

Pure Healthcare Group Limited

Privacy Notice for Agency Workers



PRIVACY NOTICE FOR CONTRACTORS

Pure Healthcare Group Limited, a company registered in England and Wales under registration no. 12401287
Registered Office: 214 Grangewood House, 43 Oakwood Hill, Loughton, IG10 3TZ
VAT Registration No. 343 0516 34

In accordance with the General Data Protection Regulation (GDPR), Pure Healthcare Group of 30 crown Place, London EC2A 4EB has implemented this privacy notice to inform you of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

A) DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- a) processing is fair, lawful and transparent
- b) data is collected for specific, explicit, and legitimate purposes
- c) data collected is adequate, relevant and limited to what is necessary for the purposes of processing
- d) data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- e) data is not kept for longer than is necessary for its given purpose
- f) data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- g) we comply with the relevant GDPR procedures for international transferring of personal data

B) TYPES OF DATA HELD

Personal data is any information about an individual from which that person can be identified. It does not include anonymous data which does not identify the individual.

We collect, store and use several categories of personal data about you in order to carry out effective and efficient processes. We keep this data in a file relating to each contractor and we also hold the data within our computer systems, for example, our accounts systems. It is your responsibility to keep us up to date with any changes to your personal details so that we can make sure that your personal data is accurate. If your personal details change, you must notify our Governance, Risk & Compliance Manager, Katie Rowland.

Specifically, we collect, store and use the following types of data:

- a) personal details such as name, previous names, title, address, phone numbers, email address, date of birth
- b) your photograph
- c) your gender
- d) marital status
- e) bank account details
- f) payment rates
- g) contract of employment
- h) payslips
- i) Employment history & references
- j) Right to Work and ID documentation
- k) Professional Registration & Qualifications
- l) Immunisations and occupational health clearance

- m) Mandatory training
- n) ID cards

C) COLLECTING YOUR DATA

You provide several pieces of data to us directly during any contract negotiation period, for example your name and address, and subsequently upon the start of your engagement, for example, your bank details.

In some cases, we will collect data about you from third parties, such as intermediaries who may act as an introducer.

Personal data is kept in files or within the Company's HR and IT systems.

D) LAWFUL BASIS FOR PROCESSING

The law on data protection allows us to process your data for certain reasons only. In the main, we process your data in order to comply with a legal requirement, in order to perform the contract we have with you or in pursuit of our legitimate interests.

The information below categorises the types of data processing we undertake and the lawful basis we rely on.

Activity requiring your data	Lawful basis
Carry out the contract that we have entered into with you e.g. using your name, contact details	Performance of the contract
Ensuring you receive payment	Performance of the contract
Making decisions about who to enter into a contract with	Our legitimate interests are to assess the suitability, qualifications, experience and compliance status of candidates and workers to ensure we engage appropriately qualified individuals and meet client and regulatory requirements.
Business planning and restructuring exercises	Our legitimate interests are to manage, develop and improve our business operations, workforce planning, organisational structure and service delivery to ensure the continued success and sustainability of the business.
Dealing with legal claims made against us	Our legitimate interests and legal obligations are to establish, exercise or defend legal claims, protect our legal rights and interests, and manage disputes effectively including but not limited to Regulatory Body referrals
Preventing fraud	Our legitimate interests and legal obligations are to protect the business, our clients, workers and candidates from fraudulent activity, financial crime, identity theft and other unlawful conduct.

Ensuring our administrative and IT systems are secure and robust against unauthorised access	Our legitimate interests are to maintain the security, integrity and availability of our systems, data and services, protect confidential information and prevent cyber security incidents.
Monitoring and improving our services	Our legitimate interests are to review and improve the quality, efficiency and effectiveness of our services and customer experience.
Maintaining business records and management reporting	Our legitimate interests are to manage our business effectively, monitor performance and meet corporate governance requirements.
Communicating with clients, candidates and workers regarding services and opportunities	Our legitimate interests are to operate and develop our recruitment services and maintain effective business relationships.
Maintaining NHS framework status and compliance with NHS workforce requirements	Our legal obligations are to comply with applicable healthcare, employment and regulatory requirements, including NHS framework standards and audit requirements. Our legitimate interests are to maintain our NHS framework status, demonstrate compliance with contractual and regulatory obligations, and continue providing healthcare staffing services to NHS organisations. To achieve this, we may present evidence of pre-employment checks, ongoing compliance monitoring and employment records to authorised NHS framework auditors and accreditation bodies.

E) SPECIAL CATEGORIES OF DATA

Special categories of data are data relating to your:

- a) health
- b) sex life
- c) sexual orientation
- d) race
- e) ethnic origin
- f) political opinion
- g) religion
- h) trade union membership
- i) genetic and biometric data.

Most commonly, we will process special categories of data when the following applies:

- a) you have given explicit consent to the processing
- b) we must process the data in order to carry out our legal obligations

- c) we must process data for reasons of substantial public interest
- d) you have already made the data public.

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations. However, we may ask for your consent to allow us to process certain particularly sensitive data. 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 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.

F) FAILURE TO PROVIDE DATA

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract with you or performing the contract that we have entered into.

G) CRIMINAL CONVICTION DATA

We will only collect criminal conviction data where it is appropriate given the nature of the services you are to provide to us and where the law permits us. This data will usually be collected during contract negotiation, however, may also be collected during your engagement. We use criminal conviction data to determine your suitability, or your continued suitability for the engagement. We rely on the lawful basis of We rely on the lawful basis of **legal obligation** to process this data in order to comply with our legal, safeguarding and regulatory obligations and to determine your suitability for work within healthcare settings to process this data.

H) WHO WE SHARE YOUR DATA WITH

Employees within our company who have responsibility for recruitment, administration of payment and contractual benefits and the carrying out of performance related procedures will have access to your data which is relevant to their function. All employees with such responsibility have been trained in ensuring data is processed in line with GDPR.

Data is shared with third parties for the following reasons:

- To obtain employment referencing
- To conduct Criminal Record Checks with Disclosure & Barring Service (DBS), Access NI, and Protection of Vulnerable Groups (PVG)
- To verify Identity and Right to Work (TrustID & Home Office)
- To obtain occupational health clearance (Healthier Business)
- To book and verify mandatory training (providers are dependent on the training completed/booked)
- To present your file to a prospective client by completing a checklist or uploading requested documents
- To complete a NHS Framework Audit through an external auditor
- To process your payment and administration of payroll (Integra Back Office Solutions)
- To assess experience, skills and knowledge through clinical interview (in house or through Healthier Business)

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.

We have a data processing agreement in place with such third parties to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

We do not share your data with bodies outside of the European Economic Area.

I) PROTECTING YOUR DATA

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

J) RETENTION PERIODS

We only keep your data for as long as we need it for, which will be at least for the duration of your engagement with us, though in some cases we will keep your data for a period after your engagement has ended. Our retention periods are determined in accordance with legal, regulatory, contractual and business requirements. In most cases, personal data relating to workers and employees will be retained for up to 6 years following the end of the engagement, unless a longer retention period is required by law, regulatory requirements, ongoing legal proceedings or NHS framework obligations.

K) AUTOMATED DECISION MAKING

Automated decision making means making decisions about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

L) DATA SUBJECT RIGHTS

You have the following rights in relation to the personal data we hold on you:

- a) the right to be informed about the data we hold on you and what we do with it
- b) the right of access to the data we hold on you. More information on this can be found in our separate policy on Subject Access Requests
- c) the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification'
- d) the right to have data deleted in certain circumstances. This is also known as 'erasure'
- e) the right to restrict the processing of the data
- f) the right to transfer the data we hold on you to another party. This is also known as 'portability'
- g) the right to object to the inclusion of any information
- h) the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our separate policy on your rights in relation to your data.

M) CONSENT

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

N) MAKING A COMPLAINT

If you consider your data rights have been breached, you can make a complaint to us at any time using any of the following methods:

- Email: complaints@purehealthcare.co.uk
- Post: Pure Healthcare Group, 30 Crown Place, London EC2A 4EB
- Telephone: 02071399999

More information is available in our separate policy on our complaints procedure:



PHGCP -
Complaints Procedure

You can also raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

O) DATA PROTECTION COMPLIANCE

Our Data Protection Officer is:

Peter Newbury
02071399999
Peter.Newbury@purehealthcare.co.uk

Our appointed Governance, Risk & Compliance Manager in respect of our data handling activities is:

Katie Rowland
02071399999
Katie.Rowland@purehealthcare.co.uk