Privacy Notice

Rinicare Privacy Notice

Updated 19 JULY 2022

We take the security and privacy of your data seriously and intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security.

We have 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.

This privacy notice applies to current and former employees, workers, volunteers, apprentices, consultants and customers of Rinicare. It does not form part of any contract, and we may make changes at any time.

1. 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

2. Types of Data Held

a. For Rinicare-held data

We may hold personal data to carry out effective and efficient processes. We keep this data within our computer systems. Specifically, we may hold the following types of data:

a) recruitment information such as your application form, CV, references, and qualifications
b) personal details such as name, address, phone numbers
c) your emergency contact details

d) your image, whether captured by CCTV, photograph, or video
e) your gender
f) marital status and family details
g) bank account details
h) payment rates and other details held in your contract of employment (or contract for services)
i) your identification documents including passport and driving license and information in relation to your immigration status and right to work for us
j) Information relating to disciplinary or grievance investigations and proceedings involving you (whether you were the main subject of those proceedings)
k) Information related to your performance and behaviour at work
l) Training records
m) Any other category of personal data that we may notify you of from time to time

b. Regarding software held by Rinicare-provided software hosted by organisations:

n) Rinicare does not host or process the data from any Rinicare-provided systems without express permission or knowledge of its users. For third-party organisation-hosted software, their own privacy policy applies.

3. 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.

a. All personal data is kept in physical files, or within the Company's HR and IT systems and backups.
b. Any clinical data held by Rinicare-provided software is held in digital form in a system wholly self-contained (sandboxed) and fully managed by the organisation using the software, in which case our privacy's remit stops, and that organisation's privacy policy applies (see section 18 - "Scope")

4. Lawful Basis for Processing

a. For Rinicare-held data

The law on data protection allows us to process your data for certain reasons only. We only process your data to comply with legal requirements, to fulfill our contract obligations 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.

Privacy Notice

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
Business planning and restructuring exercises	Our legitimate interests
Dealing with legal claims made against us	Our legitimate interests
Preventing fraud	Our legitimate interests
Ensuring our administrative and IT systems are secure and robust against unauthorised access	Our legitimate interests

b. Software held by Rinicare-provided software hosted by organisations

Rinicare's deployed software only holds the data required to perform its advertised functions, following data minimisation principles.

No further data is being collected without a legitimate interest in the stated *Intended Purpose* for the clinical software – a summary is always available at https://rinicare.com/regulatory/.

No data is ever collected or shared with third parties without your express knowledge and consent.

5. Special Categories of Data

For Rinicare-held data (such as employee or contractor), we will process special categories of data relating to:

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.

6. Failure to provide data

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

7. 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 (see section 4) to process this data.

8. 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 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 processing in line with GDPR.

We do not share, and actively prohibit, the transfer, trading, or disclosure of data with third parties. The only exception to this is 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 in such event, to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of such data.

9. Protecting Your data

c. 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.
d. Rinicare manage all data is a secure manner with up-to-date standards; this includes both Rinicare's internal system as well as Rinicare-provided clinical software deployed on any platform.

e. Data is always stored and transmitted in an encrypted form; our security policy is available upon request from our Data Protection Officer (see section 16 below) and www.rinicare.com/regulatory

10. Retention Periods and Data Destruction

a. 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 period is 6 years.
b. Organisations making use of Rinicare-deployed clinical software can manage their own retention period; please refer to their their own privacy policy.
c. Where applicable, data is automatically deleted, beyond the retention period, and this includes any backups.
d. All data is erased and purged to prevent unauthorised or accidental retrieval.
e. Rinicare audit our data yearly to ensure all data has been securely removed from the systems described in this document.

Rinicare complies with Article 17 of the UK GDPR guidelines ("Right to be forgotten"):

f. For Rinicare-held data, please submit your request to our Data Protection Officer, see section 16 below who will ensure that the data has been deleted within 30 days of your request.

g. For Rinicare software data, hosted and held by a third-party organisation, please refer to the third-party's organisation's privacy policy.

11. Automated Decision Making

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

12. 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.

Privacy Notice

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

13. Consent

a. 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.

b. Should the purpose of the data collection change, we will re-obtain authorisation from you.

c. Parental consent must be obtained for any data provided by individuals under the age of 13; should you become aware of parental consent not being provided please report this to our Data Protection Officer – section 16 below.

14. Making a Complaint

If you think your data rights have been breached, you are able to 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.

15. Reporting data confidentiality breaches

The UK GDPR introduces a duty on all organisations to report certain personal data breaches to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

Rinicare has robust breach detection, investigation, and internal reporting procedures in place. This will facilitate decision-making about whether notification to the relevant supervisory authority or the affected individuals, or both is required.

You may find our Data Breach Notification Policy at www.rinicare.com/regulatory.

Rinicare keeps a record of any personal data breaches, regardless of whether you are required to notify.

Please report any breaches to our Data Protection Officer, James Jackson dpo@rinicare.com.

16. Data Protection Compliance

For all personal data hosted by Rinicare, you can exercise any of the rights listed in this privacy notice and according to the laws of England and Wales in writing:

Privacy Notice

For attention of:
Data Protection Officer
Rinicare Limited
Waulk Mill, Bengal Street, Ancoats
Manchester
M4 6LN
United Kingdom

You can email our Data Protection Officer, at dpo@rinicare.com

17. Time Frames

Any requests pertaining to the above shall be processed within 30 days of the request being made.

18. Scope

This privacy notice no longer applies should you follow third-party digital links to another provider or connect to a non-Rinicare managed system; in this case you should consult the third-party's policy.