Employee Privacy Notice

At Mountain Healthcare (MH) we are aware of our obligations under the UK General Data Protection Regulation (UK GDPR) and are committed to processing your data securely and transparently. This privacy notice outlines, in accordance with UK GDPR, the types of data we hold about you as an employee of MH, why we do so, how we use and share that information, how long we retain it, what rights you have and other relevant details regarding your data.

This notice applies to job applicants, prospective, current and former employees.

Data controller details

Mountain Healthcare Limited is a data controller, meaning that it determines the processes for handling your personal data where you are employed by Mountain Healthcare. Our contact details are as follows:

Mountain Healthcare Limited
First Floor, Station Place
Argyle Way
Stevenage
England
SG1 2AD

Tel: 0330 223 0099

We are registered with the ICO, and our registration number is: Z9725343.

Data Protection Queries

Please contact Governance via governance@mountainhealthcare.co.uk for any concerns or queries in relation to our processing of your data or this privacy notice.

Data Protection Officer

Our Data Protection Officer is Tania Palmariellodiviney. Our Data Protection Officer team can be contacted via email RCI-DPO@Rcigroup.co.uk.

Data protection principles

We are committed to adhering to the following data protection principles in relation to your personal data:

Lawfulness, Fairness, and Transparency

We process personal data lawfully, fairly, and in a transparent manner.

We ensure that employees are informed about the purpose and legal basis for processing their data. Clear communication is provided through privacy notices and policies.

Purpose Limitation

We collect personal data only for specified, explicit, and legitimate purposes and do not process it further in a manner that is incompatible with those purposes.
Personal data is collected strictly for purposes related to your employment and any additional uses are clearly communicated to you.

Data Minimisation

We ensure that personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
Only the minimum amount of personal data required for specific purposes is collected and processed.

Accuracy

We take reasonable steps to ensure personal data is accurate and, where necessary, kept up to date.
Regular reviews and updates are conducted to ensure the accuracy of employee data. Employees are encouraged to report any changes to their personal data.

Storage Limitation

We keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
Personal data is retained only for as long as necessary and in accordance with our data retention policy. Data no longer required is securely deleted.

Integrity and Confidentiality

We process personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
Robust security measures, including encryption and access controls, are implemented to protect personal data. Regular training is provided to employees on data protection and security.

Accountability

We are responsible for and able to demonstrate compliance with the above principles.
We maintain records of our data processing activities and regularly review our data protection practices ensuring compliance. Data protection impact assessments (DPIAs) are conducted where necessary.

Types of data we process

We hold two types of data for you:

1. **Personal data** – data about you that you can be identified with, i.e., your name, contact details, national insurance number, date of birth, bank details, etc. basically any personal data that relates to you and that can be used to identify you.

2. **Personal special category data** – this is also your personal data but includes more sensitive information about you. This type of data requires a higher level of protection. Special category data is information about your:

    - race;
    - ethnic origin;
    - political opinions;
    - religious or philosophical beliefs;
    - trade union membership;
    - genetic data;
    - biometric data (where this is used for identification purposes);
    - health data;
    - sex life; or
    - sexual orientation.

Personal data can include information relating to criminal convictions and offences. This also requires a higher level of protection.

How we collect your data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment exercise, where we will collect the data from you directly or a third party in form of a recruitment agency or job advertising platform. This includes the information you would normally include in a CV and a cover letter and/or notes made by our recruiting officers during a recruitment interview.

Further information will be collected directly from you when you complete forms at the start of your employment, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies as well as the Disclosure and Barring Service DBS.

Sources of Employee Data (Indirect Collection)

In some cases, employee data may be obtained from sources other than the employee directly. These sources include:

1. **HR and Payroll Systems** – Information such as employment history, salary details, benefits, and performance records may be generated and maintained within HR and payroll software.

2. **Line Managers and Supervisors** – Feedback, performance appraisals, absence records, and disciplinary actions may be recorded by an employee's line manager or other supervisors.
3. **IT and Security Systems** – Data such as login records, access control logs, and email monitoring may be collected for cybersecurity, compliance, or operational purposes.
4. **Third-Party Service Providers** – External providers such as occupational health services, background check companies, training providers, or benefits administrators may supply data relating to medical assessments, DBS checks, professional qualifications, or pension schemes.
5. **Colleagues and Other Employees** – Data about an employee may be collected through peer feedback, whistleblowing reports, or grievance procedures.
6. **Regulatory Bodies and Government Agencies** – Authorities such as HMRC, the Home Office, or regulatory bodies may provide data for tax, immigration status, professional licensing, or compliance purposes.
7. **Publicly Available Sources** – In some cases, information may be gathered from public sources such as LinkedIn, professional registers, or published articles where relevant to employment or regulatory requirements.

Storage and Access

Your personal data is kept on a secure cloud environment at our head office.

We implement robust security measures to protect your personal data. Only authorised personnel who require access to your files to perform their job duties have access to this information. Access is strictly controlled and monitored to ensure your data is handled with the highest level of security and confidentiality.

Why we process your data

We primarily process data to fulfil our legal obligations as an employer and to support your employment with us. **Please note that not all processing activities require your consent.** In fact, for employment purposes, consent as a legal basis is rarely necessary and is only appropriate in specific circumstances where the processing is not essential as part of your contract.

However, we will be transparent and honest about our processing activities with you at the time of processing so that you can decide whether you wish to go ahead with your application and/or employment.

Some of the details we collect and process about you may be used for different but related purposes, as long as they are compatible with the original purpose. For example, if you provide us with your name and contact details during your application, we can also use this information for purposes related to your employment.

Below, we have provided a table detailing the information we collect and process, along with the purpose and legal basis under UK GDPR Article 6. For special category data, we have also included an additional condition under UK GDPR Article 9.

Do bear in mind that consent for a specific action is different to consent for processing activities. For example, if you give your consent to be referred to occupational health, we do not rely on your consent for the data being processed as part of the referral.

Processing of Personal Data and DNA Collection

Depending on your role, certain aspects of data processing may feel intrusive. For example, if your position requires it, we may need to collect your DNA. We follow strict management protocols and conduct this processing in full compliance with legal requirements. If you have any concerns, we encourage you to speak with us, and we will do our best to address them and provide reassurance.

Information we process	Purpose for processing	Legal Basis for processing under article 6 GDPR	Additional condition for processing special category data under Article 9 GDPR
Name	Identification and communication	Contract	N/A
Contact details (address, phone number, email)	Communication	Contract	N/A
Date of birth	Age verification and eligibility for employment	Legal Obligation	N/A
National Insurance number	Tax and social security purposes	Legal Obligation	N/A
Employment history	Assessing suitability for the position	Contract	N/A
Education and qualifications	Verifying skills and qualifications	Contract	N/A
References	Background checks and verifying previous employment	Contract	N/A
CV or resume	Assessing suitability for the position	Contract	N/A
Application form details	Assessing suitability for the position	Contract	N/A
Interview notes	Assessing suitability for the position	Contract	N/A
Proof of identity (e.g., passport, driving licence)	Identity verification and right to work compliance	Legal Obligation	N/A

Proof of address	Identity verification and correspondence	Contract	N/A
Criminal record check (if applicable)	Assessing suitability for certain roles, compliance with legal obligations	Legal Obligation	Substantial Public Interest
Bank account details	Salary payment processing	Contract	N/A
Emergency contact information	Emergency contact in case of an emergency	Legitimate Interest	N/A
Health information (e.g., medical history, disability status)	Ensuring workplace adjustments and compliance with health and safety regulations	Contract	Legal Obligation
Photograph	Identification and security	Legal Obligation	N/A
Payroll information	Salary processing and benefits administration	Contract	N/A
Performance records	Performance management and professional development	Contract	N/A
Training records	Tracking and managing employee development	Contract	N/A
Attendance records	Managing leave, absences, and timekeeping	Contract	N/A
Disciplinary and grievance records	Managing employee relations and compliance with legal obligations	Contract	Legal Obligation
Contract details	Establishing the terms of employment and contract management	Contract	N/A
Work permits or visas	Verifying right to work and compliance with immigration laws	Legal Obligation	N/A
DNA (Job role dependant)	To comply with our legal obligation to the Forensic Science Regulator Act 2021. Staff DNA must be on an elimination database(s) in line with the Forensic Science Regulators Code of Practice.	Legal Obligation	Substantial Public Interest

Criminal conviction data

We conduct DBS checks for everyone as part of our commitment to ensuring the highest levels of safety and trust. Given the sensitive nature of the services we provide, it is crucial that all staff, regardless of their specific role, meet our rigorous standards. Collecting criminal conviction data allows us to make informed decisions about the suitability of all individuals who join our team, ensuring that they align with our safeguarding policies and the expectations of our staff, patients, clients and regulatory bodies. This approach is essential

not only for compliance but also for maintaining the integrity and security of our care environment.

If you do not provide your data to us

We need to process your data to fulfil our duties under your employment contract or potential employment. If you don't provide the necessary data, we won't be able to perform these duties, which might affect our ability to offer you a job or consider you for employment.

Additionally, if you don't update us with essential information, like your right to work in the UK or the results of a required criminal records check, we may not be able to continue your employment.

If you have any concerns in relation to giving us any of the requested information, please feel free to contact us to discuss them.

Sharing your data

Some of your data may be shared within MH, and our parent organisation, RCI Group Limited, where it is necessary for them to undertake their duties. We ensure that this sharing is done on a strict need-to-know basis and only when appropriate sharing agreements are in place to protect your information.

This includes, for example:

- Sharing information with your line manager for their management of you.
- The HR department for maintaining personnel records.
- The payroll department for administering payment under your contract of employment.
- Our parent organisation, RCI Group Limited, for the purpose of consolidating reporting and improving operational efficiencies, or where we are using their services for compliance and auditing functions.
- Subsidiaries of the RCI group for purposes outlined in intergroup sharing agreements. For example, some departments of some subsidiaries support each other in departments like HR and Finance. In any case this is on a need-to-know basis, strictly access controlled and only for purposes outlines within the sharing agreements.

This may also include sharing data with third parties:

- HMRC, because they require access to certain financial and personal details for tax and national insurance purposes.
- The Disclosure and Barring Service (DBS), because they need to verify whether individuals are eligible to work in positions that require a clear criminal record, especially in roles involving vulnerable groups.
- Occupational Health providers, because they need to assess your suitability for the role or manage any health-related adjustments in the workplace.

- Relevant Police Forces, because staff DNA profiles may be identified on processed evidence (crime stains) or where appropriate, significant Environmental Monitoring contamination. This is to help identify and investigate genuine contamination events to ensure the integrity of the forensic evidence is preserved, that investigations are not misled by unidentified contamination, resource is not wasted during an investigation and cases are not delayed from reaching a judicial conclusion through the courts.
- Forensic Information Database Service (FINDS) as they manage and maintain the Contamination Elimination Database (CED)
- Cellmark as they are our chosen Forensic Service Provider (FSP) who will manage and process DNA data for MH's Staff Elimination Database (SED), they also process data on behalf of FINDs for the CED.
- Other SARC providers if an employee transfers to another SARC provider from MH and their CED DNA profile transfers over to the new provider. This is to ensure investigations into contamination issues can continue effectively.
- All data sharing is conducted safely and in accordance with legal requirements, ensuring your information remains secure and confidential.
- Our Data Protection Officer to give us necessary and appropriate data protection advice

Suppliers of services and systems may also have access to some of your information. This access is limited to what is absolutely necessary but crucial for operational tasks such as processing your payments through software or managing company benefits provided by suppliers for example. It is essential to ensure the efficient execution of employment-related processes, while rigorously maintaining data security and legal compliance.

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.

Where we share your data with third parties, we provide written instructions and have necessary agreements in place, and/or ask for evidence of their assurances, to ensure that your data are held securely and in line with UK GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

Access to your information is governed by stringent data processing and sharing agreements as well as information security checks.

How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it for, which will be at least for the duration of your employment with us though in most cases we will keep your data for a period after your employment has ended. In any case we follow as a minimum, statutory retention periods and/or have documented justification based on necessity for retention of your records.

Please contact us if you wish to obtain a copy of our retention schedule.

Automated decision making

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.

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.
- the right 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 your manager.
- the right 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
- the right 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.
- the right 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.
- the right to portability. You may transfer the data that we hold on you for your own purposes.
- the right 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.
- the right 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.

Consent

In any case where we asked for your consent to use your data, you have the 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 and you can withdraw it by contacting HR. The right to withdraw consent does not apply in cases where we did not rely on consent as a legal basis so even if you wish to object to processing of your data, we may not always be able to do so.

Not all rights are absolute, and exemptions may apply. You can find out more about this here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/ .

If you wish to exercise any of your rights under UK GDPR, please contact HR.

Transfers of Personal Data Explained

Sometimes, we need to use systems, software, or suppliers that are located outside the UK. This means that your personal data might be transferred to other countries. We only do this when it's necessary, and we make sure your data is protected by similar safeguards as those in the UK.

Here's a clearer breakdown:

Why transfer data?

We use top-notch software and services that might be based outside the UK, because they may be able to provide a product that is unavailable by a UK supplier. This ensures we have the best tools to do our jobs efficiently and securely.

Where does the data go?

Your data may be transferred to countries that either:

- Have been given an adequacy status by the UK. This means they have data protection laws that are similar to those in the UK.
- Have similar safeguards in place. These safeguards ensure that your data remains as protected as it would be in the UK.
- What does 'adequacy' mean?
- Adequacy status is granted to countries whose data protection laws are strong enough to protect your data to a similar standard as the UK.

What are similar safeguards?

These could include:

- Contracts that oblige the recipient to protect your data.
- Privacy Shield frameworks or similar agreements that ensure data protection.

Is this common?

- Yes, transferring data internationally is a standard practice in today's digital world. Many companies do it to use the latest and most effective technologies available.

In essence, while your data might be sent to other countries, we always ensure it is handled with the highest level of security and care, just as it would be here in the UK.

If you would like more information about the systems or suppliers that we use, that may mean transferring your data out of the UK, please get in touch, we are happy to answer your questions.

Making a complaint

We'd always ask you to let us know if you are unhappy with our processing activities in relation to your data, however you also have the right to complain to the ICO at any point. They are the supervisory authority in the UK for data protection matters.

Their contact details are as follows:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Contact Number: 0330 223 0099

This Privacy Notice was updated on 15th July 2024 and will be reviewed annually and as and when our processing activities change or any changes in data protection legislation require it.