The data we handle and the legalities of holding data

As a healthcare company, Core Body Clinic Ltd. has a legal obligation to collect and process information for the purposes of medical records and also personal records from both patients and our staff. We also must process any information we receive from website enquiries. Therefore, we ensure we have a strict policy on data protection and ensure we follow the best practice guidelines as indicated by GDPR.

In 2015 we began using a software package called **TM3** (Blue Zinc) for all our diary and booking handling and for the storage of patient-specific case notes and personal data. TM3 is a secure database that is accessed via an encrypted server over the internet. For each practitioner, there is a unique username and password for accessing the database. The system is logged out if the screen is left idle ensuring that no one else can access the computer. TM3 is backed up by 3 servers so your data is safe from being lost and there is no chance the system can be accessed by a third party.

Core Body Clinic, Ltd. directors, Adrian Wagstaff and Sarah Wagstaff have gone through many years of data protection training. For the purposes of fulfilling our GDPR obligations, both directors represent the clinic, with Sarah being the official Data Officer. You can email her at info@corebodyclinic.co.uk as she is the principal administrator.

Terms:

Personal Data

This amounts to all the information we hold about a person. This includes name; date of birth; address; email; phone number; and GP. It also includes personal information concerning your health, information that you have volunteered to share during a consultation. We hold this information about patients and staff. We have a legal obligation to do so.

Clinical Notes

These are the clinical details about the injury or problem for which you have attended the clinic. They are highly sensitive and often contain personal and private information. Clinical staff are governed by the Data protection act, the competencies set out by the Health and Care Professions Council (HCPC) and the Chartered Society of Physiotherapy. They are not shared with anyone. Misuse or sharing without your consent will result in dismissal and reporting to the HCPC.

Consent

“permission for something to happen or agreement to do something” (Oxford.)

When a patient comes into the clinic, we ask them to sign and read our consent form. It is important that you understand that we will look after your data and not share it with anyone. Furthermore, if you want to see how we handle the data and how we ensure it remains secure you can ask to see our policy on data control. The added importance of the consent form is that you give your approval for data handling and storage, and an assessment and treatment with the clinic. We need you to be informed about the process of assessment and treatment and ensure you are clear about this process. For this, we need your consent. Signing the document ensures we have your approval, even though you have made the conscious decision to book and attend a consultation. In any case, we treat your private information with absolute confidentiality.

ICO – Information Commissioners Office

HCPC – Health and Care Professions Council

What is GDPR (General Data Protection Regulation) ?

GDPR has been set up to allow consistency throughout Europe with the handling of data and to ensure all companies and service providers handle data in an appropriate and fair way and in a way that is explicit to customers and patients. The key areas that GDPR highlight as being particular data rights for individuals are listed below:

- Right to be informed – the fair processing of your data
- Right to access – the data we hold on you
- Right to erasure – the right to be forgotten should you wish to delete your data
- Right to recertification – if we hold data that is inaccurate then you may ask for it to be rectified
- Right to restrict processing – to prevent the processing of your data
- Right to data portability – transferring your data elsewhere
- Right to Object – to processing, marketing that is direct and the use of your data for research.
- Right to question automated decisions

Why do you need my data?

Medical and healthcare notes must be kept in a concise and intelligible way so that is clear a clinician has collected sufficient information, and that this information tells a story about an individual's problem. We must keep this information as evidence that we have treated you as this forms an important part of your medical history. We are required by law to keep this for 7 years after you have visited the clinic if you are over 18 years of age at the time of the 1st consultation. If you are under 18 then we must keep the information for 25 years. Should you wish to reflect on your treatment some time afterwards, then having accurate and available notes would support the involved parties.

Your personal information relating to address and date of birth is essential so that we can accurately identify a patient. We may have 2 or 3 patients on our system with the same

name. We may only be able to tell them apart by date of birth or address. These details are essential and must be included within your consent, so we can securely identify our patients. This information is kept as a minimum for the duration of the treatment.

Who owns my data?

Core Body Clinic, Ltd controls your data and we obtain the information from our patients and staff. However, it is the individual themselves who 'own' the data. None of your data will be transferred without your consent.

Why do you want my email?

Email is the standard way to communicate with patients and we have had great success in developing a business that relies on email. If you wish to book an appointment online, then we will require an email. At Core Body Clinic, Ltd. we only use emails to provide details about your appointment booking or to relay information about our opening times. Emails also provide a reminder about a booking. These are sent at the time of booking and also automatically sent out the day before your appointment. We may send you an email about your treatment and for communication relating to billing. We will also send an email about special opening times. Any sensitive information will only be passed to you via email if you approve. We do not send out marketing material via email and will only send emails if they are relevant to your time at the clinic. If you have opted to have an email sent to you or to join our mailing list, then we will add you to the list. If you want to be removed, then this will be done on request. You do not have to give an email. However, we find this is best for appointment reminders.

We will never share your email with anyone else.

Can I see my clinical notes and the data you hold about me?

Yes, we will make this information available for you at any time you wish. You will need to write to the Data Protection Officer (Sarah Wagstaff) or the Director (Adrian Wagstaff) and consent to the release of the information. A small administration charge is made for this.

Insurance companies can also request to see the notes. However, you must give your consent for this, and we would require written approval from the patient.

What if I don't want my data stored?

Should you not wish this information to be kept after your treatment is complete you must be aware that it is the policy of Core Body Clinic Ltd that notes would be kept for 7 years or 25 years in the clinic. The law requires that your notes be kept for the required duration. This protects both patient and clinician. You have the right to ask for the data to be transferred and destroyed. This does affect our legal obligations.

How do you know you are secure?

To ensure we are maintaining security we perform an audit once a year to ensure all our processes are in keeping with GDPR.

We have prepared our checklist in accordance with the guidelines set out by ICO (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/)

I have paid by card payment, is this safe?

We take payments through World Pay. This is chip and pin and is one of the safest methods to take a card payment. We are compliant with the PCI DSS (payment card industry data security standard). This is something that we check annually with World pay.

I want to know how my data is stored

You can have all the information relating to data storage by requesting a call back from the clinic directors or by emailing info@corebodyclinic.co.uk.

Audit Date: 20th June 2019

Article update: 23rd June 2019