PLINICAL LEGAL DOCUMENT

Data Processing Agreement

Version: 2.2
Effective: When the Agreement incorporating this version is concluded (clause 2.3)
Last updated: 21 October 2026
Operator: MTX STUDIO Ltd trading as Plinical
Company no. 15856187
Registered office: Bartle House, 9 Oxford Court, Manchester, England, M2 3WQ

Plinical Data Processing Agreement

Version 2.2 | Document date 21 October 2026

Terms governing the processing of clinic personal data by MTX STUDIO Ltd on behalf of UK clinic businesses and self-employed professionals using Plinical. This agreement forms part of each customer's accepted Order and covers the service term, security, Sub-processors, international transfers and the return or deletion of data.

This Data Processing Agreement (the DPA) is between the clinic business or self-employed professional identified as the customer in the accepted Order and its electronic acceptance record (the Controller) and MTX STUDIO Ltd, trading as Plinical, company number 15856187, whose registered office is at Bartle House, 9 Oxford Court, Manchester, England, M2 3WQ (the Processor).

This DPA forms part of the subscription terms and accepted order under which the Controller receives the Plinical service (together, the Agreement). The Order is the electronic order or other written service order identifying the contracting customer and the service purchased or taken on trial. This DPA applies to all Customer Personal Data Processed on the Controller's behalf. The clinic's legal identity, contact details and authorised representative are incorporated from the Order and acceptance record as described in Schedule 5.

1. Definitions and interpretation

1.1 Applicable Data Protection Law means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003, and any legislation that replaces, amends or supplements them; and the EU GDPR and relevant EEA member-state law only to the extent they apply to the Processing.

1.2 Controller, Data Subject, Personal Data, Personal Data Breach, Processing, Processor, Special Category Data and Supervisory Authority have the meanings given by Applicable Data Protection Law.

1.3 Customer Personal Data means Personal Data Processed by the Processor on behalf of the Controller through the Plinical service. Restricted Transfer means a transfer of Personal Data to which the international-transfer requirements in Chapter V of the UK GDPR or EU GDPR apply and for which a valid transfer basis is required.

1.4 Sub-processor means another Processor engaged by the Processor to Process Customer Personal Data. References to writing include durable electronic communications. If this DPA conflicts with the Agreement on Processing of Customer Personal Data, this DPA prevails. Mandatory standard transfer clauses prevail over conflicting terms.

2. Scope roles and duration

2.1 The Controller determines the purposes and essential means of Processing Customer Personal Data.

The Processor provides the hosted and automated Plinical service on the Controller's behalf as described in Schedule 1. Clinic staff use their own credentials. Under the current operating model, MTX staff do not access clinic patient records or sign in to clinic workspaces; support is by ticket and reply with guidance or a solution.

Hosted storage and automated operations are distinct from staff access to readable patient records.

2.2 Each clinic is a separate Controller and logical tenant. The Processor does not become controller of a clinic's patient records merely by providing the service. The Controller remains responsible for clinical decisions, record content, patient communications, retention choices and the lawfulness of its instructions.

2.3 This DPA takes effect when the Agreement incorporating this version is concluded through the recorded Order and acceptance process, or when the parties otherwise agree in writing to incorporate this version (the Effective Date). It applies during any trial involving Customer Personal Data and continues while the Processor Processes Customer Personal Data, including the limited retention under clause 12. Separate handwritten signatures are not required for recorded online acceptance. Publication of this DPA does not by itself bind a clinic or replace a version it has already accepted.

2.4 For limited business contact details, subscription billing data, fraud prevention, service security evidence and records the Processor must keep for its own legal obligations, MTX may act as an independent controller. That processing is described in the Privacy Notice and is outside this DPA. This does not permit MTX to reclassify clinic health data as its own controller data or repurpose it for product development.

2.5 Before commencing any Processing of Customer Personal Data, the Processor shall have in place the applicable security measures, Sub-processor contracts, permissions for the actual data categories and international-transfer safeguards required by clauses 6, 9 and 10. Where a requirement is not met, the Processor shall prevent the affected Processing until it is met. Live patient-data use during a trial is permitted only when the Processor has enabled that use and these requirements are satisfied.

Demonstration environments shall use synthetic data and remain separate from clinic datasets.

3. Controller instructions

3.1 The Processor shall Process Customer Personal Data only on the Controller's documented instructions, including instructions concerning Restricted Transfers, unless UK law requires otherwise, or applicable EU or member-state law requires it where the EU GDPR applies. The Agreement, this DPA, the Controller's configuration and authorised use of the service, and durable written support requests are documented instructions.

3.2 If law requires Processing beyond the Controller's instructions, the Processor shall inform the Controller before Processing unless the law prohibits that notice. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes Applicable Data Protection Law, and may suspend the affected Processing while the parties resolve the issue.

3.3 The Processor shall not sell Customer Personal Data, use it for advertising, or use it to train generalpurpose artificial-intelligence models. The Processor shall not contact patients for its own marketing.

Service-generated communications are sent only on the Controller's instruction.

4. Controller responsibilities

4.1 The Controller shall: (a) have a lawful basis under Article 6 and a valid Article 9 condition for health or other Special Category Data under the UK GDPR and, where applicable, the EU GDPR, together with any additional safeguards required by applicable law; (b) give required privacy information; (c) ensure instructions are lawful, fair and proportionate; (d) configure permissions and retention appropriately; (e) keep authorised-user details current; and (f) respond to Data Subjects and regulators. Where records concern children or persons lacking capacity, the Controller is responsible for the applicable authority, transparency and safeguarding requirements.

4.2 The Controller shall ensure that only authorised staff use the service, protect clinic codes and credentials, promptly disable leavers, and not upload data that is excessive for the stated clinical or administrative purpose.

4.3 Where the Controller enables email or SMS, it determines the recipients, content and timing. It shall minimise sensitive detail in subject lines and message bodies and shall obtain any consent required for non-transactional messages. Plinical is not a patient portal and patients do not receive accounts.

5. Confidentiality and personnel

5.1 The Processor shall bind personnel and contractors handling service operations, business/support information or any inadvertently supplied Customer Personal Data to enforceable confidentiality duties and appropriate data-protection/security instruction. Access to permitted operational information shall be limited to what their role requires. This clause does not grant personnel access to clinic patient records or clinic workspaces. The staff-access and ticket-support boundary in clause 2.1 applies; the Controller must not send patient records, unredacted clinical screenshots, passwords or decryption keys in support tickets.

5.2 The confidentiality obligations survive termination. The Processor remains responsible for its personnel's compliance with this DPA.

6. Security

6.1 Taking account of the state of the art, implementation cost, and the nature, scope, context and purposes of Processing, as well as risks to individuals, the Processor shall implement and maintain appropriate technical and organisational measures meeting Article 32 of the UK GDPR. The baseline measures are in Schedule 2.

6.2 The Processor may update security measures to reflect technical development, provided an update does not materially reduce the overall protection of Customer Personal Data. The Processor shall regularly assess the effectiveness of relevant controls and remedy material deficiencies within a risk-appropriate period.

6.3 The Controller acknowledges the shared-responsibility measures in Schedule 2, including its responsibility for user administration, endpoint security, accurate contact details, appropriate exports and secure handling of downloaded files.

7. Personal Data Breaches

7.1 The Processor shall notify the Controller without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data and in any event within 24 hours of that awareness. The first notice need not contain every fact and may be followed by phased updates without undue further delay. The Processor shall not wait for a completed investigation or a supplier's final report. Notice shall be sent to the Controller's nominated privacy/breach contact and account or notices email.

7.2 The notice shall, so far as available, describe the nature of the breach; affected categories and approximate numbers of Data Subjects and records; likely consequences; containment, remediation and mitigation; the incident contact; and information reasonably needed for the Controller's Articles 33 and 34 UK GDPR duties.

7.3 The Processor shall promptly investigate, contain and remediate the breach, preserve appropriate evidence, provide material updates, and reasonably assist the Controller. Notification is not an admission of fault. The Controller decides whether to notify a Supervisory Authority or Data Subjects, unless law places a direct duty on the Processor.

7.4 The Processor shall not notify affected patients or another third party about the Controller's breach without the Controller's instruction, except where legally required or urgently necessary to reduce imminent harm; where permitted, it shall consult the Controller first.

8. Data Subject rights and regulatory assistance

8.1 Taking account of the nature of Processing, the Processor shall use appropriate technical and organisational measures to help the Controller respond to requests to exercise rights under Applicable Data Protection Law.

8.2 If the Processor receives a request concerning Customer Personal Data directly from a Data Subject, it shall not substantively respond except on the Controller's instruction or as required by law. It shall forward the request to the Controller without undue delay and ordinarily within five business days, where the Controller can be identified.

8.3 Taking account of the nature of Processing and information available, the Processor shall reasonably assist with security, breach assessment and notification, data-protection impact assessments, prior consultation with a Supervisory Authority, records of Processing and demonstrations of compliance.

8.4 Assistance included in ordinary service functionality is provided without additional charge. The Processor may charge reasonable, pre-agreed fees for exceptional, bespoke or excessive assistance unless the need arose from the Processor's breach of this DPA.

8.5 Fees, ordinary service limitations and administrative procedures shall not prevent or delay assistance, information or access required by Applicable Data Protection Law. The Processor shall provide information and assistance in time for the Controller to meet applicable statutory deadlines, taking account of the information available and the urgency of the request.

9. Sub processors

9.1 The Controller gives general written authorisation for the Sub-processors listed in Part A of Schedule 3 and for replacements or additions made under this clause. A listed service may Process Customer Personal Data only within its stated purpose and data scope and after clauses 2.5, 9.4 and 10 have been satisfied.

Services marked optional operate only when enabled or configured for the relevant purpose.

9.2 The Processor shall give at least 15 calendar days' prior electronic notice of every intended addition or replacement of a Sub-processor that will Process Customer Personal Data, without a materiality threshold.

Notice shall identify the provider, function, affected data, locations, relevant transfer safeguards and proposed start date. The Controller may object during that period on reasonable, documented dataprotection grounds. The Processor shall manage its supply chain so that an upstream change does not bypass the notice period; if necessary it shall prevent the affected data reaching the new provider until the period has elapsed and objections have been addressed, or obtain the Controller's specific prior written authorisation.

9.3 The parties shall work in good faith to address an objection before the new Sub-processor Processes the affected Customer Personal Data. If no reasonable solution is available, the Controller may stop using the affected feature or terminate the affected service without penalty and receive a pro-rata refund of prepaid Fees for the unused affected service. The Processor shall provide a lawful export or return route under clause 12. These remedies do not limit other rights for breach or rights under Applicable Data Protection Law.

9.4 Before a Sub-processor Processes Customer Personal Data, the Processor shall enter into a binding written contract imposing the same data-protection obligations required by Article 28(3), with an equivalent level of protection to this DPA and sufficient guarantees of appropriate technical and organisational measures. The Processor remains fully liable to the Controller for the Sub-processor's performance. The contract and any applicable sensitive-data permission must cover the actual processing, data categories and services used; a listing in Schedule 3 is not a substitute for this requirement.

9.5 Auth.js is used as an application authentication library and is not, by that fact alone, a third-party Subprocessor. Fresha is not connected by live API; a clinic-initiated CSV import does not make Fresha a Subprocessor of Plinical.

10. International transfers

10.1 The Processor shall not make a Restricted Transfer except on the Controller's documented instructions and in compliance with Applicable Data Protection Law. Schedule 3 identifies known locations and global-processing qualifications.

10.2 For an onward Restricted Transfer, the Processor shall verify an applicable adequacy decision or UK adequacy regulation covering the particular recipient and data, or put a valid appropriate safeguard in place before the transfer. Contractual safeguards shall use the legally applicable UK International Data Transfer Agreement (IDTA) or UK Addendum to the EU Standard Contractual Clauses (SCCs), and EU SCCs where required. Where MTX transfers clinic data as processor to a vendor as sub-processor, the appropriate module of the 2021 SCCs is Module Three where legally applicable. Required tables and annexes must accurately describe the data, including health data, and the parties, purposes, locations and safeguards. The Processor shall complete any required data-protection test or transfer risk assessment and implement necessary supplementary measures.

10.3 If a direct Controller-to-Processor transfer becomes a Restricted Transfer without an applicable adequacy route, the parties shall complete and enter the legally applicable mechanism in Schedule 4 before that transfer. The current UK clinic-to-UK MTX relationship is not itself made a Restricted Transfer solely by an onward vendor transfer. The parties shall execute replacements required by law.

10.4 A hosting region describes the primary location selected for a service and does not, by itself, exclude remote support, security telemetry, resilience, content delivery or legally compelled access elsewhere.

The Processor shall accurately document material transfer routes and limit access to what is necessary.

10.5 Where relying on the UK Extension to the EU-US Data Privacy Framework, the Processor shall verify the recipient's active participation, coverage of the relevant legal entity, service and data, and any required sensitive-data identification. A claim of US certification without the UK Extension is insufficient for that UK adequacy route. Where a safeguard ceases to be valid or sufficient, the affected Restricted Transfer shall stop until a lawful alternative is in place. The Processor shall make relevant safeguard information and copies available to the Controller on request, with proportionate redactions that do not prevent assessment of the protection.

11. Audit and information rights

11.1 The Processor shall make available all information necessary to demonstrate compliance with Article 28 of the UK GDPR and this DPA, including relevant policies, independent assurance, security questionnaires, Sub-processor and transfer information. Confidentiality, trade-secret and other-customer protections shall be applied through proportionate redaction or secure review arrangements and shall not be used to withhold information necessary to exercise statutory rights.

11.2 The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by it. Routine audits may normally occur once in any 12-month period on 30 days' notice, during normal business hours and using remote/documentary evidence first where sufficient. Additional audits and shorter notice are permitted following a Personal Data Breach, a reasonable evidence-based concern, a regulator's requirement or whenever necessary to comply with Applicable Data Protection Law. These arrangements shall not obstruct an effective audit or inspection.

11.3 Where remote evidence is insufficient, the Processor shall permit a proportionate on-site inspection.

An independent auditor shall be subject to confidentiality and appropriate security arrangements; any reasonable competitor objection must not prevent appointment of a suitable auditor. The Controller bears its own routine audit costs. Reasonable fees for exceptional assistance must be agreed in advance and must not be prohibitive or impede statutory rights. No Processor assistance fee applies where the audit identifies a material Processor breach. The Processor shall promptly remedy confirmed material non-compliance.

11.4 The Processor shall immediately inform the Controller if, in its opinion, an audit instruction infringes Applicable Data Protection Law.

12. Return export and deletion

12.1 During the term, the Processor shall provide export functionality and necessary assistance for Customer Personal Data. At the end of the service, the Controller may choose return in a commonly used electronic format followed by deletion of copies, or deletion, except to the extent law requires storage.

Return must cover the Customer Personal Data within the Processor's control, including relevant records, attachments and related personal data that a standard self-service export omits. A payment dispute shall not defeat the Controller's return or deletion rights.

12.2 Unless the Agreement grants longer, the Controller may retrieve or request return of Customer Personal Data for 30 days after termination. During this period, retained data shall be restricted to return, deletion, necessary protection and legally required storage. On receipt of an earlier lawful deletion instruction, the Processor shall act without undue delay. After the retrieval period, the Processor shall delete active copies without undue delay. Residual copies in protected backups shall be put beyond ordinary use and deleted through the normal backup cycle no later than 90 days after active deletion, unless law requires longer storage. The Processor shall record the active-deletion date and backupdeletion deadline. These obligations apply to the particular clinic's data and do not depend on closing a shared vendor account.

12.3 This DPA continues to protect retained copies until deletion. Backups may be restored only for necessary disaster recovery, security or legal purposes. Deleted or restricted records shall be put beyond ordinary use again and re-deleted promptly after restoration, without restarting the original deletion deadline. On written request the Processor shall confirm the scope and completion of deletion, including Sub-processors and remaining protected backup expiry dates. If law requires retention, it shall identify the basis, data, period and access restrictions to the Controller unless legally prohibited; business convenience alone does not permit retention.

12.4 The Controller is responsible for exporting any records it must retain and for maintaining legally required clinical records after the service ends.

13. Records cooperation and legal requests

13.1 The Processor shall maintain records required of it by Applicable Data Protection Law and cooperate with the ICO or another competent Supervisory Authority in performance of their tasks.

13.2 If the Processor receives a legally binding request for Customer Personal Data from a public authority, it shall review the request, disclose only what it is legally required to disclose, and notify the Controller before disclosure unless prohibited. Where appropriate and lawful, it shall challenge requests that are unlawful, disproportionate or inconsistent with applicable transfer safeguards.

13.3 The Processor shall not voluntarily provide bulk or indiscriminate access to Customer Personal Data to a public authority.

14. Service communications and documents

14.1 Transactional email and optional SMS are sent as the Controller's communications. The Processor shall use only the contact and message data needed to deliver, troubleshoot and evidence those communications and shall apply the Sub-processor and transfer obligations in clauses 9 and 10.

14.2 Invoice links provided without a patient account must be time-limited and access-controlled. The Controller shall avoid including unnecessary Special Category Data in invoices, email subject lines, SMS messages and referral-recipient addresses.

14.3 Patient signatures captured in the presence of clinic staff form part of the Controller's records. The Processor shall not use signature images for biometric identification unless the parties expressly agree separate documented instructions and safeguards.

15. Change in law

15.1 The parties shall amend this DPA where reasonably necessary to comply with a binding change in Applicable Data Protection Law, a Supervisory Authority requirement or replacement standard transfer clauses. The Processor shall give reasonable notice where practicable.

15.2 If a change materially affects cost or service design, the parties shall discuss a proportionate implementation in good faith, but neither party is required to continue unlawful Processing.

16. Liability

16.1 Each party remains responsible for its own compliance with Applicable Data Protection Law. Nothing in this DPA relieves the Processor of obligations or liabilities imposed directly on processors.

16.2 Liability arising from this DPA is governed by the exclusions and limitations in the Agreement, except to the extent such exclusion or limitation is prohibited by law. Nothing limits liability for fraud, fraudulent misrepresentation, or any liability that cannot lawfully be limited.

16.3 A Data Subject's or regulator's rights are not reduced by this clause.

17. Notices

17.1 Privacy requests, breach notices and security reports to the Processor shall be sent to support@plinical.com. The Controller's privacy, breach and notices contacts are those identified under Schedule 5. Formal legal notices may also be sent to the registered or principal office. Operational incident notification shall not wait for DPO availability.

17.2 A party shall keep its notice details current. A notice is deemed received when delivered through the applicable account, electronic-signature platform or email without a delivery failure, or on recorded delivery to the stated office.

18. General

18.1 No variation of this DPA is effective unless recorded in writing and agreed by authorised representatives, except an update expressly permitted by clauses 6, 9 or 15.

18.2 If any provision is invalid or unenforceable, it shall be read down to the minimum extent necessary and the remainder continues in effect. A delay in exercising a right is not a waiver.

18.3 No person other than the parties has a right under the Contracts (Rights of Third Parties) Act 1999 to enforce this DPA, except that this does not exclude rights expressly conferred on Data Subjects by mandatory standard transfer clauses.

18.4 This DPA and the Agreement constitute the entire agreement concerning its subject matter and may be executed in counterparts and by electronic signature.

19. Governing law and jurisdiction

19.1 This DPA and any non-contractual obligations arising from it are governed by the law of England and Wales.

19.2 The courts of England and Wales have exclusive jurisdiction, except where Applicable Data Protection Law or mandatory standard transfer clauses give a Data Subject or Supervisory Authority another forum or jurisdiction.

Schedule 1 Details of Processing Subject matter. Provision of the cloud-based Plinical B2B clinic-management service to clinic businesses and self-employed professionals and their authorised users, including hosting, ticket-and-reply support, security, clinic administration, patient-record functionality, communications, documents, reporting and exports.

Duration. For the service term and the limited return, deletion and backup periods in clause 12.

Nature and purpose. Hosted storage and automated operations enabling the Controller and its authorised clinic users to record, organise, retrieve, consult, use, communicate, export, restrict and delete their data.

This description does not mean MTX staff consult patient records. Return/deletion assistance uses controlled service capabilities consistent with clause 2.1.

Data Subjects. Patients and prospective patients; emergency contacts; parents, guardians and representatives; GPs, referrers and referral recipients; clinic staff, clinicians, therapists, receptionists, contractors and authorised users; and other individuals included in clinic records or communications.

Personal Data. Clinic and staff details; names, contact details, dates of birth; emergency-contact and GP details; appointment history; rooms, therapists and services; assessments, clinical and communication notes; treatment plans; consent responses; handwritten or digital signature images; referrals; invoices and records of external cash, card or bank-transfer payments; imported historic data; reports and exports; user actions, timestamps, IP addresses, browser/device data and security/audit records.

Special Category Data. Health and medical information, including medical history, assessments, symptoms, diagnoses where recorded, medications, allergies, clinical notes, treatment plans, referrals and consent information. Other Special Category Data may appear if entered by the Controller. Signature images are not treated as biometric data unless used for unique biometric identification. Criminalconviction or offence data is outside the standard service scope unless separately agreed in writing with the legal conditions and safeguards required by Article 10.

Frequency. Continuous or recurring while the Controller uses the service; event-driven for emails, optional SMS, exports, referrals, invoice links, support and CSV imports.

Storage and hosting. Structured application data: PostgreSQL hosted by Neon in London. Application functions: Vercel London (lhr1) as configured. Files and generated PDFs: Vercel Blob, Washington, D.C., USA (iad1). Provider control-plane, support, edge, resilience or security processing may occur elsewhere as described in Schedule 3 and applicable vendor terms.

Controller rights and obligations. The Controller may configure authorised users and roles, access and correct records, use exports, issue documented instructions, object to Sub-processors, request assistance, receive breach notices, audit compliance, and choose return or deletion. It must meet clause 4 and the shared responsibilities in Schedule 2.

Patients do not have Plinical accounts, cannot sign in to a patient portal, and cannot self-book or manage their records. A patient may receive a time-limited invoice link or clinic-generated communication without receiving a service account.

Schedule 2 Technical and Organisational Measures The measures below are binding minimum outcomes. They are applied proportionately to risk and may be implemented through the Processor's own controls and its contracted infrastructure providers.

Tenant and access control Processor measures. Separate clinic tenancy in application logic; authorisation checks scoped to clinic; Admin, Clinician and Receptionist permissions; unique staff accounts; no MTX staff access to clinic patient records or clinic workspaces; least-privilege access to permitted operational information and prompt revocation of internal access.

Controller responsibility. Assign minimum roles; keep user lists current; disable leavers; do not share accounts, passwords or clinic codes.

Authentication and sessions Processor measures. Use maintained authentication components; protect password and session material using industry-standard mechanisms; secure cookies/session controls; rate limiting and abuse controls appropriate to the assessed risks; restrict privileged operational access.

Controller responsibility. Use strong unique passwords; secure email accounts and endpoints; report suspected credential compromise promptly.

Encryption and secrets Processor measures. TLS for data in transit over public networks; encryption at rest for production databases, files and protected backups; managed secrets outside source code; rotation or revocation after suspected exposure. Document encryption coverage, key custody and the boundary at which application or provider services decrypt data; restrict and log privileged key and deployment operations. Clinic credentials do not by themselves establish end-to-end encryption or clinic-exclusive key custody.

Controller responsibility. Protect exports and downloaded files; use secure networks and approved devices.

Files, links and communications Processor measures. Store clinical documents, signatures and imported data in access-controlled storage; use application-authorised access or expiring links for patient-facing invoice delivery; minimise email/SMS payloads; provide ticket-and-reply support without staff access to clinic patient records or clinic workspaces.

Controller responsibility. Verify recipient details; avoid unnecessary health detail in email/SMS; do not forward expiring links insecurely.

Logging and monitoring Processor measures. Record relevant authentication, user action, security and administrative events; protect logs from unauthorised alteration; review alerts and investigate suspicious activity; configure Sentry in its Germany/EU organisation; scrub or exclude health data, credentials and message bodies before transmission; exclude session replay.

Controller responsibility. Review clinic audit information; notify the Processor of suspicious activity.

Availability and recovery Processor measures. Use resilient managed infrastructure; maintain risk-appropriate backup and recovery arrangements; document and periodically test restoration or continuity procedures; monitor service health.

Controller responsibility. Maintain local continuity procedures for urgent clinical work and retain exports where needed by professional rules.

Secure development Processor measures. Apply change control and code review proportionate to risk; manage dependencies and security patches; separate production from development/demo use; use synthetic data in demonstrations, public screenshots and development tests; test material security changes.

Controller responsibility. Use synthetic or fully redacted information for support and tests; do not provide production patient data or clinic credentials to support personnel.

Vulnerability management Processor measures. Monitor relevant vulnerabilities; triage by severity and exposure; remediate critical or high-risk issues within a risk-appropriate period; control production access; commission or perform periodic security testing appropriate to service maturity and risk.

Controller responsibility. Keep browsers, operating systems and endpoint protection current.

Incident response Processor measures. Maintain an incident process for detection, containment, evidence preservation, remediation, lessons learned and notifications under clause 7; keep escalation contacts current.

Controller responsibility. Keep notices email current; cooperate promptly; preserve relevant local evidence.

Personnel and suppliers Processor measures. Confidentiality commitments; data-protection/security instruction; the no-access boundary in clause 2.1; need-to-know operational information; due diligence and Article 28-equivalent contracts for Sub-processors; transfer safeguards where required.

Controller responsibility. Authorise Sub-processors under clause 9 and raise evidence-based objections promptly.

Deletion and disposal Processor measures. Deletion from active systems and downstream providers under clause 12; access restriction during retrieval; protected backup expiry without restarting clocks after restoration; secure disposal of media or provider-managed deletion; documented deletion confirmation on request.

Controller responsibility. Export required records before termination and securely delete unnecessary local copies.

Schedule 3 Service providers and authorised Sub processors Part A identifies clinic-data Sub-processors by service. The Processor shall maintain the exact contracting entities, account applicability and downstream suppliers in its controlled register and provide relevant details on request. Authorisation is subject to clauses 9 and 10, including permission for the data categories processed. Optional services operate only when enabled for the relevant purpose. Primary storage regions do not exclude support, control-plane or onward processing elsewhere.

Part A Clinic data Sub processors Provider and servicePurpose and dataConfigured location and boundary London (lhr1); global support/control plane Vercel application Application requests, clinic functions may apply. Health-data processing must be hostingand necessary operational telemetry. expressly permitted by the applicable contract.

London, UK. The applicable account contract Structured clinic, staff, patient, health, Neon databasedetermines the legal supplier and any appointment, invoice and audit records. permitted support or onward processing.

Washington, D.C., USA (iad1). Private storage, Clinical files, PDFs, signatures, uploads authorised access and expiring document links.

Vercel Blob and metadata.Health-data permission and lawful US transfer safeguards are required.

Ireland dispatch (eu-west-1); US Clinic-instructed email, recipients, account/metadata/log/API processing. Any Resendcontent where permitted, delivery health content or attachments require a metadata and logs.contract and transfer annex covering those categories.

Optional SMS: recipient telephone UK service with recipient-network routing. AI The SMS Worksnumber, minimal message and Optimiser and any per-message AI optimisation delivery/routing metadata.override shall remain disabled.

Germany/EU storage. Exclude special-category Optional scrubbed error and data, credentials, message bodies and session Sentryperformance diagnostics, technical replay; assess relevant support/onward identifiers and events. transfers.

Ireland (eu-west-1) as the production primary/read location. No health or clinical Optional rate-limit counters, short-lived Upstash Redispayloads; changes to replicas, failover or identifiers and technical metadata. processing locations are subject to clauses 6, 9 and 10 as applicable.

Part B Providers for MTX controller purposes Cloudflare Turnstile protects public clinic registration and uses limited browser/network signals and tokens, with global processing. MTX is controller for registration security; Cloudflare acts as processor for delivery and as a separate controller for improving bot detection. Form contents and clinical information must not be sent to Turnstile. This is not blanket authorisation to use clinic patient data for a vendor's own purposes.

Stripe handles payments for clinics' subscriptions to MTX, using billing contacts, payment information and transaction/security metadata. MTX acts as controller for that billing. Stripe has processor and independent-controller functions under its applicable terms. Stripe is not a patient-payment integration or a Sub-processor of

clinic clinical records in this scope. Do not send patient records, clinical descriptions or patient identifiers in Stripe metadata.

Schedule 4 Restricted Transfer Safeguards This Schedule is a precautionary contractual framework. It becomes operative between the Controller and Processor only where their direct transfer is a Restricted Transfer without another valid mechanism. It does not replace the Processor's duty to put a separate mechanism in place with an overseas Subprocessor.

A UK restricted transfers A.1 Where UK Data Protection Laws apply and the Controller-to-Processor transfer requires an appropriate safeguard, the parties incorporate the EU Standard Contractual Clauses described in Part B and the following mandatory wording: Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

A.2 For Part 1 of the Approved Addendum: Table 1 consists of the party identities, addresses, contacts and acceptance details in this DPA and the Order and electronic acceptance record described in Schedule 5; the start date is the Effective Date. Table 2 identifies the Approved EU SCCs as the 2021 SCCs, Module Two (controller to processor), with clause 7 docking applying, clause 9 option 2 general authorisation and a 15-calendar-day notice period, and the clause 11 optional redress provision not applying. Table 3 consists of Schedules 1 and 2, Part A of Schedule 3 and the party details in Schedule 5. In Table 4 both the importer and exporter may end the Addendum as permitted by its mandatory clauses. The ICO Approved Addendum is incorporated without modification except as it permits.

A.3 The exporter is the Controller and the importer is the Processor. The frequency is continuous or event-driven for the term. Special Category Data and safeguards are described in Schedules 1 and 2. The competent authority is the ICO. Nothing in this DPA changes the Approved Addendum beyond changes it permits.

B EEA restricted transfers B.1 Where the EU GDPR applies and the direct Controller-to-Processor transfer requires an appropriate safeguard, the parties incorporate the European Commission Standard Contractual Clauses adopted by Decision (EU) 2021/914, Module Two (controller to processor), to the extent legally available for the transfer. Clause 7 applies; clause 9 uses option 2 with 15 calendar days' notice; the optional redress provision in clause 11 does not apply. If that instrument is not legally available for the transfer, the parties shall put another valid mechanism in place before the transfer.

B.2 For clause 17, the governing law is the law of the EEA state where the exporter is established if that law permits third-party beneficiary rights; otherwise Irish law. For clause 18, the courts are those of that same state or, where Irish law applies, Ireland. The competent Supervisory Authority is determined under clause 13 of the SCCs.

B.3 Annex I.A is completed by the party identities, addresses, contacts, roles and acceptance details in this DPA and Schedule 5, including the incorporated Order and electronic acceptance record. The Controller's relevant activity is providing clinic services and using Plinical for the purposes in Schedule 1; the Processor's activity is providing Plinical on the Controller's behalf. Annex I.B and Annex II are completed by Schedules 1 and 2. Annex I.C is determined under clause B.2 and SCC clause 13. Annex III, where required, is Part A of Schedule 3 together with the relevant entity and contact details supplied under that Schedule. Before relying on these clauses, the parties shall record the applicable Supervisory Authority and any further annex information required for the particular transfer. Electronic acceptance under Schedule 5 constitutes signature for incorporated transfer clauses to the extent permitted by those clauses.

C Transfer assessment and supplementary measures C.1 Before relying on contractual safeguards, the responsible exporter shall complete and document any required data-protection test or transfer risk assessment, considering the destination law and practice, data sensitivity, access likelihood, onward transfers and effective remedies.

C.2 The parties shall implement supplementary technical, contractual or organisational measures identified as necessary, which may include strong encryption, minimisation, access separation, short retention, transparency reporting and challenge of disproportionate government requests.

C.3 If an applicable safeguard is invalidated or no longer sufficient, the parties shall promptly suspend the affected Restricted Transfer unless and until a lawful alternative is implemented.

Schedule 5 Party details and electronic acceptance A Processor details Legal entity: MTX STUDIO Ltd, trading as Plinical. Company number: 15856187. Registered office:

Bartle House, 9 Oxford Court, Manchester, England, M2 3WQ.

Privacy, breach and legal notices:support@plinical.com. Data Protection Officer contact: Theodoros Mentis, th.mentis@mtxstudio.com.

B Controller details The Controller is the legal person identified in the accepted Order and its electronic acceptance record.

Those records form part of this DPA and identify its legal name, business type, registration number where applicable, registered or principal business address, clinic or trading name, notices email and the accepting representative's name and role. For a sole trader, the Controller is the individual carrying on the business; for a partnership, the Order must identify the legal partnership or partners as applicable. A clinic trading name does not replace the contracting legal identity.

The Controller's account and notices email is its privacy and breach contact unless it has nominated a separate contact in the Order or account. The Controller shall keep these details accurate and promptly notify the Processor of changes. Updating contact details does not change the identity of the contracting party.

C Acceptance and retained agreement The Processor offers this DPA as part of the Agreement. By affirmatively accepting the Order and Agreement incorporating Plinical Data Processing Agreement version 2.2, the accepting representative confirms authority to bind the identified Controller. Both parties are bound from the Effective Date under clause 2.3. No separate signature page or manual completion of this document is required.

The Processor shall retain a durable record identifying the Controller, the authorised representative, the accepted Order, this DPA version, the exact text made available and the date and time of acceptance. It shall make a downloadable or otherwise retainable copy of the accepted DPA and Order available to the Controller. Acceptance evidence shall relate to the version actually presented and accepted.

This DPA has document date 21 October 2026 and version 2.2. Its document date is not a substitute for the customer-specific Effective Date. Later versions apply to an existing Controller only through the variation provisions of the Agreement and this DPA. The acceptance record remains linked to the version originally accepted.