1. Introduction

This document provides information about how we collect and process personal data for the **patients that we assess, report on and offer treatment to**. Your rights and protections are a high priority. The information provided below is to more fully explain our privacy approach. Where you have entered general "contact us" and other information on our web site please see our web site privacy policy. Should you have any questions or if you think there is information that would help improve this document please contact us tel: 01905 612056 email: enquiries@sunrehab.co.uk

We want you to be comfortable about patient confidentiality. Our clinical staff are governed by the regulations laid out by the Chartered Society of Physiotherapy and the Health & Care Professions Council. Our administrative staff are supervised under the same regulations**.** Our clinical partners are subject to the same regulations in their own right and by agreements with us. Other suppliers only have access to information when needed under strictly controlled conditions and confidentiality.

2. Information use

Sun Rehabilitation is an occupational health (OH) provider registered with and regulated by the Information Commissioner (ICO) www.ico.org.uk under the Data Protection Act.

- We are a Data Controller and sometimes a Joint Data Controller
- Our technology and clinical partners are Data Processors working under our direction.

We use your information to provide you with our occupational health services which are designed to help you be "well at work". These may include:

Physiotherapy | Case Management | Workplace assessments | Vehicle Assessments | Training and advice |Statistical information for your employer to prevent injuries at work (anonymous data only)

In some specific cases where we conduct onsite company-based clinics (where the records are not held by us the company is the Data Controller) we only process referral data in providing that treatment. In these cases, we do so under a processing contract with that Data Controller. We may gather and report anonymised statistical data to demonstrate the service provision.

3. Information we collect

- Contact details, age, gender, personal and job role information to help communicate with you and provide the correct care
- Sensitive health information (where it may impact treatment), information on the condition we are to review and treat
- Sometimes we use photographs to help us to be accurate in describing the problems and recommending treatment (we will normally discuss this with the patient at the time)

4. Information Sharing

- We will not disclose your information out side of the Sun Rehabilitation businesses and your referrer except as below
- We will share your information with our network of regulated, physiotherapy and occupational health partners where appropriate. This allows us to provide you with occupational health services closer to your work place or home.
- With our data hosting partners working to strict security and compliance standards. These parties are Data Processors under our control by contract.
- Where your employer or occupational health service has referred you, we will provide them with a report normally after the initial assessment, and if treatment is given during the course of treatments and at your treatment discharge
    a. You will be asked on a consent form to choose how this is handled under the Access to Medical Reports Act
    b. Summary details of this information can be found in the Access to Medical Reports section of this document

5. Your Rights

Your privacy rights and preferences are important to us. In some cases, you have the right to change your mind in respect of information that you have given us. This is covered under the rights set out below.

You as the Data Subject have the following rights under Data Protection Legislation.

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

For example, our consent documents, our privacy information web pages and other information that we provide to you are part of our obligations under item 1, the right to be informed and in some situations our need to gain your consent.

6. Lawful Basis

The lawful basis for collecting and processing patient data is not always simple. We have set out below a rational for the lawful use of data for the various and sometimes complex circumstances that exist in our organisation when we provide occupational services.

Basic contact data

Our lawful basis for holding your basic contact details is

Where we have an arrangement directly with you the patient: Lawful basis is “Contract/ pending contract” (Article 6(1)b of the GDPR regulations).

Where we hold a contract directly or indirectly with your employer/ OH referrer for delivering these services: Lawful basis is 6(1)f “legitimate interest”.

We may use this contact information to contact you to better understand your needs and process the referral. This for example may include your preferred treatment location.

Sensitive or Special Category Health-related Information

Where a referral containing health-related data comes from a third party such as an OH referrer or employer we will hold that data securely and use it to arrange appropriate services for the patient.

If we do not receive clear information from the third party we will hold patient data securely for a short time on the assumption that the provider has a clear legal basis to supply the data to us.
If we do not receive sufficient information to confirm the legal basis from the referrer or the patient we shall delete the health-related data. We may not then be able to treat the patient until we have collected the required data again.

Our lawful basis for processing sensitive health related data and any health professional notes and reports is

As health professionals based on our contract with the patient or the employer or OH referrer to provide OH services.

As described in Article 9(2)h of the GDPR regulations “purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis”

This is subject to paragraph 3 (which states “when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy”).

We will ask the patient for medical treatment and reporting consent at the earliest opportunity in our assessment and / or treatment cycle and that shall be at or before the first appointment (normally <1 month).
This is to ensure the preferences of the patient are clear for the sharing of any report with other parties such as the patients OH referral company and employer. This provides choice for the patient specifically under the separate “Access to Medical Reports Act 1988”.

There may be times when we disclose information under a legal obligation, in this case we will disclose information that is required of us by law on receipt of an appropriate request.

Urgent Care

Although very unlikely, should you need any urgent care while being treated by one of our professionals we may share your information with emergency services under the Vital Interest lawful basis (9(2)c of the GDPR regulations but by verbal consent if you are able. This is reserved for rare situations where your life may be at risk or you need urgent care to protect your health.

Telephone consultations only

Our practitioners shall take appropriate measures to properly identify the patient on the call before discussing sensitive information.

The telephone consultation will often include the sharing between patient and healthcare practitioner of sensitive health-related information. The lawful basis remains in this case as stated above.

In the case of a telephone consultation it is NOT considered practical to seek signed consent. To ensure we have considered the rights and preferences of the patient we will seek to verbally obtain the consent of the patient during the call. The practitioner shall document this on the normal consent form and sign as the Clinician. They will note the patient was not present. The form shall be processed and filed in the normal way with the case documentation.

7. Data Processing

We process data when we receive a referral from the patient or the employer or a third party occupational health provider servicing the patient or their employer.

Where we have asked for or receive health-related information and are providing occupational health related assessment or treatment we will process this data as required under Article 9(2)h of the GDPR regulations. Your employer or OH provider should explain to you that they intend to pass your referral data to us.

Where we keep your Data - our cloud providers

We only hold and process sensitive health-related information in secure systems and/or the data is encrypted.
Our main provider (Data Processor) is the well-established global cloud service firm Citrix. Your data is held in secure, certified data centres (run by Amazon Web Services) within the European Union. Data is encrypted in transit and at rest to ensure its security. Citrix maintain strict levels of compliance with recognised international security standards (ISO 27002).

Some Citrix data processing takes place in certified data centres in the USA (and other countries) under a contract containing clauses agreed by the European Union to provide the same level of protection and in compliance with the General Data Protection Regulations. For transparency we have provided the documents below which set out agreements with Citrix. These include the data processing contract as required under the regulations along with a description of procedural and technology security protections that are in place. Also included is a list of Citrix partners (sub processors) that are held to the same contractual terms.

https://www.citrix.com/content/dam/citrix/en_us/documents/buy/enterprise-saas-eusa.pdf

https://www.citrix.com/buy/licensing/citrix-data-processing-agreement.html

https://www.citrix.com/buy/licensing/citrix-services-security-exhibit.html

https://www.citrix.com/buy/licensing/subprocessor-list.html

Where we keep your Data - our clinics and assessors

All of our clinical partners across our network clinics and teams of assessors are subject to the same conditions of professional confidentiality as Sun Rehabilitation and are regulated in a similar way. We have established contracts of engagement with these partners controlling how they process your personal data in line with the data protection regulations.

8. Data Retention

We are bound by our professional body (Chartered Society of Physiotherapy) and governing authority (Health & Care Professions Council), to keep records of your assessments and any treatment you receive.
Our normal retention period shall be eight years (if a retention period for a particular type of information is unclear we will revert to the recommended periods set by the NHS). The legal basis under which we retain these records is Article 9(2)g "substantial public interest" to ensure that we can support your ongoing care if needed and 9(2)f "exercise or defence of legal claims".

9. Contacting us to ask a question, put something right or complain.

If you have a simple question about our service please give us a call and we will try to put your mind at rest. Call: 01905 612056

If you wish to make a formal request under Data Protection Regulations, such as:

Ask a formal question or require more information| Access your record that we hold | Rectify any error in your record | Discuss erasing your record (which we can do in certain circumstances) | Restrict processing | Take your record elsewhere | Object to something we might have done relating to your data | Exercise your rights around issues of automated decision making

Please submit a request in writing to the Data Manager, Sun Rehabilitation, Workshop Business Centre, Main Street, Pinvin, Worcestershire, WR10 2ES or by email to enquiries@sunrehab.co.uk

This helps us to agree a way forward having considered your problem fully. If you have difficulty in doing this we can help you, so please call us. However please take care not to write sensitive health or personal information in an email as this form of communication is NOT secure. Alternatively, you may complete the secure online form here.
https://podio.com/webforms/20473046/1400870

Please provide enough information for us to:

Contact you |Identify you |Find our records of your assessments or treatments |Understand your issue or problem |Understand what you believe we should do to resolve the situation.

The Information Commissioner has some useful advice on handling complaints https://ico.org.uk/for-the-public/raising-concerns/

We carry out identity checks to ensure we are talking with the right person. We will answer a lawful request and will not normally charge you for accessing your data protection rights so long as your request is clear, fair and reasonable and does not breach any other rights or obligations.

We have 30 days to review your request and respond to you once we have identified you and understand the scope of your request (in some clearly defined circumstances this can take longer). We will work to respond as soon as we practically can. If you are not happy with the outcome of a request to us please do get in touch again. We will try to resolve the issue with you.

In any event you may complain to the Office of the Information Commissioner if you feel that you cannot reach a resolution with us. The ICO website is www.ico.org.uk for general advice or concerns reporting https://ico.org.uk/concerns/

10. Access to Medical Reports

ACCESS TO MEDICAL REPORTS ACT 1988 (Revised September 1995)

Summary of Rights Related to Medical Reports Obtained from GP's and Medical Consultants

No application may be made to a General Practitioner or specialist/ consultant for a medical report relating to an employee without:

a) The employee being notified that a report is being requested, and

b) The employee's consent to the application being made

An employee has the right to:

- Refuse to allow a report to be requested from a general practitioner or specialist

- Request to see the report before it is sent
- Refuse to allow the report to be sent, after having seen it
- Request that changes to be made to report before it is sent because he/she considers it to be incorrect or misleading, (this request must be made to the GP or specialist in writing) or
- Request that his/her views are attached to the report if there is any of it with which he/she disagrees and which the GP or specialist is not prepared to alter, (again this request must be made to the GP or specialist is not prepared to alter, (again this request must be made to the GP writing).

If the employee request access to the report before it is supplied, Sun Rehab Ltd must:

- Notify the employee when the report is being requested from the GP or specialist
- Notify the GP or specialist that the employee has made such a request.

The GP or specialist may not then supply the report unless:

Consent has been given; OR The report has been amended to take account of the employee's views or statement of those views has been attracted to it; OR A period of 21 days from the date the application for the report was made had gone by without the employee having contacted the GP to make arrangements to see the report.

If an employee consents to the report being obtained without requiring access to it prior to it being given to Sun Rehab Ltd, but subsequently decides that he/she wishes to have access to it, he/she may approach the GP or Specialists direct. In such circumstances the GP or specialist may not give the report to Sun Rehab Ltd without the employee's consent (subject to any amendments), or until a period of 21 days has passed since the employee indicated his/her wish to see the report, without the employee having contacted the GP to make arrangements to see the report.

A GP or specialist is required to give an employee access to any medical report supplied about him/her for employment or insurance purposes in the previous six months, at the employee's request.

A GP or specialist is not obliged to give access to medical report where disclosure would, in the opinion of the GP or specialist, cause serious harm to the physical or mental health o the employee, or others, would indicate the intentions of the GP or specialist in respect of the employee or where disclosure would reveal information about another person who has supplied information to the GP or specialist, unless that person has consented, or is a health professional where the information was provided in a professional capacity.

In these circumstances the GP or specialist will inform the employee that this so, and will give access to any parts of the report not affected by the above clauses. The GP or specialists will not pass on the report unless the employee gives consent.

Independent Medical Reports- Medical Reports prepared by Sun Rehab OH practitioners and sent to your employer.

It is Sun Rehab's policy that its physiotherapists should be prepared to discuss with the employee the purpose of the assessment, content of their reports and especially the type of questions that they are being asked to answer.

You can withhold your consent at any stage of the purpose and cannot be compelled to proceed. However, you must understand that management will then have to proceed and cannot be compelled to proceed using only their current knowledge and without any expert medical opinion.

Should you wish to amend a report before it is released then you have the right to suggest amendments regarding ''facts'' but not the OH Physiotherapists opinion.

Should you wish to make any comment about the occupational health report please contact your Human Resources Department or Manager who will liaise with Sun Rehabilitation on your behalf.