

## **Clients Privacy Notice**

Corazon Health Ltd, to be known as the Company from here on, serving as both the Data Controller and Data Processor, is committed to protecting the rights of the individual and acknowledge that any personal data of yours that we handle will be processed in accordance with the General Data Protection Regulations 2018 (GDPR) and the current data protection legislation. This notice applies to clients of the Company and their employees.

### **Data protection principles**

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way.
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you.
- only use it in the way that we have told you about.
- ensure it is correct and up to date.
- keep your data for only as long as we need it.
- process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed.

### **Types of data which may be collected:**

The following data maybe collected, held and stored by the Company, including:

- Personal information (e.g.name, address, date of birth, email address, phone numbers)
- Characteristics (e.g. gender, ethnicity - for health surveillance accuracy)
- Medical or health information including whether or not you have a disability
- National Insurance number
- Current and previous job titles, job descriptions, hours of work and other terms and conditions relating to your employment
- Documents provided to us by your employer (e.g. sickness absence leave records and any other documents relevant to the request for a service from your employer)
- Occupational health records
- Health surveillance records
- Relevant reports from other health practitioners e.g. General Practitioners and other treating specialists

### **Who we collect your data from:**

- Human Resources personnel
- Managers
- You
- Health & Safety personnel
- Occupational Health Practitioners (e.g. occupational health physicians, nurses & technicians)
- General Practitioners & treating hospital specialists
- Physiotherapists
- Other treating health specialists

**How we collect your data:**

- Information received via:
  - Email
  - Post
  - Online - OH software system (COHORT see below)
  - Online – specific service support applications or service feedback survey sites
  - Verbal (face to face and telephone)
- Completed health questionnaires
- Occupational health assessments and/or consultations

**How your data will be stored:**

We may hold your data either in a physical format or via electronic records. This will be compliant with all relevant data processing protocols and safeguards. The appropriate security measures and data protection policies are in place to safely store your data within the European Union.

**Why we process your data:**

- For the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services based on Union or Member State law or a contract with a health professional (Article 9 (h))
- To ensure the health and safety of the employees at work and to allow consideration of any adjustments that may be required to support their ability to work.
- Data may also be used for research, audit or statistics but will be pseudonymised if this is the case.

We also collect data so that we can carry out activities which are in the legitimate interests of the Company and use lawful basis, processing being necessary for the purposes of legitimate interests. We have set these out below:

- maintaining comprehensive up to date health records about you to ensure, amongst other things, effective correspondence can be achieved.
- offering a method of recourse for you against decisions made about you via our complaint's procedure.
- business planning
- dealing with legal claims made against us
- adhering to health surveillance retention periods

**Special categories of data:**

Special categories of data that we may control/process are data relating to your:

- health
- sex life
- sexual orientation
- race
- ethnic origin
- religion

We must process special categories of data in accordance with stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing.
- we must process the data in order to carry out our legal obligations.
- we must process data for reasons of substantial public interest.
- you have already made the data public.

We may use your special category data to provide occupational health advice to your employer.

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we will ask for your consent to allow us to process certain particularly sensitive data (to include health data) under recommendations made by our professional bodies; The General Medical Council and the Nursing and Midwifery Council. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent to send information to your employer and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

**Categories of personal data which may be obtained:**

We may process your data under one or more of the following services:

- New Starter Screening
- Management Referral
- Health Surveillance
- Well Being
- Vaccinations
- Drugs & Alcohol Screening

**Recipients of your data:**

Information pertaining to the above services will be shared with appropriate others as per your consent. All reports/certificates will be sent electronically, encrypted and password protected. Only in the event of a serious risk to life to you or others will confidentiality be breached.

**New Starter Screening:**

Your data is usually provided to us by Human Resources personnel or specialist recruitment teams. Following an occupational health assessment, we will provide the above with a certificate detailing your fitness for the role. Any specific health information about you will be agreed between you and the occupational health practitioner and will be subject to your explicit consent.

**Management referrals:**

Your data is usually provided to us by Human Resources, Health and Safety personnel or your line manager. Following an occupational health assessment, we will provide the above with a report/s, any specific health information about you will be agreed between you and the occupational health practitioner and will be subject to your explicit consent. As we are only the processor of the Management referral form received from your employer, we will not include this in any SARS requests.

**Health surveillance:**

Your data is usually provided to us by Human Resources or Health and Safety personnel or your line manager. Following any health surveillance, we will provide the above with the surveillance undertaken and the outcome of that surveillance. Any specific health information about you will be agreed between you and the occupational health practitioner and will be subject to your explicit consent.

**Well Being:**

The only data provided to us by Human Resources/Well Being/Health and Safety personnel or your line manager is your name. We will never provide feedback that might identify you individually but we will provide to the above anonymised data such as number of staff seen and generic outcomes such as number of people seen with high blood pressure.

**Vaccinations:**

Your data is usually provided to us by Human Resources, Health and Safety personnel or your line manager. Following any vaccinations, we will provide the above with a certificate detailing vaccinations carried out and the outcome of any related blood tests if appropriate. Any specific health information about you will be agreed between you and the occupational health practitioner and will be subject to your explicit consent.

**Drugs and alcohol screening:**

Your data is usually provided to us by Human Resources, Health and Safety personnel or your line manager. Following any drugs and alcohol screening we will provide the above with the outcome of the testing as per your consent unless it is a contractual obligation.

**Transfer of Data:**

Should we no longer be required to be your employer's occupational health provider you will be informed by your employer of the consent process regarding transferring the records held by the Company to another occupational health provider.

If our contract ends with your employer, we will stop processing your information and all personal data and health records will be transferred to your employer's next occupational health provider unless you withhold your consent.

**How long we keep your data for:**

The Retention period starts the date when.

- We have been informed an employee has left the employment of one of our clients (or an individual disassociates from a client)
- The client ceases to trade and no other provision is made for the records
- When a client is made "inactive" (18 months after last invoice)
- The client leaves and we have not been able to transfer records to a new occupational health provider.

We expect your employer to regularly update us with current employees and leavers. In line with data protection principles we will not hold data for which there is no provision to hold under the current data laws.

Where there is no transfer of records from a previous provider into Corazon Health, all data requests should go to the previous provider.

**Exceptions:**

Where it is not possible to tell whether the records are health surveillance records or any other form of occupational health records, or when we can't practically separate the type of record, the longer retention period will be applied.

Retention periods can vary depending on why we need your data, as set out below:

<b>Type of Data</b>	<b>Maximum Retention Period</b>	<b>Reason for Length of Period</b>
<b>New Starter Screening</b>	6 years + 1 after start of retention period as outlined on page 5 above or 75 years of age (whichever is longer)  Where informed by an employer that an individual did not take up the job offer or receive incomplete questionnaires data will be discarded at 2 years.  Where the data pertains to a trainee position and the individual leaves the organisation, the date of our retention period starts on the completion of the course.	As recommended by the British Medical Association (BMA)  Defence of legal claims
<b>Management Referrals and associated appointments</b>	6 years + 1 after start of retention period as outlined on page 5 above or 75 years of age (whichever is longer)	As recommended by the British Medical Association (BMA)  Defence of legal claims
<b>Health surveillance records and associated biological monitoring</b>	Dependant on specific guidance from the Health and Safety Executive	Health and Safety legislation and guidance  Defence of legal claims
<b>Wellbeing</b>	6 years + 1 after start of retention period as outlined on page 5 above or 75 years of age (whichever is longer)	As recommended by the British Medical Association (BMA)  Defence of legal claims
<b>Vaccinations and associated biological monitoring</b>	6 years + 1 after start of retention period as outlined on page 5 above or 75 years of age (whichever is longer)	As recommended by the British Medical Association (BMA)  Defence of legal claims
<b>Drugs and alcohol screening</b>	6 years + 1 after start of retention period as outlined on page 5 above or 75 years of age (whichever is longer)	Defence of legal claims

**If you do not provide your data to us:**

One of the reasons for processing your data is to provide your employer with information and to provide recommendations in order to provide an occupational health service to them; if you do not provide us with the data needed to do this, we will be unable to perform this service.

**Sharing your data:**

Your data will be shared with colleagues within the Company where it is necessary for them to undertake their duties. This includes, for example, Occupational Health Practitioners, Administrators linked to your case, finance personnel involved in the administering of invoicing your employer.

We share your data with third parties such as General Practitioners, Occupational Health Physicians and Nurses, with your consent, in order to further our advice to your employer.

We use sub processors to enable us to provide your employer and you with a full occupational health service for example our laboratories, partner services (e.g. physiotherapy, drugs and alcohol screening & counsellors).

We may also share your data with third parties as part of a company sale or restructure, or for other reasons to comply with a legal obligation upon us.

**Protecting your data:**

The information collected, held and used is in strict compliance with not only all current UK legislation but the confidentiality and ethical codes set out by the General Medical Council, Nursing and Midwifery Council (NMC) and the Faculty of Occupational Medicine (FOM). We are Cyber Essentials accredited.

We are fully aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction, and abuse. We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to relevant Company employees as above.

Where we share your data with third parties and sub processors, we provide written instructions to them to ensure that your data are held securely and in line with GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

All employees of the Company are subject to DBS checks where appropriate, annual data protection and GDPR training and subject to our Confidentiality and all Data Protection Policies.

**Automated decision making:**

The only decisions we may make about you based on automated decision making (where a decision is taken about you using an electronic system without human involvement) is in relation to:

- new starter screening via our on-line OH system portal - if you have answered no to all the health questions and have not exceeded an absence trigger, you may be automatically passed fit for role.

Please note that your data will not be used for profiling.

**Your rights in relation to your data:**

The law on data protection gives you certain rights in relation to the data we hold on you. These are the right:

- to be **informed**. This means that we must tell you how we use your data, and this is the purpose of this privacy notice.
- of **access**. You have the right to access the data that we hold on you. To do so, you should make a subject access request. You can read more about this in our Subject Access Request policy which is available from the Company Data Protection Officer (see below)
- for any **inaccuracies** to be **corrected**. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it.

- to have information **deleted**. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it.
- to **restrict** the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct.
- to **portability**. You may transfer the data that we hold on you for your own purposes.
- to **object** to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests.
- to regulate any **automated decision-making** and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent.

However, in some cases, we may continue to use the data where so permitted by having a legitimate or lawful basis for doing so.

If you wish to exercise any of the rights explained above please contact:

*Data Protection Officer  
Corazon Health Ltd  
5-6 The Mill  
Copley Hill Business Park  
Cambridge Road  
CB22 3GN*

Tel: 01223 83440

Email: [dpo@corazonhealth.co.uk](mailto:dpo@corazonhealth.co.uk)

**Making a complaint:**

Should you be unhappy with the response received from the Company Data Protection Officer you may make a request for an internal review by the Managing Director contactable at the address above.

The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO. <https://ico.org.uk/concerns/handling>

Please note that all Company policies and notices relating to data protection are reviewed annually.