Clinical IT Ltd
Company Number SC511715
South Charlotte Street
Edinburgh
EH2 4AN
United Kingdom

26/06/2024

Website Privacy Policy

INTRODUCTION

Important information and who we are

Welcome to Clinical IT Ltd's Privacy and Data Protection Policy ("Privacy Policy").

At Clinical IT Ltd ("we", "us", or "our") we are committed to protecting and respecting your privacy and Personal Data in compliance with the United Kingdom General Data Protection Regulation ("GDPR"), the Data Protection Act 2018 and all other mandatory laws and regulations of the United Kingdom.

This Privacy Policy explains how we collect, process and keep your data safe. The Privacy Policy will tell you about your privacy rights, how the law protects you, and inform our employees and staff members of all their obligations and protocols when processing data.

The individuals from which we may gather and use data can include

- Customers
- Business contacts

and any other people that the organisation has a relationship with or may need to contact.

This Privacy Policy applies to all our employees and staff members and all Personal Data processed at any time by us.

Your Data Controller

Clinical IT Ltd is your Data Controller and responsible for your Personal Data. Any inquiries about your data should either be sent to us by email to legal@ekora.io or by post to 5 South Charlotte Street, Edinburgh, EH2 4AN, United Kingdom.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

Processing data on behalf of a Controller and processors' responsibility to you

In discharging our responsibilities as a Data Controller, we have employees who will deal with your data on our behalf (known as "Processors"). The responsibilities below may be assigned to an individual or may be taken to apply to the organisation as a whole. The Data Controller and our Processors have the following responsibilities:

- Ensure that all processing of Personal Data is governed by one of the legal bases laid out in the GDPR (see 2.2 below for more information).
- Ensure that Processors authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing of Personal Data.
- Obtain the prior specific or general authorisation of the Controller before engaging another Processor.
- Assist the Controller in the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights.
- Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.
- Maintain a record of all categories of processing activities carried out on behalf of the Controller.
- Cooperate, on request, with the supervisory authority in the performance of its tasks.
- Ensure that any person acting under the authority of the Processor who has access to Personal Data does not process Personal Data except on instructions from the Controller; and
- Notify the Controller without undue delay after becoming aware of a Personal Data Breach.

LEGAL BASIS FOR DATA COLLECTION

Types of data / Privacy policy scope

"Personal Data" means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of Personal Data about you which we have grouped together below. Not all the following types of data will necessarily be collected from you, but this is the full scope of data that we collect and when we collect it from you:

- Profile/Identity Data: This is data relating to your first name, last name, gender, date of birth.
- Contact Data: This is data relating to your phone number, addresses, email addresses, phone numbers.
- Technical Data: This is your IP address, browser type and version, time zone setting and location, operating system and platform, and other technology on the devices you use to engage with us.
- Customer Support Data: This includes feedback and survey responses.
- Usage Data: information about how you use our website, products and services.

We do not collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

The Legal Basis for Collecting That Data

There are several justifiable reasons under the GDPR that allow collection and processing of Personal Data. The main avenues we rely on are:

- "Consent": Certain situations allow us to collect your Personal Data, such as when you tick a box that confirms you are happy to receive email newsletters from us, or 'opt in' to a service.
- "Contractual Obligations": We may require certain information from you to fulfil our contractual obligations and provide you with the promised service.
- "Legal Compliance": We're required by law to collect and process certain types of data, such as fraudulent activity or other illegal actions.
- "Legitimate Interest": We might need to collect certain information from you to be able to meet our legitimate interests - these covers aspects that can be reasonably expected as part of running our business, that will not have a material impact on your rights, freedom or interests. Examples could be your address, so that we know where to deliver something to, or your name, so that we have a record of who to contact moving forwards.

HOW WE USE YOUR PERSONAL DATA

Our data uses

We will only use your Personal Data when the law allows us to.

Marketing and content updates

You will receive marketing and new content communications from us if you have created an account and chosen to opt into receiving those communications. From time to time we may make suggestions and recommendations to you about goods or services that may be of interest

to you.

Change of purpose

We will only use your Personal Data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your Personal Data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your Personal Data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

YOUR RIGHTS AND HOW YOU ARE PROTECTED BY US

Your legal rights

Under certain circumstances, you have the following rights under data protection laws in relation to your personal data:

- **Right to be informed**. You have a right to be informed about our purposes for processing your personal data, how long we store it for, and who it will be shared with. We have provided this information to you in this policy.
- **Right of access**. This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it (also known as a "data subject access request"). See section 4.4 below for more details on how you can make a data subject access request.
- **Right to rectification**. You have a right to request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Right to erasure**. You have the right to ask us to delete or remove personal data where there is no good reason for us continuing to process it, where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **Right to object**. You can object to the processing of personal data we hold about you. This effectively allows you to stop or prevent us from processing your personal data. Note that this is not an absolute right, and it only applies in certain circumstances, for example:
    - Where we are processing your personal data for direct marketing purposes.
    - Where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground, as you feel it impacts your fundamental rights and freedoms.

- In some cases, we may continue processing your data if we can demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

- **Right to restrict processing**. You have the right to request the restriction or suppression of their personal data. Note that this is not an absolute right and it only applies in certain circumstances:
  - If you want us to establish the data's accuracy.
  - Where our use of the data is unlawful, but you do not want us to erase it.
  - Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.
  - You have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it.
- **Right to data portability**. You have the right to request the transfer of your personal data to you or to a third party. If you make such a request, we will provide you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

If you wish to make a request under any of these rights, please contact us at legal@ekora.io.

How Clinical IT Ltd protects customers' Personal Data

We are concerned with keeping your data secure and protecting it from inappropriate disclosure. Any Personal Data collected by us is only accessible by a limited number of employees who have special access rights to such systems and are bound by obligations of confidentiality. If and when we use subcontractors to store your data, we will not relinquish control of your Personal Data or expose it to security risks that would not have arisen had the data remained in our possession. However, unfortunately no transmission of data over the internet is guaranteed to be completely secure. It may be possible for third parties not under the control of Clinical IT Ltd to intercept or access transmissions or private communications unlawfully. While we strive to protect your Personal Data, we cannot ensure or warrant the security of any Personal Data you transmit to us. Any such transmission is done at your own risk. If you believe that your interaction with us is no longer secure, please contact us.

Opting out of marketing promotions

You can ask us to stop sending you marketing messages at any time by emailing legal@ekora.io.

Where you opt out of receiving these marketing messages, we will continue to retain other Personal Data provided to us as a result of interactions with us not related to your marketing preferences.

How to request your data and the process for obtaining it

You will not have to pay a fee to access your Personal Data (or to exercise any of the other rights). However, if your request is clearly unfounded, we could refuse to comply with your request.

We may need to request specific information from you to help us confirm your identity and ensure you have the right to access your Personal Data (or to exercise any of your other rights). This is a security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

YOUR DATA AND THIRD PARTIES

Sharing your data with third parties

We may also share Personal Data with interested parties in the event that Clinical IT Ltd anticipates a change in control or the acquisition of all or part of our business or assets or with interested parties in connection with the licensing of our technology.

If Clinical IT Ltd is sold or makes a sale or transfer, we may, in our sole discretion, transfer, sell or assign your Personal Data to a third party as part of or in connection with that transaction. Upon such transfer, the Privacy Policy of the acquiring entity may govern the further use of your Personal Data. In all other situations your data will still remain protected in accordance with this Privacy Policy (as amended from time to time).

We may share your Personal Data at any time if required for legal reasons or in order to enforce our terms or this Privacy Policy.

HOW LONG WE RETAIN YOUR DATA

We will only retain your Personal Data for as long as reasonably necessary to fulfil the purposes we collected it for. We may retain your Personal Data for a longer period than usual in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

NOTIFICATION OF CHANGES AND ACCEPTANCE OF POLICY

We keep our Privacy Policy under review and will place any updates here. This version is dated 26 June 2024.

By using Clinical IT Ltd, you consent to the collection and use of data by us as set out in this Privacy Policy. Continued access or use of Clinical IT Ltd will constitute your express acceptance of any modifications to this Privacy Policy.

INTERPRETATION

All uses of the word "including" mean "including but not limited to" and the enumerated examples are not intended to in any way limit the term which they serve to illustrate. Any email addresses set out in this policy may be used solely for the purpose for which they are stated to be provided, and any unrelated correspondence will be ignored. Unless otherwise required by law, we reserve the right to not respond to emails, even if they relate to a legitimate subject matter for which we have provided an email address. You are more likely to get a reply if your request or question is polite, reasonable and there is no relatively obvious other way to deal with or answer your concern or question (e.g. FAQs, other areas of our website, etc.).

Our staff are not authorised to contract on behalf of Clinical IT Ltd, waive rights or make representations (whether contractual or otherwise). If anything contained in an email from a Clinical IT Ltd address contradicts anything in this policy, our terms or any official public announcement on our website, or is inconsistent with or amounts to a waiver of any Clinical IT Ltd rights, the email content will be read down to grant precedence to the latter. The only exception to this is genuine correspondence expressed to be from the Clinical IT Ltd legal department.