EMPLOYEE PRIVACY NOTICE

Data Protection Officer
Name: The DPO Centre Limited
Email: dpo@ascenti.co.uk

In this Privacy Notice we use the terms "we", "us", and "our" (and other similar terms) to refer to the Ascenti Group who act as a data controller responsible for your personal data.

The Ascenti Group is Ascenti Physio Limited (Company Number 04530716) Ascenti Health Limited (Company Number 03225768) and Advo Health Limited (Company Number 15742346). all companies are incorporated in England & Wales. Our registered office is **Carnac House, Carnac Court, Cams Estate, Fareham, Hampshire, PO16 8UZ**.

Introduction

The Company collects and processes personal data relating to its employees to manage our employment relationship. The Company is committed to being transparent about how it collects and uses that data and to meeting data protection obligations.

Purpose

This Privacy Notice covers how Ascenti:

- **Collect**;
- **Use**;
- **Disclose**;
- **Transfer**; and,
- **Store** your data.

Collect

The Company collects and processes a range of information about you. This includes:

- your name, address (including 5 year history of addresses) and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, professional memberships, skills, experience and employment history, including start and end dates, with previous employers and with the Company;
- information about your remuneration, including details of benefits information such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants, GP details and emergency contacts;

- information about your nationality and entitlement to work in the UK;
- information about your credit history (for employees in certain roles);
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence and family leave, and the reasons for the leave;
- details of any capability, disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and scores, training you have participated in, performance improvement (capability) plans and related correspondence;
- information relating to your involvement in a complaint or incident;
- information about medical or health conditions, including whether or not you have a disability for which the Company needs to make reasonable adjustments such as specialist equipment provided to you;
- anonymised equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief;
- details of trade union membership; and
- any HR issues raised during your employment

The Company collects this information in a variety of ways. For example, data is collected through application forms, CVs, obtained from your passport or other identity documents such as your driving licence, from forms completed by you at the start of or during employment (such as benefit nomination forms), from correspondence with you, or through interviews, meetings or other assessments.

In some cases, the Company collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law.

Data is stored in a range of different places, including on your personnel file, in the Company's HR management systems and in other IT systems (including the Company's email system).

Use

The Company needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit and pension entitlements.

In some cases, the Company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave

to which they are entitled. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted / suitable to undertake the role in question.

In other cases, the Company has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the Company to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of capability, disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the Company complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- obtain required clearance from a commissioning organisation to work on a contract;
- provide references on request for current or former employees;
- respond to and defend against legal claims, complaints and incidents;
- maintain and promote equality in the workplace;
- provide you with access to our IT systems, networks, applications and hardware and monitor the use of those assets to ensure compliance with our Information Security and Data Protection policies and procedures.
- complete quality control and clinical audit and supervision processes including for continuous professional development.
- your name, professional title and location may be publicised externally to allow patients to book appointments online, we would make you aware that we were doing this.

Where the Company relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions and professional / trade memberships is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

In certain circumstances there may be the requirement to process your personal and special category data with the requirement of your consent. You will be informed of the nature of that processing, the purpose, and your right to withdraw your consent. If you have given consent, you can change your mind by contacting the peopleteam@ascenti.co.uk.

Criminal Record Check

The Company may carry out processing of criminal data where it is necessary for the purposes of performing or exercising employment law obligations or rights.

The Company has an appropriate policy in place to ensure that we balance a person's right to privacy with our legal requirements and the safety of our service users and details which roles require basic and enhanced criminal record checks.

This policy covers the Company's procedures for securing compliance with the principles of data processing and explains the Company's policies as regards to the retention and erasure of this data.

Equal Opportunities Monitoring

Where the Company processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring.

- Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

- An employee can require the employer to stop processing this data for this purpose by giving the employer written notice.

The Company will ensure that it has the appropriate policy, setting out the safeguards it has implemented for processing this data and how long this data will be retained.

Photographs and Videos

The company may, from time to time, photograph or take video recordings of company events or employees for promotional material, use on company social media sites or use on our website and newsfeed. You will be given advance warning of any photographs or videos being taken for these purposes and provided with the opportunity to opt-out should you not wish to appear in any such material. This will be communicated to the photographer or videographer at the time of recording. If you do not opt-out in advance you can do so by informing the photographer or videographer at the time of recording.

Disclose

Your information will be shared internally, including with members of the People Team (including Payroll), your line manager, managers in the business area in which you work, directors and IT staff if access to the data is necessary for performance of their roles. Your line manager will be given access to the HR system to access data relevant to their management of your role (e.g. monitor sickness records, managing annual leave).

For roles requiring clearances and approval by the organisation commissioning our services, information relating to employment and relevant checks will be shared to in order for the employee to be approved to work on those contracts (e.g. the Health Advisory and Assessment Service).

Medical information may also be shared internally where deemed appropriate, which could include to make reasonable adjustments for equality purposes, where we have a legal obligation to take action, or where necessary to share information for your safety, and the safety of patients. For example, our People Team may need to transfer Occupational Health information to our Governance Team in order to meet our reporting and safeguarding obligations.

The Company shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. The Company may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The Company also shares your data with third parties that process data on its behalf. These organisations include:

Pension Providers & Brokers
Employee Assistance Service Providers
Employee Benefits Programmes
Occupational Health Services
Healthcare Providers
Training Providers
Financial Wellbeing Platforms
Insurance Providers
Legal advisors
Employment Screening Services
Providers of Employee Platforms
HMRC and other statutory bodies

We will share your data with carefully selected third parties when:

- You specifically request it, or a disclosure is required in order for us to provide our services and/or fulfil our contractual obligations to you;

- We are under a legal or regulatory duty to disclose your information.

Your data may be shared with public agencies or other statutory bodies / entities where there is a legal requirement for us to do so.

Your data may be transferred to countries outside the United Kingdom (UK) or European Economic Area (EEA) to respond to an employment reference request only on the basis that this is necessary for the performance of a contract between the individual and the Company or for pre-contractual steps taken at the individual's request. Such transfers will be done in accordance with Company Policies and procedures.

The Company will otherwise not transfer your data to countries outside the EEA.

In limited circumstances, the third parties that we engage with may be required to transfer minimal personal information out of the UK or EEA to countries not deemed by the ICO (and/or European Commission as relevant) to provide an adequate level of personal information protection. In such circumstances, the transfer will be based on safeguards that allow the transfer to be conducted in accordance with data protection legislation, such as the specific contracts approved by the ICO (and/or European Commission as relevant) and robust technical organisational measures to protect your data.

Advo Health Employees only

If you are employed by Advo Health and you undertake a role relating to the Health Advisory and Assessment Service, your data will be shared with the Prime Provider under which those services operate (e.g. Serco or Ingeus) and the DWP who commission those services. The following Advo Health Employee data is shared with the Prime Providers:

- Person/ Employee ID
- Full Name & Preferred Name, Home Address, Gender, Advo email and personal email address
- Job Role, PRN/NMC/GMC Number, Clinical Occupation
- Salary Information/ Payslips

Start Date, Hours worked, Working Pattern, Leave Date, Absence Data This data is shared with the Prime Providers for the purposes of the provision of and access to IT networks, systems, applications and equipment by the Prime Providers, and with the DWP for the provision of training on those systems, for rota planning, audit and safeguarding reporting purposes. Where this is the case, it is shared under the Contract Lawful Basis.

Data is also shared with the Prime Providers for the purposes of the audit of costs and monitoring the use of IT. Where this is the case it is done so under the Legitimate Interest Lawful basis, as it is in Advo Health's Legitimate Interest to ensure that our employees are abiding by the relevant information security policies and ensure the safe and secure functioning of all IT systems, networks

applications and hardware used by Advo Health employees in connection with their role and to claim back costs where appropriate from the Prime Providers.

And for assessors only

Details of your professional qualifications, training, appraisals, indemnity insurance cover.

Details of any referrals to professional regulatory bodies, the outcome and any sanctions or clinical approval revocation made by those regulatory bodies.

We have a Legal Obligation to share this data with the Prime Providers for the purposes of Clinical Governance. This is because assessors who assess claims for Personal Independence Payments and Work Capacity Assessments on behalf of the DWP must adhere to the Welfare Reform Act 2007, Equality Act 2010, Special Security (Medical Evidence) Regulations 1998 and the Health and Social Care Act 2012, and we need to provide evidence of compliance.

How does the Company protect data?

The Company takes the security of your data seriously. The Company has internal policies and controls in place to try to ensure that your data is secure, and is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. The HR system is ring fenced with tiered levels of access, ensuring only relevant data is accessed by People Team staff and specific staff that have access to the system and limited IT staff (who sign additional confidentiality forms before access is granted). Multifactor authentication is used to access HR systems. People Team/Payroll documents containing sensitive personal data are password protected when they are emailed out. Payslips are accessed by staff online and in the event payslips are required to be sent by post, only a Manager on the authorised payslip distribution list will be given sealed employee payslips for their department.

Where the Company engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Store

Data is stored in a range of different places, including on your personnel file, in the Company's HR management systems and in other IT systems (including the Company's email system).

The Company will hold your personal data for the duration of your employment. After the end of employment your data is deleted after seven years from your leave date.

For those recruitment applicants who are not successful in progressing to interview stage, the Company will delete applicant data six months after the date of the application. For applicants who are offered a role but do not start with the Company, the Company will delete data six months after the date of interview.

In the event of a complaint, incident or a legal claim, data will be securely held within our Risk Management Systems and managed in accordance with the data protection legislation.

Your rights

As a data subject, you have a number of rights. You can:

- ask for a copy of your information;
- ask for information to be corrected;
- ask for information to be erased or deleted;
- ask for us to limit or restrict processing;
- object to us processing your data, in particular where we use the data for direct marketing, including profiling for direct marketing purposes. The right to object does not apply if we must process the data to meet a contractual or legal requirement;
- ask us to send you a copy in a structured digital format or ask for us to send it to another party.

Some rights however, may be limited. We may be obliged by law or regulation to keep information. On occasion there may be compelling legitimate interests to keep processing your data.

If you want a copy of your data, to object to how we use your data, or ask us to delete or restrict how we use it, please send your request to dpo@ascenti.co.uk.

Automated decision-making

None of the Company's employment decisions are based solely on automated decision-making.

Profiling

None of the Company's employment decisions are based on profiling.

Call recording

Calls via our phone systems may be recorded. This is to ensure ongoing training and monitoring. Call recordings will be kept for a period of one calendar month from the date of the call. If you need to make a personal call, to the People Team for example, this should be discussed with your line manager in the first instance as recording may be disabled or a private location with non-recorded calls may be made available.

Further information

If you wish to raise a query on how we have handled your personal data you can contact our Data Protection Officer at dpo@ascenti.co.uk

You have the right to raise a concern at any time to the Information Commissioner's Office ("ICO") who is the UK supervisory authority for data protection issues. For more information on submitting a concern, or the data protection regime in general, please visit the ICO's website.

References:
Data protection and Confidentiality Policy
P103 Data Lifecycle Management