Irish Reflexologists Institute 2018

GDPR Guidance for Irish Reflexologists

MESSAGE FROM THE IRIL COMMITTEE:

The new General Data Protection Regulations (GDPR) will come into law from 25th May 2018, with renewed emphasis on each practitioner as a Data Controller. We urge the need to be more mindful than ever of an individual's rights to privacy in all aspects of processing their personal and sensitive data.

Under GDPR, an individual has enhanced rights in respect of their personal data, including the right to question and challenge how it is used, the right to be told clearly the purpose of why the data is collected and who it will be shared with, the right to request a copy of all of the data held in manual and electronic form, and the right to have it corrected or destroyed (when applicable). There is an increased obligation to only process and use the data for the purposes it was collected, and to keep the data safe and secure and out of reach of anyone who is not entitled to see or use it. With this in mind we have asked Mr. Dainow to research for the IRIL and how this impacts us as an Institute and a reflexologist.

Brandt Dainow *bd@thinkmetrics.com* *Digital Consulting*

TO: Members of the IRIL from Brandt Dainow

I have discussed the new data requirements for members of the Irish Reflexologists Institute with the Irish Data Protection Authority. There are no specific regulations for reflexologists, or any other independent therapist working in the health sector. This document shows what we agreed was reasonable, given the nature of the work and the type of business.

However, please be aware this does not constitute formal legal advice or official government guidance. It is possible court cases or additional regulations could change some of this advice. If you follow this guidance, it is still possible you could be found in breach of data regulations at some stage in the future, but you will be able to argue you followed the best advice available at the time, which most courts should accept. However, it is highly unlikely you will ever find yourself in court over these issues unless you are blatantly careless with client records.

The situation

The new rules start **May 25.**

The main change is that **your client records are no longer your property. Client records are now the property of the client.** You are merely looking after the records for the client.

Because client records do not belong to you, you cannot do whatever you like with them.

It doesn't matter what information is contained in client records – the rules are the same.

Restrictions on using client records

1. You are allowed to store client records ***only*** because you cannot provide services without those records. You cannot use them for any other purpose.
2. If you can provide services without client records, then you are not allowed to take client records.
3. You are legally obliged to ensure client records are as accurate as possible, and do not hold any information which you do not need. For example, you cannot add a note that the person is a bad-tempered, grumpy so-and-so who is never satisfied.
4. You cannot use client records for marketing. This means you cannot gather all the emails together and send out an email message advertising a gift card, workshop or anything else. If you want to use client records for marketing, you must explicitly ask the client first.

Controlling access to records

This is the really important change. You MUST comply with this section.

1. You must control access to the client records.
2. You need a **Data Protection document.** This is a formal document which lists how you control access.
    - This lists your own steps to protect client records.
    - This must include a list of everyone who has access to the records, and why they have access.
    - You must be able to demonstrate how you control access to client records.
    - It must list the name and details of who to contact if a client wants to check their records.

3. Many people believe that if you keep names separate from details you are meeting the new regulations. For example, you could have a list of client names with a code number for each, then only store the code number on their records. The idea is that looking at the record without knowing who the code number applies to makes the data safe**. THIS IS WRONG.** *This technique is discussed and specifically forbidden under the new regulations.*
4. No one is allowed access to client records unless they are:
    - Treating the client within your clinic
    - Billing the client
    - Booking an appointment
5. It is very easy to comply if your client records are on paper. It is much harder, and requires some computer skill, if you want to keep client records online or in your computer.

Client records on paper

1. If your client records are on paper, you must keep them in a locked container (box, filing cabinet, etc.)
2. You must control access to the key. Only people who need access to client records should be given the key.
3. You must record in your Data Protection Document where the key is kept and how you control access. It would be OK to simply keep the key on your key ring and state you keep the key with you at all times.
4. If you make copies of the key, you should detail how many copies, who has them, why they have them, and how they ensure no one else gets the key.

Client records online

1. If you store client records in an online system, you are responsible for how that system stores the records. It is your responsibility to ensure that system meets the new regulations.
2. You must state you have checked how their systems work, read all their privacy policies and terms and conditions, and that you certify these are all compliant with the new regulations.
3. You must ensure the following:
    - The records are stored on servers inside the EU, and never leave the EU. This means the company does not store backups outside the EU and does not transmit records through systems which go outside the EU.
    - The company staff may never look at the records. The company must maintain access records to show this.
    - The company systems may never process the records.
    - The company must store the records under encryption. Encryption must meet minimum technical standards.
    - The company may not give the records to anyone else. This means that if the company is purchased by another company, all records must be destroyed OR you will have to get permission from each and every client that the records can now be held by the new company.
4. CLINIKO PRACTICE MANAGEMENT. Cliniko is the most popular online system in Ireland for storing therapist client records. However, it is NOT compliant with the new rules because the records are stored in Australia. Cliniko have said they *hope* to be compliant by May 29, but cannot guarantee this.
5. It is not enough to trust statements by a company that they are compliant. You are legally obliged to check they are telling the truth, and you are legally obliged to say you have done this.
6. You are specifically forbidden from using the free versions of Google products for client records, such as Google Docs or Google Drive – they are all stored in the USA and read by Google. The paid Google for Business system is OK because data is stored in EU and not read by Google. But you are still obliged to read their policies and ensure they are EU compliant. Their policies are massive documents, so allow 1-2 weeks to read them.
7. **Ensuring online compliance is almost impossible.** Checking proper compliance requires information most companies will not give you, such as how they encrypt records, do backups, manage systems etc. Companies have never been asked for such information by outsiders before, and most won't even know how to tell you, and won't want to. It also requires sufficient technical skill to assess their systems. If you don't know what public key encryption is, or how virtual server systems work, you don't have enough technical knowledge to vouch for them. *If you can't vouch for them, you can't use them*.

Client records on your own computer

1. All records must be kept under password protection. This need not be complicated.
2. If you store records in Word or Excel, you can put password protection on those documents. Word and Excel have unbreakable password protection and are more than enough. How you do this is different for each version of Word or Excel. Simply search YouTube or Google for "password protect ms word" or "password protect excel" with the version (eg: "password protect excel 2010") and you will get detailed, easy to follow instructions. You can find what version you have by going into Help and then looking for "About Word" or "About Excel"
3. Alternatively, you can put password protection on the folder containing client records. Search for "password protect windows XX folder" replacing XX with your version of Windows (eg: "password protect windows 10 folder"), or equivalent for Mac IOS.
4. Alternatively, you can put password protection on the whole computer. For example, you can set your screen saver so that it requires you to log into the computer whenever you return. If you are not sure how to do this, a computer shop should be able to do this for you in 5 minutes.
5. You may not write the passwords down where they can be found. Regulations specifically forbid writing passwords on post-its and sticking them up in the office. Ideally you should memorise all passwords. If you *need* to write them down, that must be kept under lock and key. Staff may not store passwords in notebooks or on their phones, they must memorise them.
6. The best passwords are sentences. They are long, which makes them hard to break, and they are easy to remember. A password like "I-live-in-South-Dublin" is almost unbreakable. Come up with a system for creating passwords like this which are easy to remember. Do not use swearwords, names or birthdays of family members – they are the first thing hackers will try.
7. If you keep records on a laptop, you may not use that laptop over unsecured Wi-Fi connections. These are most free Wi-Fi connections available in public places like Starbucks and Airports. They do not provide sufficient security protection. If you are not sure if a Wi-Fi connection is secure, don't use it.
8. If you keep client records on your computer, you MUST have good anti-virus software. Viruses often try to steal copies of records, so you must be able to show you have taken reasonable steps to prevent this. Good virus software need not cost anything. Microsoft Defender and AVG both offer free versions and are very powerful. The important thing is that the virus software updates at least once a week. This is your responsibility. If you can't tell if your anti-virus software updates every week, change it. MacAfee and Norton's are often given free with new computers, but they require a paid subscription before they start updating. *You should have good anti-virus software anyway. If you don't have anti-virus software now, you are almost certainly infected with viruses – you can get them from just visiting a website.*
9. All of this applies just as much if you keep client records on a phone or tablet. However, getting the correct security on an Android device is technically difficult and you are better off using a Windows or Apple device.

Client access to their records

1. Clients can ask to see their records at any time.
    - You may not charge for this.
    - You do not have to give them access to records stored online or in your computer if you can print them out – just give them the paper printout.
    - You are allowed up to 14 days to comply.
2. If a client asks you to fix incorrect information, **you *must*** do so. If you think the information is correct, you can ask them for proof your information is wrong first.
3. If a client wants you to completely destroy their records, you *must* do this within 14 days. You must provide a formal statement via email or post that you have destroyed their records.
4. Clients are not allowed access to their records if seeing them would cause serious mental or physical harm. If you are not a registered doctor, psychologist or psychiatrist, you are not legally qualified to make that decision and must consult the client's own doctor, psychologist or psychiatrist for their assessment. You could require the client do this and ask the client to produce a letter from them stating it is OK.
5. You may not give client records to another practitioner. If a client wishes to transfer their files to another practitioner, give the files to the client, who can transfer them personally. Ask the client if they want you to keep a copy or destroy the records. Do not discuss the client with another practitioner unless the client formally asks for this in writing or email.

Using Phones and Tablets

1. Ensure the device locks automatically either via password, pin, fingerprint or other security system.
2. Formally log out of email, don't just close the browser or phone – that leaves the connection open.
3. Only download client data into the device if you absolutely have to in order to deliver the service, and delete it as soon as possible afterwards.

Transporting client data

1. Documents containing client personal data should be securely transported
2. They may not be left on display in transit e.g. left on the seat of a car. If someone can break into the car and steal the documents, don't leave them in the car. Documents should not be left for longer than necessary in the boot of a car.

Access to records by Garda Síochána

1. You may not show client records to the **Gardaí** just because they ask.
2. You may get permission directly from the client for this. Otherwise consult a solicitor first. The guidelines on police access are not finished at this time, but they will probably require a search warrant.

Access to records by other government departments

1. You may not allow other government departments access to client records, unless the client gives formal agreement.
2. If the department tries to insist, get a solicitor involved immediately. The government department will probably need a search warrant.

Keeping records

1. You must keep client records after the person has stopped being a client – unless the client asks you to destroy them.
2. There are no clear rules on how long you should keep them. The Data Protection Agency is currently saying seven years because you have to keep all other business records for seven years.

Email Communication

1. You should not communicate with clients using an email system which sends emails outside the EU. This includes free versions of Hotmail, Gmail, Yahoo mail, and any other US system.
2. **Gmail is especially forbidden.** The free version stores all emails in the USA and these are read by Google in order to gather information about who you communicate with and what you discuss. The paid version of Gmail is safe because email is stored in the EU and is not read by Google. Gmail for Business starts at $5/month.
3. You can *probably* send appointment reminders, but this is a grey area. You definitely cannot include any details about what's going to be treated or other medical information.
4. You may not communicate with clients via Facebook Messenger. Messenger keeps a complete copy of the entire communication in the USA and processes it.
5. In general, try to avoid communicating with clients via Facebook at all. Facebook have claimed to be compliant, but current legal opinion is that they are not.

Shredding Documents

1. Ensure that shredding bags or bins are not left open when full. Documents for shredding containing personal or sensitive information should be treated with the same security as if they were still on your desk until they have been destroyed.

Training

1. The Data Protection Commission has prepared a series of PowerPoint presentations on different aspects of data protection which are available on its website and on You tube. (www.youtube.com/dataprotection).

SUMMARY – making it easy

The easiest solution is:

1. Keep all client records on paper, in a locked box.
    a. Keep the key with you at all times.
    b. Write up a document which says this and put it somewhere on the wall where clients can see it.
2. Use a paid email system, like Office 365 or Gmail for Business.

Data Policy Statement

(insert practice name) recognises that your privacy is important and is committed to respecting your privacy. We will apply appropriate protection and management of any information you share with us. The information you submit will be kept confidential and with the highest standards of security. The information you provide will be held and used in accordance with the General Data Protection Regulations.

Any personal information provided by you will only be used for the following purposes:

- Delivering therapies
- Booking appointments
- Billing
- Marketing (but only if you agree)

Staff will only be allowed access to your records for these purposes.

We may also be required under law to surrender records to a legal authority. We will inform you of any such request unless forbidden by law.

Please understand it is not possible to treat you if we cannot hold any records on you at all.

Data Controller

You should contact our Data Controller for all matters related to your records. The Data Controller for this clinic is (insert name). They can be contacted by phone on (phone number), by email at (email address) and by post at (postal address).

Where is the data stored?

Records are stored in a locked filing cabinet at (insert address).

The key holder is …….. and the key is kept with this person at all times.

Who has access to your records and why?

(list all people by name, and which of the above purposes they need access for)

We will not share your records with any commercial organisation or therapist under any circumstances.

How long is data retained?

All records must be retained for a period of 7 years after the last appointment. However, all records will be destroyed at any time if you request it.

Your rights

You can demand to see all our records on you at any time. Please allow up to 14 days for us to provide them. If you think some information is incorrect, or not needed for the above purposes, you may request we correct or remove it. Since this is an important change, please do so in writing via registered post. Where records are held in computers, in the interest of preserving data security, we reserve the right to provide printed copies instead of electronic files.

You can demand we destroy all records we hold on you. Please allow up to 14 days for us to comply. Requests for destruction of records should be sent in writing via registered post.

Consultation Form

You will need to add the following to the end of your consultation form:

☐ I give permission for you to hold my records in order to deliver your services (*Please tick the box)*

(Please understand that if you decline to give the above permission we will unfortunately be unable to deliver any services to you)

☐ I give permission for you to use this information for marketing purposes such special offers and health information (*Please tick the box)*

(This is completely voluntary and you are under no obligation to agree. This will not affect how we treat you)

Client Review of Consultation Form

We recommend that you request each client to review their consultation form, to make any adjustments that are necessary and to sign the form for each treatment. Here is a sample of a second sheet that can hold the signatures each visit:

I confirm that I have reviewed and updated my personal consultation form and have informed this practitioner of any changes in my health conditions or medication.

Client Signature _____Date _____ Therapist Sig._____

Client Signature _____Date _____ Therapist Sig._____

Client Signature _____Date _____ Therapist Sig._____

Client Signature _____Date _____ Therapist Sig._____

Client Signature _____Date _____ Therapist Sig._____

Client Signature _____Date _____ Therapist Sig._____

Client Signature _____Date _____ Therapist Sig._____

Client Signature _____Date _____ Therapist Sig._____

Client Signature _____Date _____ Therapist Sig._____

Client Signature _____Date _____ Therapist Sig._____

What the New Laws mean for you as an individual
from the Official GDPR Website

General Data Protection Regulation (GDPR) from 25th May 2018 will replace current data protection laws in the European Union.

The new law will give individuals greater control over their data by setting out additional and more clearly defined rights for individuals whose personal data is collected and processed by organisations. The GDPR also imposes corresponding and greatly increased obligations on organisations that collect this data.

Personal data is any information that can identify an individual person. This includes a name, an ID number, location data (for example, location data collected by a mobile phone) or a postal address, online browsing history, images or anything relating to the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

The GDPR is based on the core principles of data protection which exist under the current law. These principles require organisations and businesses to:

- collect no more data than is necessary from an individual for the purpose for which it will be used;
- obtain personal data fairly from the individual by giving them notice of the collection and its specific purpose;
- retain the data for no longer than is necessary for that specified purpose;
- to keep data safe and secure; and
- Provide an individual with a copy of his or her personal data if they request it.

Under the GDPR individuals have the significantly strengthened rights to:

- obtain details about how their data is processed by an organisation or business;
- obtain copies of personal data that an organisation holds on them;
- have incorrect or incomplete data corrected;
- have their data erased by an organisation, where, for example, the organisation has no legitimate reason for retaining the data;
- obtain their data from an organisation and to have that data transmitted to another organisation (Data Portability);
- object to the processing of their data by an organisation in certain circumstances;
- Not to be subject to (with some exceptions) automated decision making, including profiling.

Organisations and businesses collecting and processing personal data will be required to meet a very high standard in how they collect, use and protect data. Very importantly, organisations must always be fully transparent to individuals about how they are using and safeguarding personal data, including by providing this information in easily accessible, concise, easy to understand and clear language.

For organisations and businesses who breach the law, the Data Protection Commissioner is being given more robust powers to impose very substantial sanctions including the power to impose fines. Under the new law, the DPC will be able to fine organisations up to €20 million (or 4% of total global turnover) for the most serious infringements.

The GDPR will also permit individuals to seek compensation through the courts for breaches of their data privacy rights, including in circumstances where no material damage or financial loss has been suffered.

In the coming period further information will be provided here on the rights of individuals under the GDPR.