres Strait Islander peoples as the first people of Australia and that sovereignty has not been ceded.

Housekeeping

- Please remain on mute when you are not contributing.
- The Q&A session will be at the end, feel free to use the **chat function** or **raise hand button** to **ask questions** at the end of the webinar.
- The webinar is being recorded but we will stop recording during Q&A.
- Please complete our feedback survey (sent to your email and posted in chat at the end).

Community Legal Centres Australia

WELFARE RIGHTS & ADVOCACY SERVICE

Presenters:

Catherine Eagle	Principal Solicitor – Welfare Rights & Advocacy Service, State PII Representative from WA and convenor of the National PII Network
Lisa Kleinau	Solicitor – King & Wood Mallesons

KING&WOOD MALLESONS

Facilitator:

Meg Houston	Capacity Building Manager – CLCs Australia

COMMUNITY LEGAL WESTERN AUSTRALIA

Plan for session

- What is the duty of confidentiality and where to find it?
- What can go wrong and tips for dealing with confidential information
- What are a lawyer’s obligations under Privacy laws
- Best practice tips for dealing with personal information
- Draft Privacy Policy
- Draft Data Protection and Response Internal Process

Risk Management Guide (RMG)

- Guide for CLCs in delivering legal and related services
- Chapter 2 mandatory standards
  - 2.12 duty of confidentiality
  - 2.12.1 centre workers, volunteers … must comply with ethical contractual and other legal duties of confidentiality
  - 2.12.2 Any statutory or contractual requirements for the privacy protection of personal information must be met
- Chapter 6.6 confidentiality
- Chapter 8.19 privacy laws
- Appendix H Sample Privacy Policy

RMG Chapter 6.6 Confidentiality

A duty of confidentiality can arise from a number of sources including:

- A contractual duty through a service agreement, employment contract or client agreement
- An ethical duty informed by a code of ethics
- A statutory duty governed by professional regulation
- A fiduciary duty arising from the solicitor/client relationship
- Under equity

Each State/Territory has Legal Profession laws that govern lawyers and legal practices in that jurisdiction

Legal Professional Conduct Rules 2010 (WA)

Rule 9: Confidentiality

(1) ‘client information’ means information confidential to a client of which a practitioner becomes aware in the course of providing legal services to the client.
(2) A practitioner must not disclose client information to a person other than the client unless the person is:

(a) an associate of the practitioner’s law practice; or

(b) a person engaged by the practitioner’s law practice for the purposes of providing legal services to the client; or

(c) a person employed or otherwise engaged by an associated entity of the practitioner’s law practice for the purposes of providing administrative services to the client.

(3) Sets out exceptions

NOTE: Each jurisdiction has similar provisions including in the Australian Solicitor's conduct rules.

Practices around confidentiality – what can go wrong?

Some examples of situations where breaches occur

- relaying information to a person who has not been authorised to receive it
- leaving a client file (or document) out in a place that other clients have access to
- talking to a client where others can hear (working from home)
- leaving a message with another person/on a shared phone for a client to call back (is it safe to leave a message?)
- emailing to a shared email account or to the wrong email address
- faxing to a public place
- allowing a client to use an office computer
- having client information on portable devices that are not secure (password protected) and are lost/stolen

Best Practice Tips for dealing with confidential information

Information is or becomes confidential when for example:

- In the circumstances surrounding disclosure of the information to the CLC, or because of the nature of the information it ought in good faith to be treated as confidential
- The information is marked as confidential to the person to whom it belongs
- The information is subject to obligations of legal professional privilege owed by the CLC

Confidential information may lose its confidentiality where:

- The information is in or has become part of the public domain (other than through a breach of an obligation of confidentiality owed by the CLC or a third party)
- The information was developed by the CLC or a third party independent of the disclosure by the person to whom it belongs
- The CLC acquires the information from a third party entitled to disclose it

How to deal with confidential information

Key obligations:

- Only use, disclose or copy the information for the purpose for which it was given to the CLC (the Approved Purpose)

- Only share the information with people in your organisation who need it for that Approved Purpose

- Establish and maintain effective security measures to safeguard the information from unauthorised access use copying or disclosure. Use the same degree of care as a prudent person would use to protect their confidential information
    - E.g. keeping confidential documents in locked cabinets or if the documents are electronic applying password protection to the documents and any device they are stored on

- If the information is used, disclosed or copied for a purpose other than the Approved Purpose in a way that could significantly affect the interests of the person to whom that information belongs take reasonable steps to: (1) notify the person and (2) remedy the effects of the unauthorised use, disclosure or copying to the extent possible

What do privacy laws regulate?

- Purpose: protect the handling of personal information about individuals, including its collection, use, storage and disclosure
- Personal information: means information or an opinion, whether true or not, about an identified individual, or an individual who is reasonably identifiable
  - Sensitive information: includes information or opinion about an individual's health, race, political opinion, religious beliefs, sexual orientation or criminal record
- Includes obligations in respect of data breaches

Sources of obligations

- Primary legislation: Commonwealth *Privacy Act 1988* (Cth)
- Applies to:
  - CLCs Australia
  - Any CLC which has had an annual turnover of over $3m in any financial year since FY2001/2002
  - Any CLC which is a contracted service provider under (or a subcontractor in relation to) a contract with a Commonwealth, State or Territory entity, but only to the extent of the services it provides under the contract
  - Any CLC which has entered into a contract with a government entity (e.g. a funding agreement) requiring the CLC to comply with Commonwealth privacy law (including the Australian Privacy Principles (**APPs**))
  - Any CLC which is in possession or control of material which records a person's tax file number in a manner connecting it with the person's identity

Sources of obligations

- State and territory specific legislation exists in all jurisdictions other than South Australia (which has an Information Privacy Principles ‘Instruction’) and Western Australia
- In WA, in 2019 the ‘Privacy and Responsible Information Sharing for the Western Australian Public Sector’ discussion paper was issued for public comment
- Other than WA, jurisdiction specific obligations apply to a CLC if:
  - It has entered into a contract with a state or territory entity (such as a funding agreement) which requires the CLC to comply with the state / territory specific privacy laws
  - Further, in:
    - the Northern Territory: a CLC who is a contracted service provider under a contract with an NT entity – to the extent of the services it provides under the contract
    - South Australia: a CLC who is a contracted service provider under a contract with an SA entity – where the contract requires the SA entity to disclose personal information to the CLC
    - Tasmania: a CLC who is a contracted service provider under a contract with a Tas entity – which relates to the collection, use or storage of personal information

Commonwealth Privacy Act requirements

- Applies to personal information of clients, contractors, volunteers, employees of related entities, and job applicants
- CLC must have a published privacy policy
- Data breach notification scheme applies
  - Data breach: occurs when information is lost or is disclosed to, or accessed by, an individual or third party without proper authorisation
  - This could happen from both a malicious action and internal errors / accidental loss or disclosure
  - Notification required if the breach is likely to result in serious harm to any of the individuals that the personal information relates to, and the CLC has not been able to prevent the risk through remedial action

Best practice tips for dealing with personal information

If your organisation is not required by law to adopt a privacy policy	• Consider adopting the "Sample Privacy Policy" as an internal document. • For CLCs in New South Wales who are subject to the *Privacy and Personal Information Protection Act 1996*, adopting this policy will assist you to comply with your section 33 obligation to implement a "privacy management plan".
If your organisation is required to adopt a privacy policy under State or Territory law but not Commonwealth law	Before adopting the Sample Privacy Policy as a publicly available document, consider making the following changes: • Limiting the scope of personal information covered by the policy, so that it is limited to the types of information the subject of your obligations under State or Territory law. • Amending the "Complaints" section to refer to the relevant law and/or privacy principles.
If a data breach occurs within your organisation	• If a data breach occurs in respect of personal information which is subject to your obligations under State or Territory privacy law, it is best practice to notify the relevant State or Territory regulator of the data breach, even though this is not strictly required.
Other "best practice" procedures your organisation should consider adopting	• Assign responsibility for managing privacy within your CLC. • Inform staff and volunteers around the relevant obligations and expectations, including through training. • Adopt procedures on when clients will be provided with notices relating to the collection of their personal information / information about privacy procedures at the CLC.
How to deal with personal information collected about potential clients which your organisation does not take on	• If the information does not need to be retained for any particular purpose, privacy legislation requires the organisation to take reasonable steps to destroy or permanently de-identify the information.

Appendix H: Sample Privacy Policy

RMG Appendix H Sample Privacy policy

Each CLC should have a publicly available Privacy policy that sets out:

- The kinds of personal information the CLC collects
- How the CLC will use that information
- The purposes for which the CLC collects personal information
- People to whom the CLC discloses information
- Security and integrity of personal information
- How the person can request access to or correct personal information and the process for complaints.

The CLC should make sure the policy is easy to access – e.g. available on the CLC website

All Board members, staff volunteers contractors and secondees are provided with a copy of the Policy as part of their induction and training and implement it fully.

CLCs can use/adapt the Sample Privacy Policy at Appendix H of the RMG

Sample Data Protection and Response Internal Process

Each CLC should have an internal policy document on it data protection and response internal process considering the following steps:

- Prevention of data breaches
- Internal reporting of suspected or actual data breaches
- Process for identifying and containing data breaches
- Process for assessing a data breach
- Process for external notification of a data breach
- Process for remediating a data breach

CLCs can use/adapt the Sample Data Protection and Response Internal Process document

Questions?