

DATA PROTECTION POLICY

Symbios Health

Controlled Document

Copyright © Symbios Health. All rights reserved.

Reference number	POL109
Version	3
Date ratified	06.03.2025
Due for review	06.03.2027
Review period	Two years unless a need for review has been identified
Committee/individual responsible	Company Director Symbios Health
Target audience	All Symbios Health staff
It is the responsibility of the Administration team to ensure this document is updated in a timely manner, controlled, and shared via teams.	
Uncontrolled Document if Copied or Printed	

Implementation plan

Group	Objective	Method	Lead	Target Start	Target End	Resources
All employees	Employees to read, understand and follow this policy.	Policy available on SharePoint	Clinical Lead, Company Director	Mar 25	Apr 25	Employees to attend Teams meeting. Reference to SharePoint -clinicians – documents - policies

Amendments

Version	Amendments	Date
2	Retention period changed from 5 to 6 years.	21.04.24
2	Clarification on “right to be forgotten” in Storage Limitation.	21.05.24
2	Removal 6 year time frame for keeping COSHH records.	21.05.24
2	Data controller details and email changed to Dr Jonathon Whittle under section 4. Data Compliant.	21.05.24
3	Data controller changed back to Dr Oliver Cooper & Linked documentation updated. Consent separated from accuracy, consent to send relating to insurance work added.	20.02.25

Contents

Section	Subject	Page
1	Legislation	3
2	Policy Statement	3
3	Your Data	3
i)	Lawfulness, Fairness and Transparency	3
ii)	Purpose Limitation	3
iii)	Data Minimisation	3
iv)	Accuracy	4
v)	Consent	4
vi)	Subject Access Requests	4
vii)	Storage Limitation <ul style="list-style-type: none"> • Health Surveillance • Medical Clinical Records 	4 5
viii)	Integrity and confidentiality (security)	5
ix)	Accountability	6
4	Data Complaint	6
5	Linked Documentation	6
6	Review and Authorisation	7
7	Quality Impact Assessment Employee	7

1. Legislation

The Data Protection Act 2018 controls how personal information is used by organisations, businesses, or the Government and is the UK's implementation of the General Data Protection Regulation (GDPR)

2. Policy Statement

Symbios Health understands the sensitivities surrounding personal medical data, as an Occupational Health Company we recognise our responsibility to treat data sensitively, fairly and in line with current legislation.

To be able to carry out the contractual business of supporting and meeting your Occupational or any other Health needs we need to collect and use certain types of personal information from our clients.

3. Your Data

All personal information is handled in accordance with the Data Protection Legislation and the seven key principles:

i) **Lawfulness, fairness, and transparency**

We have been selected by your company to help keep you healthy at work, as such we have a legitimate interest in certain data for the purposes of preventative or occupational health medicine.

Our main aim is to support you and help keep you fit, safe and healthy at work.

To do this we need to process your data.

Under the 'lawful purpose', we will collect the data necessary to undertake the business we have been contracted to undertake for our clients.

Data may be obtained from yourself or may come via a referral from your employer.

Our actions are transparent, our clinical evaluation fair and honest, all outcomes are shared with consenting parties.

ii) **Purpose limitation**

We will only use your data for the purposes of the business we have been contracted to undertake. Your data will be used to help us contact you, make appointments, keep you safe and healthy, highlight any areas where your employer needs to support you, make clinical decisions, and may be used to review insurance assessments, ill-health retirement or pension requests.

Your personal details will not be sold or traded to third parties.

iii) **Data minimisation**

We will only collect the data we require to complete the business we have agreed to undertake.

The data collected will vary depending on the assessment and the majority is obtained from you the employee giving you complete control. But please bear in mind we need to understand what's going on for you to help you in your workplace, we're being proactive to keep you healthy and can make suggestions for your GP.

We will need your name, date of birth, home address and either your work or home email address, we may ask about your general health, hazards, risks, or chemicals you may be exposed to. We may ask about your past medical history and lifestyle.

On occasion we may require specialist input or reports from your GP but we will only request information relating to your assessment or health and safety at work.

Following the assessments, we will hold your clinical reports and health surveillance results.

iv) **Accuracy**

The majority of data is obtained from you during your consultation and any examinations. There may be occasions when we require specialist input or reports from your GP and any data gathered externally will be cross referenced against the data provided by yourself to ensure we are talking to the correct person. All clinical reports are proofread prior to being sent and we undertake regular audits.

v) **Consent**

We will request your consent and offer you the chance to view the report before we share any outcomes unless we are required by law to share your data with the HSE/DVLA/UKHAS or any other relevant public body, or if your report has been requested by an insurance company.

Insurance Assessments

Assessments completed for Insurance Companies are handled differently and in line with the information commissioner's office (ICO). We are contracted by the insurance company to undertake an assessment on your employer's behalf meaning we are acting as data processors and not data controllers.

If your interaction with us is following a referral from an insurer, we will produce a report which is then sent straight to your insurer. By attending a consultation or assessment either in person or remotely, you are consenting to the consultation and for your report to be sent directly to the insurance company without you having any prior sight.

vi) **Subject Access Requests (SAR)**

Insurance assessments: In the event that you decide to put in a subject access request (SAR), we will exercise our rights for litigation privilege as defined by the information Commissioner's office (ICO) meaning we will not be able to provide additional information.

If your personal information is discussed or included in confidential communications between ourselves and the legal advisors (including in-house legal teams), we are not obliged to give it to you as part of your request. This information is considered 'privileged', which means it should remain confidential between us and the legal team.

We will however always collaborate with the insurer, and should the insurer ask for our permission or guidance to release our reports or similar then we will always advocate for a release and sharing of the data when we feel it is safe to do so.

Standard assessments: When a subject access request (SAR) is submitted, unless the data falls into the 'health data serious harm' category we will provide copies of all data held relating to the applicant.

Data will be reviewed by one of our physicians; we will withhold any data we believe has the potential to cause harm because we have a duty of confidentiality to the applicant and a duty to keep them safe from harm.

vii) **Storage limitation**

We will only keep your data for the duration of the contract when, for continuity of care, your information will be securely passed over to the next Occupational Health Provider who will continue to store your data.

While your records are in our care, we will comply with the required retention periods.

Should your employer cease trading we will hold your medical/clinical records for a further 6 years and in that time try and contact employees to offer them a copy of their health record.

We may also delete data upon request and/or after 6 years when a company informs us an employee has left and does not require their health and safety data to be stored or returned to them. However, there are exceptions to the right to be forgotten and in OH practice confidential records should as a general rule not be deleted at the request of a data subject because they fall within Article 9 (2)(h) of GDPR and also because they may be needed to defend the health professional or the employer if a claim is made, just as health professionals should not delete records which demonstrate that they are at fault.

The retention period for clinical/medical data is different to health surveillance:

Health Surveillance

- Under Health and Safety Law there is a requirement for employers to keep health surveillance records. The health Record must be kept for at least the period specified in the relevant regulations, for example 40 years under the Control of Substances Hazardous to Health Regulations (COSHH). Where regulations do not specify how long they should be kept for, the health record should be kept at least while you employ the worker. The COSHH substances currently monitored by Symbios Health include:

Antimony- The Control of Substances Hazardous to Health Regulations 2002

Arsenic - The Control of Substances Hazardous to Health Regulations 2002

Asbestos - Control of Asbestos Regulations 2012

Blood Lead Levels – Control of Lead at Work Regulations 2002

Isocyanates - The Control of Substances Hazardous to Health Regulations 2002

- General health surveillance – records are kept for the period of time the employee is employed by the company.

Medical/Clinical records

General medical and/or clinical records need to be retained for 6 years after the employee has left their employment. This is for the purpose of fulfilling professional obligations, ensuring continuity of care, meeting any legal or regulatory requirements and to meet professional obligations and medico-legal responsibilities.

viii) Integrity and confidentiality (security)

Data is encrypted and can only be accessed via layers of password protection on designated computers and/or held on a specific secure health programme purchased by us, ISO9001 registered and only accessed via the designated computers.

Paper records are held and stored securely by your employer.

Any temporary documentation generated during a clinic is shredded onsite using the company shredder.

Your data is kept confidential, we do not share any data without your consent unless there is a legal requirement. There may be occasions when we have to share data even if the employee has refused consent, for example where concerns are raised which apply to HSE/DVLA/UKHAS or any other relevant public body or if your role is considered a critical safety role or we believe your safety is at risk or you are a potential threat to others.

ix) **Accountability**

We take our responsibility for GDPR seriously, Dr Oliver Cooper is our designated data controller, and we are registered with the ICO.

Staff managing and handling personal information understand the importance of data protection and are appropriately trained, our nurses and surveillance staff are data processors, competency records are kept, and staff are appraised annually.

We foster a no blame culture where learning is paramount, and we have procedures in place should any data breaches occur.

Empowering Healthy Working

4. **Data Complaint**


UK GDPR gives you the right of access, should you have any concerns about how we store your data please contact our data controller, Dr Oliver Cooper Oli.Cooper@Symbios.Health and we will aim to answer any queries as soon as possible and within 1 month.



In the event we are unable to answer your queries you are advised to make a complaint to the Information Commissioners office (ICO).

5. Linked Documentation

STR517 GDPR Documentation Controller
 STR519 GDPR Data Plan
 STR520 Data Flow Mapping
 STR516 Legitimate Interest Assessment - IT
 STR515 GDPR Data Inventory Storage and Retention
 SOP259 GDPR Information and Guidance
 FOR365 Data Protection Agreement for SLA
 FOR366 Data Processing Agreement for SLA
 FOR370 Data Protection Agreement for Ad Hocs
 FOR371 Data Processing Agreement for Ad Hocs
 FOR402 GDPR Data Audit
 RA10 GDPR Data Breach - Risk assessment

6. Review and Authorisation

REVIEWED BY and ROLE	SIGNATURE	DATE
Dr Jonny Whittle Clinical Director		21.02.25

AUTHORISED BY	SIGNATURE	DATE
Dr Oliver Cooper		06.03.2025
Symbios Health Director		
Deborah Wassell		06.03.2025
Author - Head of Governance/ISO Lead		

7. Quality Impact Assessment/Employee

		Yes/No	Comments
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	Race	No	
	Ethnic origins (including gypsies and travellers)	No	
	Nationality	No	
	Gender	No	
	Culture	No	
	Religion or belief	No	
	Sexual orientation including lesbian, gay and bisexual people	No	
	Age	No	
	Disability - learning disabilities, physical disability, sensory impairment, and mental health problems	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	n/a	
4.	Is the impact of the policy/guidance likely to be negative?	No	
5.	If so, can the impact be avoided?	n/a	
6.	What alternatives are there to achieving the policy/guidance without the impact?	n/a	
7.	Can we reduce the impact by taking different action?	n/a	

Empowering Healthy Working