

# DRAFT

## GDPR: WHAT INFORMATION MUST YOU PROVIDE TO YOUR CONTACTS/PATIENTS?

1. The name and contact details of your organisation
2. The name and contact details of your representative
3. *The contact details of your data protection officer (not relevant)*
4. The purposes of the processing
5. The lawful basis for the processing:
  - eg medical records retention
6. The legitimate interests for the processing
  - you have asked for information on a specific subject (through an advert, or by ticking a consent box on a website or clinic sign-up form)
  - information may be relevant to your medical condition (I'm trying to help)
7. The categories of personal data obtained (not necessary if provided by the person concerned)
  - Name and address
  - Date of Birth
  - Email address
  - Telephone number(s)
  - Medical history
  - ***Medical information provided by third parties (MRI reports/scans, consultant reports)***
8. The recipients or categories of recipients of the personal data:
  - generally none, without the patient's permission
9. *The details of transfers of the personal data to any third countries or international organisations (not relevant to osteo and chiro clinics)*
10. The retention periods for the personal data (8 years or up to age 25 if longer for medical records)
11. The rights available to individuals in respect of the processing:
  - to be informed of what is kept (unless they provide it in person – in which case they know!)

# DRAFT

## **DRAFT**

- to access data (free of charge, and within a reasonable, very short, timescale)
- to rectify errors
- to be forgotten (but not erasure of medical records, and you can always keep sufficient data to ensure that you know the contact has asked to be forgotten)
- to restrict processing (usually only if there's a legal dispute)
- to data "portability" (ie have it sent to an alternative practitioner)
- to withdraw consent (this opportunity must be clearly available and simple to take up)
- to object (particularly to marketing information, but also for scientific/statistical processing)
- to lodge a complaint with a supervisory authority

12. The source of the personal data (not necessary if it's the person themselves)

13. The details of whether individuals are under a statutory or contractual obligation to provide the personal data (not relevant)

14. The details of the existence of automated decision-making, including profiling (not relevant)

## **DRAFT**