Clinic.co Data and Privacy Policy

Welcome to Clinic.co's privacy policy. Governance and Security are at the core of Clinic.co and we are committed to respecting your privacy and protecting your personal data.

We are registered with the Information Commissioners Office (ZA201864) and For the UK specifically, Clinic.co is compliant with the 2018 Data Proection Act / GDPR.

1. Introduction:

This privacy policy tells you how Clinic.co handles your personal data – as a patient, clinician or administrator using the platform.

Confidentiality and Data security is paramount at Clinic.co and our systems comply with all GDPR, NHS Information Governance, Information Commissioner Office (ICO) and US Health Information Technology (HIT) Standards for Health Information Management (HIM) Practices.

This latest version of our privacy policy was updated on 5th February 2021. It will be regularly updated as new features requiring explanation are added and as further clarity is required.

We have written our Data and Privacy Policy as clearly as possible, but key we wish to state that **we will never sell or pass any data to a third party**. **We also do not use pixels or cookies to undertake website tracking.**

If you have any questions from it, please email us at: info@clinic.co
Clinic.co's registered address is: 1 Curtain Rd, London EC2A 3JX

Clinic.co can be used in two ways, firstly directly (by Clinicians who self-register on the platform) or by an organisation (e.g. an NHS Trust or other healthcare supplier). This affects the data controller / processor relationship. When providing a service at an organisational level, that organisation is the data controller for all data apart from the clinician's user account (login) data. Clinic.co in these circumstances is the data processor. When Clinic.co is supplied directly to a clinician, Clinic.co is both the data controller and data processor.

2. Clinic.co as data controller:

Clinic.co Ltd provides technical services to individual clinicians and organisations to facilitate patient care through video consultation. To enable this certain data has to be controlled (user account data – email, password, profile data). The data is required to be able to provide the service and is therefore maintained for the duration of that individual's account.

When Clinic.co provides services directly to self-registered clinicians, Clinic.co also controls additional data required to enable the platform to work (e.g. appointment data, contact data). In these circumstances, Clinic.co is both the data controller and data processor.

Account data:

Account set up information:

- Name of Account Holder.
- Email address of Account Holder.
- Occupation/Purpose of using the platform and the relevant Registration Number.

Additional profile information (voluntary):

- Voluntary Profile picture/blur screen background image where it contains personal information – this is uploaded voluntary by the Account Holder.
- Information provided by the clinician in the calendar feature.

Financial information (voluntary):

- Payment for Clinic.co by Account Holders: For premium or organisational accounts, Clinic.co charges a fee. Payment details are managed through our payment partner, Stripe. Clinic.co does not have access to, record or process financial information directly. The privacy notice and data protection policy for Stripe can be found in the links.
- Payments from patients/users to Clinic.co: Clinic.co has an inbuilt payment function. Self-Paying patients can pay for the appointment upfront and Account Holders are paid subsequently.

Activity on the Clinic.co system:

- Clinic.co records basic account activity of Account Holders on the system – this includes the number of consultations initiated on the system (text or email), number of consultations charged for and total price charged for consultations.
- For premium customers, we also record the total number of hours recorded and size of records.

3. Clinic.co as data processor:

Where Clinic.co is commissioned at an organisation level (e.g. NHS Trusts), we act as data controller for account login data but data processor for all other data (for examples, data around appointments, appointment duration etc).

4. Personal data we collect about you:

Personal data recorded depends on your method of interacting with us.

Clinician:
To enable the platform to function we control and process account and scheduling / booking data (as explained above).

Administrator:
To provide access to clinician accounts we have to control and process administrator account data. No additional data is required

Client / Patient:
We are NOT an electronic records management system and hence do not collect any patient health data.

- For governance security, Clinic.co retains a record of consultation requests sent to patients for audit, governance and monitoring use of Account Holders. This information is purged periodically.
- Patient data is comprised of the information provided by the clinician (specifically, name, email addresses or telephone number of patient and other information inputted by the clinician as part of setting up the consultation).
- Account Holders can contact clinic.co for data to be removed at any time – see Paragraph 10 for details.
- Account Holders may use certain features such as the ability to read a pulse rate through the video stream – in these circumstances patient data is never recorded or stored.

Messaging and Files: Withing the platform clients / patients can send the clinician text messages and files (such as images of scans). These are transferred direct to the clinician's email inbox and are not stored by Clinic.co

Video Data:

- By default no video is stored. Consultations are live streamed only.
- However, for Premium Account Holders, with patient agreement, consultations can be recorded (premium accounts) and that video can then be stored and shared with the patient.
    - Recordings are not viewed by the Clinic.co team and access is strictly limited to specific members of the technical team when authorised by the video creator for service maintenance with audit trails developed.
    - Recordings are controlled by the Account Holder who can choose to record, delete or share with the patient/user.
    - Recordings are not shared with third parties (unless the Account Holder grants Administrator Access to other users or the Account Holder is part of a Organisation signed up to clinic.co) and held on a separate server based in the country of the Account Holder.

Information you voluntarily provide when Organisations, Account Holders or Users contact us:

- If you contact us by phone or email, we may keep a record of that correspondence in case we need to contact you in relation to the issue for which you contacted us or operational performance improvement.
- If you report a problem to us, we may keep a record of that information in case we need to contact you in relation to the issue for which you contacted us. The

information which you give may include your name, email address and details regarding your account.
- If you are a business, when you contact us, the information which we collect may include: your name, email address and telephone number; the name of your business and your business title and your business address.

Newsletters or emails

- From time to time, we may need to contact Account Holders to update you on changes to our service, additional features or governance matters via your sign up email address.
- We do not share this information with third parties and will only contact Account Holders for the any of the reasons above.

5. Cookies

You may be aware that some organisations use cookies / information from 3rd parties to track browsing habits and target advertising specifically to your interests. Clinic.co does not use cookies at all for these purposes. Similarly, we do not provide cookies to third parties. We do, however, use cookies to remember your preferences within the Clinic.co website and from third parties as part of single sign on.

5. Disclosure of personal data and third-party processors.

The Clinic.co platform works with multiple organisations and if you are an Account Holder who has an account through a Partner Organisation (for example an account paid for by your employer), your Organisation will have access to limited information regarding your use of the system – as set out above.

Separate to this, we will only share your information with other organisations, where we have your permission to do so or where required by law.

Clinic.co uses three third party processors – the data protection policies for each is provided in the links – the lawful basis is legitimate interests in order for us to provide our service:

- AWS – All data is hosted via Amazon Web Services located in the country of the user– Privacy Policy here.
- Clickatell (UK) – Text provider to support generation of text messages – Privacy Policy here.
- Stripe – Payment system to receive financial information (patients to Account Holders and Account Holders to Clinic.co) – Privacy Policy here. This is not relevant to NHS usage as this only concerns when payment is made by the user to the clinician.

6. Data Sharing and Storage

Data originating in the UK is retained on EEA based servers. However, where a user utilises the system outside of the UK/EEA, in which servers are used based in that region. Countries outside of the EEA may not have laws which provide the same level of protection to your personal data as laws within the EEA. Where this is the case, we will put in place appropriate safeguards to ensure that such transfers comply with applicable data protection laws.

7. **Keeping your Information Secure:**

Security is central to Clinic.co and we take the security of our users very seriously. Clinic.co is fully secure and compliant with GDPR, ISO27001, ISO9001 and DCB0129. Video and audio communication is only visible to participants on the call and transmitted over an encrypted connection. It is not recorded or stored on any server unless initiated by the clinician. When recorded, it is safety stored in servers based in the UK.

All live streamed video consultation data is encrypted and only viewable and audible to the intended recipient. The lawful basis for processing this data is the legitimate interest to enable the function of the platform to work.

The text message or email contains a link and when pressed on, the caller is asked to agree to share video and audio data (via a pop-up message before any information is transmitted). There free text field may be used by Account Holders where they deem additional patient consent is required. Once confirmed by the user/patient, video and audio is established. If the Account Holder chooses to store video / audio data that data is stored encrypted and for the length of time determined the Account Holder or Organisation.

8. **Secure Data Processing**:

For UK users, we host our servers in the UK (via Amazon Web Servers). We are Cyber Essential compliant, and our technology stack and systems are compliant with the NHS Data and Security Information Toolkit.

We offer end-to-end encryption for live media – using TLS/DTLS-SRTP for encrypting the media; this works by using a secure handshake to derive the keys for encrypting the payload of the RTP packets. We use TLS 1.2 for inflight data and are compliant with HIPAA and NHS standards. All the data at rest is AES256 bit encrypted in the same country as the client.

The Clinic.co system is hosted on Amazon infrastructure and we follow strict policies as to our handling of personal data and conduct regular reviews of our infrastructure and server security. All staff are trained in the proper handling of personal data and observe our data handling policies. All staff actions on our system are auditable and staff are only provided with access to areas of our system, according to their role.

9. **How long we keep your information**

We will retain your personal data for as long as you wish to be communicated with from us or use our system and for a reasonable period of time since you ceased using the system.

The length of time we keep the personal data will vary dependent on how long we need the personal data to deliver, maintain or improve our services and whether we require the information as part of a dispute or to comply with a legal obligation.

10. Deletion

Once it is no longer necessary for us to retain your personal data, we will ensure that it is permanently and securely deleted or anonymised. We are happy to delete any personal information we store about our community. For requests, please email info@clinic.co with the word 'Delete' in the Subject Field Title and our team will action your request.

11. Right to Know

We think it is important that you are able to control your personal information. You have the right to ask us not to process your personal information. The law also gives you the right to request a copy of the personal information we hold about you. We will consider this a Subject Access Request and will action this within the appropriate time frame set out in the Data Protection Act. Any Subject Access Requests can be made by emailing info@clinic.co. You can also exercise your right to prevent such processing at any time by contacting us.

12. Summary

This policy explains the lawful reasons for data usage and processing within Clinic.co. We really do welcome any questions, comments and requests you may have regarding this Policy. It will be updated, so please do check it and contact us on info@clinic.co if you have queries and/or comments.

13. ICO Registration:

Clinic.co Limited is registered as a data controller with the ICO:

Registration number: ZA201864
Date registered: 25 August 2016