Inner Actions Privacy Policy

Introduction

(Relevant APPs: 1, 5)

Luisa Dal Molin trading as Inner Actions is committed to protecting the privacy of client information and to handling your personal information in a responsible manner in accordance with the Privacy Act 1988 (Cth), the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Australian Privacy Principles and the Health Records (Privacy & Access) Act 1997 (ACT) (referred to as privacy legislation).

This Privacy Policy explains how I collect, use and disclose your personal information, how you may access that information and how you may seek the correction of any information. It also explains how you may make a complaint about a breach of privacy legislation. This Privacy Policy is current from January 2018. From time to time I may make changes to this policy, processes and systems in relation to how I handle your personal information. I will update this Privacy Policy to reflect any changes. Those changes will be available on the Inner Actions website and in the practice.

Collection of Information

Contact and Accounting Information

(Relevant APPs: 3, 4)

I collect information that is necessary and relevant to provide you with mental health and wellbeing care, and to manage the practice. This information may include your name, address, date of birth, gender and contact details.

Contact and accounting information may be stored on my computer accounting system. Information necessary to prepare Tax Invoices for Medicare claims such as the referring doctor may also be stored in the accounting system.

Credit card and EFTPOS details are not generally stored other than in the restricted form provided by bank transaction records (EFTPOS terminal receipts). This information will be held for up to 6 months as required by banking merchant agreements.

Sensitive Healthcare Information

(Relevant APPs: 3, 4, 5)

Sensitive healthcare information may include your health information, family history, notes of sessions, information provided by GP's in referrals, names of other health professionals (e.g. your GP's name) and similar sensitive information necessary for me to assist you.

Personal and sensitive information may be stored on my computer client management system. Wherever practicable I will only collect information from you personally. However, I may also need to collect information from other sources such as your GP, treating specialists, and other health care providers. This information is only collected with your permission either directly to me or to the other provider.

I am required by law to retain healthcare records for certain periods of time depending on your age at the time I provide the services. Normally, in the ACT, I am required to maintain records for a minimum of seven (7) years.

Other Information

(Relevant APPs: 3, 4, 5)

I collect information in various ways, such as over the phone or in writing, in person in my Turner practice or over the internet if you transact with me online. This information will be collected preferentially by me but on occasion by support staff on my behalf (e.g. voicemail messages, email messages and faxed information are facilities which may be accessible to administrative support staff in order to facilitate service provision). Information will only be accessed by administrative staff to the degree necessary to direct the information or request or to facilitate service provision (e.g. Respond to a voice message to change an appointment time, record accounting information, or similar administrative tasks).

In emergency situations I may also need to collect information from your relatives or friends.

Use and Disclosure

(Relevant APPs: 6, 7, 11)

I will treat your personal information as strictly private and confidential. I will only use or disclose it for purposes directly related to your care and treatment, or in ways that you would reasonably expect that I would use it for your ongoing care and treatment. For example, disclosure to your referring GP in progress reports which are required under Mental Health Treatment.

There are circumstances where I may be permitted or required by law to disclose your personal information to third parties. For example, to Medicare, Police, insurers, solicitors, government regulatory bodies, tribunals, courts of law, hospitals, or debt collection agents. I may disclose information about you to outside contractors to carry out activities on my behalf, such as a solicitor or debt collection agent. I impose security and confidentiality requirements on how they handle your personal information and limit it to that essential to perform the service.

Anonymity or Pseudonymity

(Relevant APPs: 1, 2, 3)

The Australian Privacy Principles allow you to see me anonymously or to use a pseudonym. While there is nothing to stop you seeing me under a pseudonym, and I do not check your personal details, I advise caution about doing so as it can cause some problems in relation to the use of my services. You need to be aware that seeing me under a pseudonym can affect your ability to access health records in the future as I will require proof of identity for this. Use of a pseudonym may prevent access to medical benefits and Medicare rebates. EFTPOS and Credit Card access requires that you use a card in the name of the person paying.

I cannot see you while maintaining two identities – one for Healthcare Information and another for accounts as this would prevent me from complying with the Health Records (Privacy and Access) Act 1997.

Use of a pseudonym will also make it difficult to talk about your issues and personal situation as you will be trying to maintain an identity while talking about what is happening for you.

Data Quality and Security

(Relevant APPs: 10, 11)

I will take reasonable steps to ensure that your personal information is accurate, complete, up to date and relevant. For this purpose, I may ask you to confirm that your contact details are correct when you attend a consultation. I request that you let me know if any of the information I hold about you is incorrect or out of date.

Personal information that I hold is protected by:

- securing my premises;

- placing authorisation requirements and passwords on databases to limit access and protect electronic information from unauthorised interference, access, modification and disclosure; and
- providing locked cabinets for the storage of physical records.

As of late 2017, I utilise the services of Healthkit (an Australian Health Services provider, not the Apple App), for recording of session information and notes. Healthkit utilises bank level security for encryption and maintains information in secure data centres located in Australia. Healthkit has passed security and operational tests to make it compliant with Medicare and DVA. Information pertaining to Healthkit's security can be found at https://www.healthkit.com/manual/FAQs#Other_questions

I take electronic security seriously and invest time and effort to maintain it. I utilise commercial grade antivirus and malware protection on my computers. I utilise data encryption for information stored offsite from this location (eg. Backups or cloud services).

Access

(Relevant APPs: 12)

You are entitled to request access to your health records. I request that you put your request in writing and I will respond to it within a reasonable time. There may be a fee for the administrative costs of retrieving and providing you with copies of your health records. I may deny access to your health records in certain circumstances permitted by law, for example, if disclosure may cause a serious threat to your health or safety. I will always tell you why access is denied and the options you have to respond to my decision.

Corrections

(Relevant APPs: 10, 13)

If you believe that the information I have about you is not accurate, complete or up-to-date, I ask that you contact me in writing specifying the inaccuracy and correction you seek. The Health Records Act 1997 (ACT) limits my options for changing health records and in general I am not able to change a record. I can however attach your requested correction to the file.

Complaints

(Relevant APPs: 6, 13)

If you have a complaint about the privacy of your personal information, I request that you contact me in writing. Upon receipt of a complaint I will consider the details and attempt wherever possible to resolve it to your satisfaction. If you are dissatisfied with my handling of a complaint or the outcome you may make an application to the Australian Information Commissioner or the ACT Health Services Commissioner.

Overseas Transfer of Data

(Relevant APPs: 8, 16)

I am conscious that "cloud" computing services such as Dropbox, Google Cloud Storage, Microsoft OneDrive and similar services are normally located overseas and not subject to Australian Privacy legislation. Accordingly, I do not utilise these or any other similar services for client information.

I do utilise an overseas cloud service provider for backup of my documents including documents relating to clients. This information is encrypted with 256-bit AES encryption locally before being transmitted to the backup site. The backup site further encrypts the files resulting in a double layer of encryption. I believe these measures meet the requirements of APP8 and 16 in relation to cloud storage and preserve your privacy and the confidentiality of the material.

I will not transfer your personal information in plain or readable form to an overseas recipient unless I have your consent or am required to do so by law.

Web Site Information and Email Server

(Relevant APPs: 4, 8)

Web servers typically automatically collect data such as your IP address, browser, operating system and related information to enable them to track location and the serving of appropriate pages (e.g. different pages for desktop or mobile, or browser specific pages).

The website server may make a record of your visit and log the following information for security and statistical purposes:

- your public IP address;
- your top-level domain name (usually your ISP/RSP);
- the date and time of access to the website;
- pages accessed, and documents downloaded;
- the previous website visited; and
- the type of operating system and browser software in use.

Inner Actions does not utilise such information for individual tracking or advertising purposes. If I believe my web-site is under attack I will ask IT support/security people to track the source of such attacks utilising web-server collected information.

The Inner Actions website uses "Google Analytics", a website usage service provided by Google Inc. (Google). Google Analytics uses cookies to help analyse how users use the website. Google Analytics anonymously tracks how visitors interact with the website, including where they came from, what they did on the website and whether they completed any transactions on the website.

The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of compiling reports on website activity and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google states that they will not associate your IP address with any other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser, however please note that if you do this you may not be able to use the full functionality of the Inner Actions website. By using the website, you consent to the processing of data about you by Google in the manner and for the purposes set out above.

Email

(Relevant APPs: 4, 8)

Email servers track information on email sources. Additionally, email servers operate on a store and forward basis meaning that each server along the path may have a copy of the email which can be accessed by that servers' administrative staff. This is true for all email systems. Clients are encouraged to be aware that email is not a secure system and should not discuss clinically significant details via email unless they understand the risk of potential eaves-dropping by people not subject to Australian law.

Contact

(Relevant APPs: 12)

Please direct any queries, complaints, or requests for access to health records to me.