PLINICAL LEGAL DOCUMENT

Privacy Notice

Version: 2.8
Effective: 2 November 2026 (from publication)
Last updated: 2 November 2026
Operator: MTX STUDIO Ltd trading as Plinical
Company no. 15856187
Registered office: Bartle House, 9 Oxford Court, Manchester, England, M2 3WQ

This Notice explains how Plinical uses personal data for its website, clinic business relationships, subscription billing, support and security, and how you can exercise your rights. Each clinic controls its patient records. Plinical processes those records on the clinic's instructions under the Data Processing Agreement.

This edition applies from publication. It provides privacy information and does not ask you to consent to all processing or replace your clinic's own privacy notice.

MTX STUDIO Ltd, trading as Plinical (MTX, Plinical, we, us or our), provides the Plinical public website and business clinic-management service. Personal data means information about an identified or identifiable person. A controller decides why and how personal data is used; a processor handles it on a controller's instructions.

1. Scope

1.1 This Notice applies to visitors to plinical.com and official Plinical pages; prospective and current clinic contacts; clinic administrators and Authorised Users; suppliers and professional advisers; and people who contact or correspond with us.

1.2 It also describes the data we process for clinics as a processor. The clinic's own privacy notice explains its purposes, legal bases and patient-record decisions. The Plinical Data Processing Agreement (DPA) sets out our obligations to the clinic.

1.3 Plinical is a business clinic-management service currently available only to clinics in the United Kingdom (England, Scotland, Wales and Northern Ireland). Patients do not have Accounts, do not sign in to a patient portal and cannot self-book or manage their records through the current Service.

1.4 An Account is a clinic organisation account and its authorised staff access. Customer Personal Data means the personal data processed for a clinic under the DPA. The SaaS Terms govern the clinic subscription. This Notice explains our processing and does not change those contractual terms.

2. Who is responsible and how to contact us

2.1 MTX STUDIO Ltd is a private company limited by shares registered in England and Wales under company number 15856187. Its registered office is Bartle House, 9 Oxford Court, Manchester, England, M2 3WQ.

2.2 MTX STUDIO Ltd is the controller for its own processing described here. Contact support@plinical.com for privacy requests or complaints, or write to our registered office. A subject line such as "Privacy request" or "Privacy complaint" helps us route your message, but is not required.

2.3 Our designated Data Protection Officer (DPO) is Theodoros Mentis. You may contact him directly at th.mentis@mtxstudio.com, by telephone on +49 1525 4199506, or by post at Schierker Str. 31, 12051 Berlin, Germany. MTX STUDIO Ltd's ICO registration reference is ZC226522.

2.4 For patient records and clinic operations in the Service, the relevant clinic is normally the controller and MTX is its processor for hosted and automated operations. Clinic staff use their own credentials; MTX staff do not access clinic patient records or sign in to clinic workspaces. Patients should contact their clinic first. We forward

requests to the relevant clinic where it can be identified and assist it under the DPA.

2.5 If we process limited business contact, subscription billing, fraud-prevention, service-security or legally required records for our own purposes, we do so as controller even if the person also works for a clinic.

2.6 Clinic personal-data processing is subject to the DPA, including security measures, supplier permission for the actual data categories and lawful international-transfer arrangements. We must prevent affected processing where those requirements are not met. Live patient data may be used in a Trial only when that use is enabled and those requirements are satisfied. Demonstration and testing environments use synthetic data.

3. Controller and processor role map

Processing contextMTX roleResponsibility Website visits, enquiries, business contacts We determine the stated purposes and Controller and marketing preferenceshandle rights requests.

We use limited business, billing and Subscription administration, business Controllertechnical information for our own stated support and our service-security records purposes.

Clinic-managed staff profiles, roles, patient The clinic controls these records and user records, appointments, clinical documents, Processorpermissions. We follow its instructions and invoices and audit trailsthe DPA.

The clinic determines the recipient, content Email, SMS, referrals and invoice links sent Processorand purpose; we provide the technical for a clinic service.

4. Personal data we use as controller

4.1 Identity and professional data: name, title, role, clinic or organisation, professional contact details, company details and authority to act.

4.2 Account and access data: business account identifiers, administrator email, clinic code, authentication-related information, access events, timestamps and security information used for our own account administration and service protection. Clinic-managed workforce profiles, permissions and patient-record audit trails are processed for the clinic. The same identifier may appear in both contexts; its use determines our role.

4.3 Commercial and billing data: plan, Order and acceptance records, document versions and timestamps, invoices, subscription status, billing contacts, amounts, payment references, paymentmethod descriptors, optional SMS credit purchases and business correspondence. Stripe collects payment details for clinic subscription and credit payments. We do not store full card numbers or card security codes in Plinical. Patients pay their clinics outside Plinical; patient and clinical data must not be entered into subscription-billing metadata.

4.4 Website, enquiry and support data: form submissions, trial requests, messages, support tickets, correspondence, call or meeting notes and records of assistance.

4.5 Technical and security data: IP address, browser and device information, timestamps, requested pages or functions, login and security events, diagnostic error and performance information, rate-limit signals and anti-bot tokens. Collection depends on the function used and enabled services. This operational information is distinct from optional audience analytics described in section 21.

4.6 Preference and marketing data: cookie choices, communication preferences, opt-ins, opt-outs, objections and suppression records.

5. Clinic data we process for clinics

Depending on clinic use and configuration, Customer Personal Data may include:

CategoryExamples Clinic details, staff names and contact details, Admin/Clinician/Receptionist Clinic and staff roles, credentials, clinic codes and configuration.

CategoryExamples Patient identity and Names, contact details, dates of birth, emergency contacts and GP details. contacts Appointments and Appointment history, diary, room, therapist and service information. operations Medical history, medications, allergies, assessments, treatment plans, clinical Health and clinical notes and communication notes.

Treatment and informed-consent responses and signature images captured Consent and signatures while a patient is present with clinic staff.

Referrals and documentsReferral details, letters, nominated recipients, files and generated PDFs.

Invoices and records of payments received externally by the clinic through cash, Invoices card, bank transfer or another method outside Plinical.

Historic CSV imports, including exports from systems such as Fresha; reports, Imports, reports and audit exports, user actions, IP addresses, device/browser data and timestamps.

6. Sources and whether data is required

6.1 We obtain controller data directly from you; from your clinic, employer or Account administrator; automatically from your use of the Website or Service; from our operational providers; and, for prospective clinic contacts, from the clinic's own public website and from Companies House, as described in section 11.

6.2 Clinic-controlled data comes from the clinic and its staff, historic imports, individuals dealing with the clinic, and recipients selected by the clinic. Fresha is not connected by a live Plinical API merely because a clinic uploads a historic Fresha CSV export.

6.3 We need account identity, business contact and security information to create and protect an Account and provide requested services. Billing information is needed to take payment and keep required accounting records. Without the necessary information, we may be unable to provide the relevant service or answer your enquiry. Optional marketing consent may be declined without preventing a subscription.

Required and optional fields are identified where information is collected.

6.4 Support is ticket-based: a clinic describes its issue and we reply with guidance or a solution, without staff access to its patient records or clinic workspace. Do not send patient records, clinical notes, unredacted clinical screenshots, medical documents, passwords or decryption keys through public forms or support tickets. Use synthetic examples or fully redacted information to describe an issue.

6.5 When we receive your data from another source, we provide the applicable privacy information within one month, or earlier if we first contact you or disclose it to another recipient, unless a lawful exception applies. You can ask us about the specific source of information we hold about you.

7. Purposes and legal bases where MTX is controller

The bases below are contract (UK GDPR Article 6(1)(b)), legal obligation (Article 6(1)(c)), legitimate interests (Article 6(1)(f)) and consent (Article 6(1)(a)). Contract applies only where the contract is with you personally, for example as a sole trader, and the processing is necessary for that contract or steps you requested. A contract with your employer does not make contract the lawful basis for processing your details.

PurposePersonal data and lawful basis Identity, professional, enquiry and commercial data. Contract or Enquiries, demonstrations, trials requested pre-contract steps where you are personally the contracting and contractingparty; otherwise legitimate interests in responding to enquiries and managing prospective clinic relationships.

Identity, account, business communications, support and relevant technical data. Contract where necessary to serve an individual Account administration and contracting customer; otherwise legitimate interests in managing service support business accounts, authorised contacts, support and service communications.

Billing contacts, payment references, transaction and acceptance records.

Subscriptions and optional creditContract for an individual contracting customer; legitimate interests in purchasesadministering a corporate customer relationship and collecting amounts due.

Invoices, transaction and business-contact information. Legal obligations Accounting and tax recordsto maintain accounting and tax records, including under applicable company and tax legislation.

Necessary account, technical, security and communication data.

Security, abuse and fraud Legitimate interests in protecting people, data and systems, investigating preventionmisuse and preventing fraud. Legal obligation where a specific law requires action.

Identity, contact, request and relevant service records. Legal obligations Privacy requests, complaints and under data-protection law and other applicable requirements, including legal duties binding court or regulatory demands.

Relevant identity, commercial, support and security records. Legitimate Legal claims and disputesinterests in establishing, exercising or defending legal rights; legal obligation where retention or disclosure is required.

Professional contacts and preferences. Consent for electronic marketing Business marketingwhere required; otherwise legitimate interests in relevant business promotion where electronic-marketing law permits it. See section 10.

Technical and preference data. Legitimate interests in operating a secure, Website operation and usable website for necessary functions. Consent for optional device preferencesaccess where required. A cookie exception does not itself supply a UK GDPR lawful basis.

Minimised support, technical and operational information. Legitimate interests in resolving faults and improving reliability and usability. This Service improvement purpose does not authorise independent use of identifiable patient records. Optional measurement follows section 21.

8. Legitimate interests

8.1 Where we rely on legitimate interests, the interests include operating and improving a secure B2B service; responding to professional enquiries; managing clinic relationships; contacting prospective clinic businesses about Plinical as described in section 11; preventing abuse and fraud; protecting legal rights; and sending relevant business marketing where permitted.

8.2 We assess whether processing is necessary, balance the interests against individuals' rights and apply safeguards such as minimisation, limited access and retention. We do not rely on legitimate interests where your rights and freedoms override those interests. You may ask about the relevant assessment and object as explained in section 17.

9. Health and other special category data

9.1 Health information, medical history, medications, allergies, clinical assessments, treatment plans and some consent information are special-category personal data. MTX normally processes these only as processor for the clinic under the DPA and the clinic's documented instructions.

9.2 The clinic selects its Article 6 lawful basis and Article 9 condition and meets its transparency, treatment-consent and clinical duties. Consent to treatment is not automatically consent to data processing. We do not sell clinic personal data or use it for advertising, our own marketing or training general-purpose artificial-intelligence models. Creating anonymous statistics from clinic data must itself fall within documented clinic instructions and the DPA; only irreversibly anonymised information may then be used independently.

9.3 Signature images are used to evidence form completion and are not used by MTX for biometric identification. Any new biometric-identification use would require separate instructions, assessment and safeguards.

9.4 Do not send patient health information through public forms or support tickets. If it is sent accidentally, we limit handling to securing it, notifying the relevant clinic where identifiable, and arranging return or deletion under lawful instructions, with any legally required handling. It does not authorise access to clinic records. If we exceptionally need special-category data for our own legal claims, we rely on an appropriate Article 6 basis and Article 9(2)(f) where its requirements are met. Legitimate interests alone do not authorise use of health data.

10. Marketing and service communications

10.1 We send necessary verification, security, subscription and service messages using the applicable bases in section 7. These messages are limited to operational purposes. Marketing choices do not prevent necessary service messages.

10.2 Promotional communications identify MTX STUDIO Ltd or Plinical and provide a clear unsubscribe or objection method. We apply the UK GDPR and the Privacy and Electronic Communications Regulations to the recipient and channel.

10.3 Where electronic-marketing law permits it, we may send relevant business marketing to corporate subscribers and rely on legitimate interests for named business contacts. For individual subscribers, including sole traders and some partnerships, we use consent unless a valid soft opt-in applies: we obtained the address during a sale or genuine sales negotiation, promote our own similar services, and offered a clear opt-out both when collecting the details and in every message. We honour objections and do not treat a marketing opt-out as subscription cancellation. Prospecting of clinic businesses is described in section 11.

10.4 You may opt out at any time using the message link or support@plinical.com. We may retain minimal suppression information so that we continue to honour the request.

11. Business contacts and prospecting

11.1 We find and contact prospective clinic businesses to tell them about Plinical. We collect this information from sources other than the person concerned, so this section is our notice under UK GDPR Article 14. The first email we send includes a link to this Notice.

11.2 What we collect: the business contact's name, their role, the business email address, the clinic name, and public business details such as the company number and the address published for that clinic. This prospecting does not use patient records.

11.3 Where it comes from: the clinic's own public website, and the Companies House record for that clinic. We use a business email address only where the clinic has published it on its own website.

11.4 Why we use it: to contact the business about Plinical. The lawful basis is legitimate interests (UK GDPR Article 6(1)(f)). The interest is introducing our clinic-management service to UK clinic businesses that publish their own details. We balance that interest against the limited business-contact data, the professional context of the message, and the right to stop the contact. You may ask us about that assessment, as described in section 8.

11.5 Who this covers: UK clinics that are limited companies or limited liability partnerships. Those businesses are corporate subscribers under the Privacy and Electronic Communications Regulations. Regulation 22 of those Regulations, which requires consent for some electronic mail marketing, does not apply to corporate subscribers. Sole traders and ordinary partnerships are individual subscribers and are outside this prospecting route. Marketing to an individual subscriber follows section 10, including consent or a valid soft opt-in.

11.6 How to object or opt out: you may object, or opt out, at any time. Reply to the email, or email hello@plinical.com. You do not need particular words. We stop contacting you for this marketing. Every prospecting email explains how to opt out. Section 17 explains the wider right to object, including to direct marketing.

11.7 How long we keep it: if there is no engagement, we delete the prospect record within 12 months of collecting it. If you object or opt out, we delete the prospect record and keep only a minimal suppression record. That record is the business email address and, where needed so we do not email that clinic again, the email domain. We keep the suppression record for as long as needed to honour the request.

11.8 You may complain to us using section 18. You also have the right to complain to the Information Commissioner's Office (ICO). Information and submission routes are at ico.org.uk/make-a-complaint. The ICO normally asks you to raise the issue with us first. Contacting us does not remove your right to contact the ICO.

12. Patient facing communications sent for a clinic

12.1 At a clinic's instruction, Plinical may send transactional email through Resend, optional SMS through The SMS Works, time-limited invoice links and referral documents to recipients selected by the clinic.

12.2 The clinic determines the recipient, purpose, content and timing. It must minimise health information in subject lines, SMS messages and invoices, verify recipient details and meet any consent or direct-marketing requirement.

12.3 Invoice and document links are access-controlled and time-limited. Patients do not need a Plinical Account and do not make payments through the Service. Access to a link may generate necessary technical and security records. Stripe processing for clinic subscriptions and optional credit purchases is separate from patient invoices and payments.

13. Recipients and service providers

We share only information needed for the relevant service or lawful purpose. Providers acting on our behalf are subject to processing contracts; providers acting for their own purposes have their own privacy notices. Optional services receive data only when enabled for the relevant function. The following are the relevant services and recipient categories.

RecipientRole and relevant processing / location Website and application hosting, request handling and functions. Clinic application Vercelfunctions are configured for London (lhr1). Edge delivery, security, account, support or other provider operations may involve other locations.

Managed PostgreSQL hosting for structured application data, configured in London.

Neon Provider account, support and onward processing may occur elsewhere.

Vercel BlobFile and PDF storage configured in Washington, D.C., United States (iad1).

Transactional email dispatch configured for Ireland (eu-west-1); account data, Resend email metadata, logs and API records may be processed in the United States.

The SMS WorksOptional clinic-instructed SMS delivery. Its AI Optimiser is disabled.

Optional error and performance monitoring using the Germany/EU storage organisation. Configuration excludes or scrubs clinical content, credentials and Sentry message bodies and excludes session replay. Enabled monitoring uses only necessary technical information.

Registration anti-bot protection using limited browser and network signals and tokens, with global processing. Cloudflare acts as processor to provide protection Cloudflare Turnstile and as a separate controller to improve bot detection. We do not send registration form contents or clinical data to verify a token. See the Turnstile Privacy Notice.

Optional rate limiting configured for Ireland (eu-west-1) as the production Upstash Redis primary/read location. Clinical record content is not intentionally stored.

Clinic subscription checkout, recurring billing, optional credit purchases and related fraud/security processing. Uses billing contacts, payment information and transaction metadata, with international processing including the US and India. Stripe Stripe acts as processor for some activities and independent controller for others; see Stripe's Privacy Policy. Patient records are not sent for billing.

Advisers and Professional advisers, insurers, auditors, courts, regulators, law enforcement and authoritiespublic authorities where reasonably necessary or legally required.

A prospective buyer, investor, lender or successor under confidentiality and data- Business transactionsminimisation controls where relevant to a genuine financing, reorganisation or sale.

RecipientRole and relevant processing / location Clinic-selected Referral recipients, patient communication destinations and other recipients recipientsselected by a clinic; MTX acts on the clinic's instructions.

Auth.js is a self-hosted application library, not a separate recipient merely because the library is used.

Fresha is not a live Plinical integration where a clinic only uploads a historic export. We do not sell personal data. We display clinic logos as endorsements only with separate permission.

14. International transfers

14.1 The Service uses UK, European Economic Area (EEA), United States and global infrastructure. Clinic application functions and structured data are configured in London; files and PDFs are stored in the United States; email dispatch is configured in Ireland with some Resend account and metadata processing in the United States. Cloudflare processes signals globally, and Stripe's international processing includes the United States and India. A selected storage region does not exclude support, security, account or onward processing elsewhere.

14.2 A UK clinic's direct disclosure to UK-based MTX is not ordinarily a restricted transfer merely because MTX later uses an overseas provider. MTX remains responsible for applying the relevant transfer rules to its onward disclosures.

14.3 A restricted transfer must have a lawful mechanism before it takes place. For UK data, this is an applicable UK adequacy regulation where it covers the recipient and processing, or appropriate safeguards such as the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses. When contractual safeguards are required, the applicable data protection test, also known as a transfer risk assessment, and any necessary supplementary measures form part of the arrangements. Contact us for the mechanism and safeguards relevant to your data.

14.4 Reliance on the UK Extension to the EU-US Data Privacy Framework requires an active certification covering the recipient and relevant data, including the UK Extension. Where EU GDPR applies, the corresponding EU transfer rules apply, using applicable adequacy or safeguards such as the EU Standard Contractual Clauses. A provider's general privacy statement or choice of storage region does not itself establish that a transfer is permitted.

14.5 Contact support@plinical.com to obtain information about the safeguards relevant to your data and a copy of the applicable safeguards. Proportionate redactions may protect confidential information and other individuals without concealing the protection provided. Transfers must remain within the legally applicable mechanism and the provider contract's permitted data categories.

15. Retention

We retain our controller records for the periods below where needed for the stated purpose. We consider the type and sensitivity of the information, the relationship, legal duties, security needs and any live dispute, and delete or anonymise information when it is no longer required. These periods do not set a clinic's clinical-record retention schedule.

RecordTypical retention Up to 12 months after the last meaningful contact or enquiry closure, Lead and enquiry data unless a relationship begins or a longer period is justified.

Prospective clinic contacts collected under section 11. Deleted within 12 months of collection if there is no engagement. On objection or opt-out, the prospect record is deleted and only a minimal suppression record is kept, as described in section 11.

Account access ends under the trial terms; minimal sales/contact records Non-converting trial contacts normally up to 12 months after trial end.

Account, administrator and During the relationship and normally up to 6 years after contract end billing contactswhere needed for tax, accounting, audit, claims or dispute records.

RecordTypical retention Invoices and accounting Normally six years from the end of the relevant company financial year, or evidencelonger where tax or accounting law requires it.

Normally up to 24 months after closure; longer where needed for an Support tickets unresolved incident, claim or recurring technical issue.

Normally 12 months and up to 24 months for privileged-administration or MTX security and operational security-relevant events; longer only where justified for an active logsinvestigation, claim or legal requirement. Clinic patient-record audit trails follow clinic instructions and the DPA.

For the life of the relevant preference or device item. We retain consent or objection evidence for as long as needed to demonstrate and honour Cookie and preference records the choice, taking account of its use and any relevant dispute. Device durations are given in the applicable cookie information.

Minimal details for as long as reasonably needed to honour an opt-out or Marketing suppression records objection.

The DPA provides a 30-day retrieval period unless the Order allows longer, followed by active deletion without undue delay. An earlier lawful Customer Personal Data after deletion instruction may be given. Protected backups are removed no termination later than 90 days after active deletion, unless law requires longer storage; restoration does not restart the deadline.

Access by former staff is removed when no longer authorised even where limited business evidence is retained. A longer period for our controller records must be justified by a legal duty, active claim or proportionate security investigation. We restrict retained information from ordinary use and review the need to keep it. For clinic-controlled data, the clinic's instructions and DPA govern; MTX's general business interests do not extend the post-termination storage period. The relevant clinic explains how long it keeps patient records during its use of the Service.

16. Security

16.1 Our security measures address tenant separation, individual authentication, clinic-user permissions, access controls, encryption in transit and at rest, protected backups, operational logging, secure development and incident response. Relevant functions also use rate limiting and bot protection.

Measures must be appropriate to the sensitivity and risks of the processing. Encryption in transit and at rest does not mean that only the clinic holds decryption keys: application or provider services may decrypt data to carry out authorised processing.

16.2 MTX staff do not access clinic patient records or sign in to clinic workspaces. Access to our own business, technical and support records is limited by role and confidentiality duties. Hosted and automated provider processing is distinct from staff access and remains subject to the DPA, permitted data categories and transfer requirements. We review security measures and update them without materially reducing overall protection.

16.3 No online service is absolutely secure. Authorised Users must use strong unique credentials, protect clinic codes and devices, remove leavers promptly, verify communication recipients and notify us without undue delay of suspected unauthorised access.

16.4 Public Website forms, email and SMS are not suitable for unnecessary clinical detail. Clinics should use approved secure workflows and maintain appropriate downtime and business-continuity arrangements.

17. Your rights

17.1 Subject to the conditions and exemptions in data-protection law, you can request access and a copy of your personal data; correction of inaccurate or incomplete data; deletion; or restriction of processing.

Where automated processing is based on consent or a contract with you, you may also request portability of data you provided, in a structured, commonly used and machine-readable format, and transmission to another controller where technically feasible.

17.2 Your right to object: you may object at any time to processing for direct marketing, including related profiling, and we will stop that use. You may also object for reasons relating to your situation where we rely on legitimate interests. We will stop that processing unless we demonstrate compelling legitimate grounds overriding your interests, rights and freedoms, or need it for legal claims. Where we rely on consent, you may withdraw it at any time without affecting processing already carried out lawfully.

17.3 Contact support@plinical.com, our DPO or our registered office. No particular wording or form is required. We may seek information reasonably necessary to verify identity or authority and clarify a request. We respond without undue delay and normally within one calendar month. Where law allows, complex or numerous requests may take up to two additional months; we explain the extension and reasons within the first month. Any permitted adjustment for necessary identity checks or clarification follows the applicable law. If we cannot act on a request, we explain why and how to complain.

17.4 If a request concerns patient or clinic data controlled by a clinic, contact that clinic first. We will not independently decide the request but will assist the clinic under the DPA. If we receive it directly and can identify the clinic, we will forward it without undue delay.

17.5 Requests are normally free. We may charge a reasonable fee or refuse a manifestly unfounded or excessive request only where law permits, explaining the reasons. Other limits may protect another person's rights, required records or applicable legal exemptions. These limits do not remove your right to complain.

18. Privacy complaints

18.1 If you are concerned about how we use your personal data, contact support@plinical.com, our DPO, or write to our registered office. Tell us what happened and the outcome you seek, with enough detail for us to identify the issue. You do not need to use a particular subject line, form or channel; we also recognise complaints received through other appropriate contact routes. Tell us if you need help or an accessible way to complain.

18.2 We acknowledge a data-protection complaint within 30 days of receiving it, make appropriate enquiries, keep you informed of progress where needed, and communicate the outcome and any action without undue delay. A complaint does not extend the separate deadline for a rights request.

18.3 You have the right to complain to the Information Commissioner's Office (ICO). Information and submission routes are available at ico.org.uk/make-a-complaint. The ICO normally asks you to raise the issue with the organisation first. Our process does not remove your statutory right to contact the ICO or seek a judicial remedy.

18.4 For clinic-controlled patient data, complain to the clinic in the first instance. You may still contact the ICO about the relevant controller's handling.

19. Automated decisions and AI

19.1 We do not use the controller data described here for solely automated decisions, including profiling, that produce legal or similarly significant effects on individuals. Automated anti-bot, security and payment checks may challenge, reject or flag an action. Contact us if you believe a check has wrongly prevented access so that we can investigate. Independent payment providers explain their own processing in their notices.

19.2 Plinical does not provide automated clinical decisions, diagnosis, treatment recommendations, risk scoring or triage. Customer Personal Data is not used to train general-purpose AI models.

20. Children

20.1 The Website and Service are directed to professional users aged 18 or over and not to children as Account holders. We do not knowingly offer consumer online services directly to children.

20.2 Clinics may lawfully record information about child patients. The clinic is controller and is responsible for lawful bases, transparency, consent or parental-authority issues, safeguarding and professional duties.

MTX processes that data only under the clinic's instructions and DPA.

20.3 If a child or parent believes information has been submitted outside an appropriate clinic relationship, contact the clinic or support@plinical.com so the controller can be identified.

21. Cookies and similar technologies

21.1 The public website stores a selected light or dark appearance in the browser's local storage under the key "theme". It reads that value on page load and has no automatic expiry. The light/dark control changes the saved choice; it does not disable storage. The Cookie Policy explains how to remove the value and the available controls. The public website also stores campaign parameters in session storage under the key "plinical.attribution". That record is kept for the browser tab, is cleared when the tab closes, and is not a cookie. It may contain utm_source, utm_medium and utm_campaign when the visitor arrived with those parameters. It does not contain names, email addresses or form content. The authenticated Service uses separate storage and access technologies for sessions, security and requested functions. Strictly necessary uses may operate without consent only where the statutory exception applies.

21.2 The public website uses standard Vercel Web Analytics for aggregate statistics such as visitors, page views, popular pages and routes, referrers, countries, devices, browsers, operating systems and bounce rate. Vercel is already described in section 13 as the website hosting recipient. The integration does not send form-field values, names, email addresses, telephone numbers, clinic codes, account identifiers, authentication tokens, payment or checkout identifiers, patient information or free-text clinical content. It may also record a custom event when someone follows a trial registration link or successfully submits the contact form. The trial-link event carries an event name, a page location label, and, when the link is a Solo or Practice pricing button, the plan (solo or practice). When the visitor arrived with them, the trial-link event and the successful contact-form event also carry utm_source, utm_medium and utm_campaign. Those events do not send names, email addresses or form content. You can opt out of storing and sending that campaign label, free of charge, with the control on the Cookie Policy page at https://www.plinical.com/cookies#campaign-analytics-opt-out. The public website also uses Vercel Speed Insights for anonymous performance metrics. Speed Insights does not use cookies and does not receive names, email addresses or form content. Advertising tracking, Google Analytics, Google Tag Manager, Meta Pixel, session replay and behavioural heatmaps remain disabled. Essential hosting, authentication, security and payment operations still process the information described in this Notice. Before enabling additional optional tracking or new measurement purposes, we will provide the necessary information and implement consent or objection controls required by law.

21.3 The public website Cookie Policy describes the marketing website, including its technologies, purposes, duration and controls. Information provided in the authenticated Service and by payment providers applies to those separate environments. Where a technology requires consent, it must not operate before valid consent. Where an exception requires a way to object, that control must be available and effective before we rely on the exception. Publishing this Notice does not itself provide consent or a technology choice.

22. Changes to this Notice

22.1 We review this Notice and update it when processing, providers, law or guidance materially changes.

The Website will carry the current version and last-updated date.

22.2 Where a new use materially affects individuals, we will provide additional or just-in-time information and, where required, obtain consent before that use begins.

22.3 Version 2.8. Document date: 2 November 2026. This edition replaces version 2.7 of the public Plinical Privacy Notice when published. Version 2.8 records the free opt-out for storing and sending the campaign label, using the control on the Cookie Policy page. Publication does not retrospectively authorise a new purpose or change the version of a customer's accepted SaaS Terms or DPA.

23. Contact

MTX STUDIO Ltd trading as Plinical Bartle House, 9 Oxford Court, Manchester, England, M2 3WQ.

Company number 15856187. ICO registration reference ZC226522.

Privacy requests and complaints:support@plinical.com.

Data Protection Officer: Theodoros Mentis, th.mentis@mtxstudio.com. Telephone and postal details are in section 2.3.

Related information: Data Processing Agreement, SaaS Terms, Cookie Policy and ICO registration.