RUTH COOIL
PHYSIOTHERAPY
& HEALTHCARE SERVICES

Data protection / Security / Complaint policy

Ruth Cooil Physiotherapy is a Ltd company trading as Ruth Cooil Physiotherapy and Healthcare Services. Allied Health Professionals (AHP's), Sports Masseurs, dietician and Doctors are required to adhere to their professional standards and be registered with the Health Professional Council (HCPC) or appropriate governing body. These regulations enforce the maintenance of high quality physiotherapy /massage/dietician /medical services and ensure to maintain confidentiality of patient and their medical records. The latest GDPR as implemented from 25th May 2018 is making our standards and codes regarding data protection also a legal requirement.

Data Collected

1) Contact details – e.g. name, address, telephone number, email address
2) Referring doctor (if appropriate)
3) Medical record – Written notes on every session, all correspondence such as referral letters, reports to other health professionals, work, lawyers.

Need for data collection

1) We need contact details to contact patients to arrange appointments, cancel or alter appointments. The patient must complete the provided information, data and consent sheet on first visit. If there is a change to existing data a new form must be completed as soon as possible.
2) We need to be able to contact a next of kin in case of emergency while at the clinic.
3) We need to be able to invoice patients for outstanding payments and send receipts for money received if required.
4) We need to be able to legally identify and match medical records with the correct individual.
5) A written / electronic record of every session and contact between patient and staff member is a legal requirement. These notes will be required by court in any dispute,

complaint and litigation. These records must be kept for a minimum of 8 years. If for 8 years no further contact has been made these records will be destroyed by shredding or incinerating.

6) Tax law require that all proof of income that will include invoices, receipt records must be kept for a minimum of 6 years.

Consent

To comply with the legal basis, consent of the individual must be obtained. Two different levels of consent are applicable to this clinic. Implied consent is an acceptance of care by the individual and authorised by the individual. This implied consent is applicable to contact details being collected and used between the clinic and the individual. The implied consent also authorizes the transfer of personal data between team members of the direct care team of the individual. This transfer can be between allied health professionals, doctors and other health professionals such as psychologist, personal trainer / strength and conditioning coach. Consent for assessment and treatment for the person and collecting of the personal data will be obtained.

The second level of consent is applicable to the special category and GDPR article 9 which demands explicit consent. There personal data covered by explicit consent is the processing / sharing of medical records / notes with a third party that is not part of the direct care team, such as workplace or lawyer. A written authorization letter by the patient is required.

Right of refusal to consent

GDPR gives each individual the right to refuse consent to all or part of data collection and control. The individual also has the right to retract their consent. In the case of refusal or retraction this clinic will then fail to comply with legal requirement and commit a crime if proceeding with treatment without keeping proper documentation. Treatment will be refused. The individual will have to seek help elsewhere.

Storage of data

Each patient has an electronic file held on a server in the UK via PPS. All written notes and correspondences in paper form are scanned on to the file. Written notes are stored in a locked filing cabinet.

Contact details and the daily diary are held on the PPS system. Email communication is via the clinics email address.

Data access

There are no administrative staff for the clinic. Only the staff providing clinical care have access to the filing cabinet, PPS system, email address and accounts spreadsheets. The confidentiality and privacy of each patient and their medical record is of utmost importance to the clinic. The clinic promises to uphold and treat personal data with respect and keep it secure.

If an administrative clerk is required, the clerk will be vetted and trusted to behave and conduct him/herself to the high professional standards this clinic demands.

Each patient has the right to view or have a copy of their own medical records and / or correspondence. Copies of the record will be given to the individual within 1 month.

In case of a third party, for instance with litigation a lawyer or a consultant, wants to have a copy of the whole or part of the medical records a written authorisation by the patient is required by the clinic before any copies will be handed over.

We will never sell or pass on contact details or spreadsheets to other companies, practices or marketing sites.

Security

The clinic will make every effort to keep data secure. The PPS patient management system is secure, backed up, password protected and the devices are scanned regularly for breaches.

Paper records are stored in a locked draw, the clinic room is locked and the main entrance to the waiting area is locked once everyone has left the building.

This clinic does not have an encrypted email service; transfer of medical records will be done either in person, mail or password protected.

Security breach

The patient will be informed immediately by the clinic of any security data breach. Steps to recover data if possible will be taken. If required the necessary authority, CSP, Police, IOC will be contacted.

In case of loss of medical records the IOC must be informed within 72Hrs

We undertake to learn from the mistakes and possible gaps and change our policy as to prevent a similar breach.

Regular review or change in practice or contact habits that will force a review will help to keep the clinic up to date.

Complaints

The clinic will endeavour to resolve all complaints internally. If this is not possible or the complaint identifies a serious breach of data protection, mediation will be obtained. This will be provided by the relevant professional network and /or the IOC. Patients can complain directly to the HCPC.

Research

The clinic does not take part in research or clinical trials, therefore data will not be released for this purpose.

Social Media and Advertising

Any patient details will be removed from any social media or marketing posts and consent gained on the use of images. The providers will endeavour to follow the advertising standards authority requirements found - Non-broadcast Code - ASA | CAP and refrain from commenting on emotive posts.

Created December 2019
Review date December 2021 completed
Reviewed Dec22, Reviewed April 2024, Reviewed April 2026
Next review April 2028