GDPR Statement - Judy Buckley Reflexology

Obtaining and storing data

What data is held?

- Name
- Date of Birth
- Phone no
- Email
- Medical history
- Medical red flag
- Treatment notes
- Relationship data
- Browsing data

Why is this data held?

- Name: client identification
- Date of birth: identification, i.e. for occasions when we have duplicate names.
- Phone: to send reminder texts the day before, to keep cancellations and no shows to a minimum; in case we need contact them to cancel due to illness etc.
- Email: to send receipts and appointment confirmations. It is never added to any marketing list.
- Doctor's details: if clients present with serious medical issues, in which case we may liaise with the GP or specialist.
- Next of kin: taken only in the case of children (with signed consent from parent or guardian and their presence in the room) and vulnerable adults.
- Medical history: to help our therapists understand what the client is presenting with on a given day, so a decision whether treatment is appropriate or not can be make, and to carry out any treatments in a safe way. We ask for a baseline level of detail as seen on our consultation chart initially and work off the extended consultation chart to seek further clarification where there is a more complex medical history.
- Medical red flags: this is taken from our paper records and noted in a highlighted area on our online system, to ensure whoever is seeing the client on a particular day is reminded and proceeds to treat appropriately. No details are given here.
- Treatment notes: our record of what happened during any contact with clients, kept only in hardcopy form.
- Browsing data: through cookies and Google analytics to help us understand how people use our website so we can identify issues and improve our service here.

Who is the data controller?

Founder & Reflexologist: Judy Buckley

How was the data obtained?

Primarily, the data we hold is obtained during face to face consultation with clients. We go through a consultation form with them and discuss their presenting problem, expanding our questions as necessary to understand.

On the original booking, we will obtain a name and phone number by phone.

Why was the data originally gathered?

Name, phone are gathered at time of booking to secure booking, letting us know who is coming in and how to contact them with reminder text or should we need to cancel due to unforeseen circumstances. Other data is needed to carry out the treatments requested by the client.

Where is the data stored?

On our phone, numbers and names are stored along with emails and facebook messages should you wish to contact us in this manner. The phone is password protected.

On our paper records, we hold client name, our chart no, phone no, medical history and treatment notes, and reports received from client in relation to their condition.

Browsing data is held by Google Analytics.

How secure is the data; encryption and accessibility?

Names, phone no, email and are stored on a phone. This phone is password protected.

These and all other details, i.e. medical history, treatment notes, etc. are kept manually in a locked filing cabinet in a locked room. Access to this room is for Judy only and access to the filing cabinet is restricted to her. The key to the cabinets is kept in the safe and can only be accessed by Judy.

Client record charts in use each day are kept in a folder that is with the therapist at all times and is not left lying around in view of a client. Folders are kept in a cabinet in the safety of Judy's client cabinet.

Is the data shared with 3rd parties and on what basis?

We use Paypal to for the client to make deposits online. Please view their privacy policy.

How long shall the data be retained?

Our insurance providers require us to retain all records for a period of 7 years after the last appointment, or in the case of minors, for 7 years after their 18th birthday. We work off this for all data.

The one exception is when we take card payments over the phone. The card number is typed directly into the terminal and is never written or stored anywhere.

Amending data

Amending incorrect data.

A change of name, address, phone no, email, doctor, etc. is done by the owner (Judy Buckley) of the clinic. Once the change needed has been brought to their attention directly by a client, or by another therapist on behalf of a client, the data will be updated straight away. Their paper records will be pulled and the update will be made to this file also.

Transferring data.

Upon receiving a request from a client to transfer data to another therapist, solicitor, medical professional, a photocopy of the paper records including all medical history and treatment history will be sent by registered post, with no amendments, to the address provided by the client. The client must sign consent to this transfer, which states the date, the name and address of the recipient and acknowledgement of permission to send. This will be kept with their original records, as a record of the transfer and request to do so.

Destroying data.

Data will only be destroyed after the allotted time frame as quoted above.

The record of client name and chart no. listed on our computer will continue to be listed with a highlighted note indicating the date of its destruction.

The paper record will be removed and shredded on site. These are brought home in 2 separate bags, one at a time, to burn in a fire, checking that all paper is properly burned and that nothing is remaining.

https://www.wikihow.com/Destroy-Sensitive-Documents

Obtaining Data and consent to hold data

How is data obtained?

- Clients make contact with us to book a treatment.
- At no point do we chase a client for details without them initiating the contact.
- We will not secure a booking without a name and phone no.
- During the initial session with a new client, a full consultation form is gone through and filled out. At this point we review our Privacy Policy with clients. They can refrain from giving us address, email, doctors details, next of kin, date of birth if they prefer and are not a child or vulnerable adult; however we will not proceed with treatment without name, phone no and medical history.
- Browsing data is obtained by their use of our website.

Data breaches

What is a data breach?

A data breach is when our online system has been accessed at the core or if our account has been accessed at our level or if a person has got access to our premises and there is evidence or a risk of data being copies, accessed, destroyed or removed from our premises. Our personal smart phones where we have accessed our online booking system pose more of a risk and so should be well locked and protected.

How to identify a data breach.

- Most systems online are so locked down that cybercriminals are looking for human error to access data.
- They are looking for card details and identity theft.
- They are getting in through administrative access
- Half or more small to medium sized businesses are hacked at some point and nearly three-quarters of these are unable to restore all information.
- Card breaches are identified when clients all begin reporting fraudulent charges on their accounts coming from our payment facility. Please see 'Card Security Fraud Prevention' for more.
- Physical break-in; be on the look-out for tampering signs at the door and windows accessing the premises, the internal doors, the safe and the cabinet where documents are stored.
- Online breaches have a number of signs that you can look out for.
- On your computer, look for unusually slow internet/computers – sign it may be exporting a lot of data.
- Look for high CPU cycle, memory usage or hard disk activity – sign it may be exporting a lot of data.
- Is your computer tampered with, not on/off as you left it?
- Are there new/moved/deleted files?
- Are there pop-ups and redirected websites while browsing (lot of advertisements) – your malware is trying to get you to slip-up and grant access.

- Locked out of accounts on first passwords entry – someone else has been trying/succeeded in getting access.

What to do if there has been a data breach.

- Fill out a Data Breach incident form asap and let the data controller know, who will then do the following.
- Within 72 hours (legal obligation or face a fine) of knowing something has happened, get in touch with the Data Protection Commissioners referring to the Data Breach form.
- Consider if clients affected need to be notified (risk of identity theft, card fraud or breach of confidentiality), so that they can take appropriate measures to mitigate the effects to their property, person or reputation. Notifying data subjects is a remedial measure intended to redress the balance and restore some measure of knowledge and control. Let them know who to contact in our organisation for more details.
- 3rd parties may need to be contacted to help; i.e. An Garda Siochana, the financial institutes.
- Keep a diary of any data breaches or suspected data breaches.