GDPR: PRIVACY NOTICES

This advice has been prepared using guidance provided by the Information Commissioner's Office (ICO). It has been discussed with their advice team and we are assured that it is perfectly adequate for an osteopathic or chiropractic practice, or for any similar business.

It doesn't have to be difficult

You DO NOT have to put up a sign in your practice, and patients DO NOT have to sign to say that they have read your privacy notice.

It is sufficient to have the privacy notice posted on your website – just make sure that it's easy to access. When patients sign to give consent that you can process their data, you could have a copy of the notice for them to read, or you could simply direct them to your web page. Don't get in a tizz about it.

Don't let anyone convince you that you have to have a multiple-page, complicated and exhaustive privacy notice on your website in order to "stay legal".

It doesn't have to be lengthy, nor does it need to be written in complex, legal, bureaucratic language.

Here's what a privacy notice should include according to the ICO:

- the intended purposes for processing the personal data
- the lawful basis for the processing
- your retention periods for that personal data (maybe Simon's chambers should also have included this)
- who it will be shared with (other practitioners, receptionists, external service providers such as PPS, TM4 or Cliniko, your Customer Relationship Manager (eg Mailchimp)).
- the identity and contact details of the data controller (normally the practitioner/practice principal)
- The right to request rectification of errors, access to data, or erasure of data (provided this is not overridden by the statutory minimum)
- The right to complain (and how – remember this relates to data processing, not health care)

- If the provision of data is a contractual requirement, whether you consider the data essential for you to fulfil your part of the deal.

It is also useful to include any relevant security measures you have in place, but it's not compulsory.

It is also useful to include any relevant data security measures you have in place, but it's not compulsory.

You are not required to spell out in your privacy notice an individual's full rights under the GDPR/Data Protection Act.

Here's an example which could be adapted for use in your clinic:

The panel below covers all the essentials of a privacy notice, and has the merit of being concise and easy to understand (the latter is a requirement of your communication under the GDPR). **The ICO have confirmed that the information provided is adequate.**

You can use this and edit it to suit your specific circumstances but don't get worried about it being written in "legalese". It has to be accurate, but you are allowed to express your own circumstances in your own words – ie in a way that another ordinary person will understand.

You will not be penalised for this – it's better that the statement is readable, than that it looks like it was produced by a committee of civil servants!

PRIVACY NOTICE

(Why we collect your personal data and what we do with it)

When you supply your personal details to this clinic they are stored and processed for 4 reasons (the bits in bold are the relevant terms used in the General Data Protection Regulation – ie the law):

1. We need to collect personal information about your health in order to provide you with the best possible treatment. Your requesting treatment and our agreement to provide that care constitutes a ***contract****. You can, of course, refuse to provide the information, but if you were to do that we would not be able to provide treatment.*

*2. We have a "****Legitimate Interest****" in collecting that information, because without it we couldn't do our job effectively and safely.*

*3. We also think that it is important that we can contact you in order to confirm your appointments with us or to update you on matters related to your medical care. This again constitutes "****Legitimate Interest****", but this time it is your legitimate interest.*

4. Provided we have your ***consent****, we may occasionally send you general health information in the form of articles, advice or newsletters. You may withdraw this consent at any time – just let us know by any convenient method.*

We have a ***legal obligation*** *to retain your records for 8 years after your most recent appointment (or age 25, if this is longer), but after this period you can ask us to delete your records if you wish. Otherwise, we will retain your records indefinitely in order that we can provide you with the best possible care should you need to see us at some future date.*

*Your records are stored**

on paper, in locked filing cabinets, and the offices are always locked and alarmed out of working hours.

electronically ("in the cloud"), using a specialist medical records service. This provider has given us their assurances that they are fully compliant with the General Data Protection Regulations. Access to this data is password protected, and the passwords are changed regularly.

on our office computers. These are password-protected, backed up regularly, and the office(s) are locked and alarmed out of working hours.

We will never share your data with anyone who does not need access without your written consent. Only the following people/agencies will have routine access to your data:

- *The medical records service who store and process our files*
- *Your practitioner(s) in order that they can provide you with treatment*
- *Our reception staff, because they organise our practitioners' diaries, and coordinate appointments and reminders (but they do not have access to your medical history or sensitive personal information)*
- *Other administrative staff, such as our bookkeeper. Again, administrative staff will not have access to your medical notes, just your essential contact details. • We also use Mailchimp to coordinate our messages, so your name and email address may be saved on their server.*

From time to time, we may have to employ consultants to perform tasks which might give them access to your personal data (but not your medical notes). We will ensure that they are fully aware that they must treat that information as confidential, and we will ensure that they sign a non-disclosure agreement.

You have the right to see what personal data of yours we hold, and you can also ask us to correct any factual errors. Provided the legal minimum period has elapsed, you can also ask us to erase your records.

We want you to be absolutely confident that we are treating your personal data responsibly, and that we are doing everything we can to make sure that the only people who can access that data have a genuine need to do so.

*Of course, if you feel that we are mishandling your personal data in some way, you have the right to complain. Complaints need to be sent to what is referred to in the jargon as the "****Data Controller****". Here are the details you need for that:*

Where children are concerned:

You are unlikely to be dealing directly with children; it is more likely that you will deal with their parents or guardians. Children must however understand why you require the personal data you have asked for, and what you will do with it, in a way which they can understand.

If you do deal with children directly (that is, persons under the age of 16), you might want to consider child-friendly ways of presenting privacy information, such as:

- diagrams
- cartoons
- graphics and videos
- dashboards
- layered and just-in-time notices, icons and symbols (see below).

If relying upon parental consent you could consider having two different versions of privacy notices; one aimed at the holder of parental responsibility and one aimed at the child.

Our advice is that the example we gave above is adequate. You are under a legal obligation to preserve medical records, but it would be very unusual if you were communicating directly with children themselves.

Alternative ways to present information:

- ***A layered approach*** *– short notices containing key privacy information that have additional layers of more detailed information.*

- ***Dashboards*** *– preference management tools that inform people how their data is used and allow them to manage what happens with it.*

- ***Just-in-time notices*** *– relevant and focused privacy information delivered at the time individual pieces of information about people are collected.*

- ***Icons*** *– small, meaningful, symbols that indicate the existence of a particular type of data processing.*

- ***Mobile and smart device functionalities*** *– including pop-ups, voice alerts and*