

Plinical Company Led Completion

Version 1.0 | Document date 16 September 2026

This statement explains how MTX STUDIO Ltd manages Plinical's legal documentation, data-protection responsibilities and service-release decisions. Company management is accountable for the decisions it makes. Completion requires evidence that the relevant legal, contractual and technical requirements are met.

This edition applies from publication as a public information statement. The company records individual operational decisions separately. Publication of this statement does not certify completion of those decisions or confer regulatory approval.

1 Company and scope

1.1 Plinical is operated by **MTX STUDIO Ltd**, company number **15856187**, registered in England and Wales. Our registered office is Princess House The Square, 3rd Floor, Shrewsbury, Shropshire, England, SY1 1JZ. In this statement, **we**, **us** and **our** mean MTX STUDIO Ltd.

1.2 Plinical provides clinic-management software to UK clinic businesses and self-employed professionals. This statement describes company governance and the conditions for completing a service release. The accepted Order, SaaS Terms and Data Processing Agreement govern each customer relationship. This statement does not amend them or waive any legal requirement.

2 Company decisions and independent advice

2.1 Christos Mentis, CEO and Director, is the company decision owner for the completion process. Management must identify the authorised decision-maker, evaluate the evidence, determine the permitted release scope and record its reasons. Developers and operational personnel implement decisions within their documented authority and supply evidence of the actual result.

2.2 Theodoros Mentis is our designated Data Protection Officer (**DPO**). The DPO advises and monitors independently, including on data protection impact assessments (**DPIAs**), and acts as a contact for individuals and the Information Commissioner's Office (**ICO**). Management retains responsibility for operational decisions and the company's compliance.

2.3 An appropriately supported company process may be carried out in-house. Relevant specialist advice is obtained where the issue requires it. An external solicitor's signature is not a general prerequisite for completing a DPIA, and neither an internal signature nor external advice replaces compliance with the applicable requirements.

3 DPO independence and allocation of duties

3.1 DPO arrangements must provide sufficient expertise, time, resources and direct access to the highest level of management. The company must involve the DPO in relevant matters, protect confidential communication, and must not instruct the DPO's conclusions or penalise the performance of DPO duties.

3.2 Other duties must be compatible with independent monitoring. Where a responsibility determines the purposes or means of processing, or creates incompatible self-assessment, it must be reassigned or another competent, conflict-free DPO arrangement established. Any transfer of duties must take effect in actual authority, permissions and working practices. A job title or countersignature is insufficient evidence.

3.3 The internal governance record must identify the allocation, effective date, retained duties and supporting implementation evidence. Earlier decisions require sufficiently independent assessment where the DPO had an operational role. The company records DPO advice and any justified decision to depart from it. ICO registration alone does not establish that these arrangements are effective.

4 Technical evidence and clinic access

4.1 Technical confirmation must identify the relevant build and environment and demonstrate the controls that apply there. Evidence covers tenant separation, permissions, encryption, key and deployment administration, private file access, communications, logs, backups, restoration and deletion as relevant. Historical tests or a preview environment do not establish the current production state.

4.2 Clinic staff use their own authorised credentials. Under Plinical's operating model, MTX staff do not access clinic patient records or sign in to clinic workspaces. Support is provided through tickets and guidance. Hosted and automated processing may decrypt data to provide authorised functions; encryption in transit and at rest does not mean that only a clinic holds decryption keys. Technical controls must support the stated operating model.

4.3 Demonstrations and tests use synthetic patient information in an appropriately isolated environment. Encrypting copied patient records does not make them synthetic or anonymous. Live patient data in a Trial is permitted only where that use is enabled and the DPA's applicable security, supplier and transfer requirements are met. Evidence supplied for governance must exclude passwords, secret keys and unnecessary patient information.

5 Supplier permissions and international processing

5.1 Before a provider processes clinic data, the company must establish the applicable legal entity, service, account terms, processing purposes, permitted data categories, security arrangements and any required international-transfer mechanism. Health-related messages, documents and metadata must be assessed according to their actual content and context.

5.2 Permission must cover the intended processing under the binding supplier agreement. A general security statement, selected hosting region or encryption does not override a contractual restriction on health or other special-category data. Supplier arrangements must also support applicable notice, assistance, return, deletion and backup obligations under the DPA.

5.3 Where these requirements are not met, affected processing must be prevented. A restricted feature or alternative service may be used only after its own requirements are satisfied and the relevant information and contractual schedules are updated. A company release decision cannot waive a provider restriction or substitute for a lawful transfer mechanism.

6 Risk assessment and the release record

6.1 A required DPIA must address the actual processing, necessity, proportionality, risks to individuals and effective safeguards. The company seeks and records DPO advice. Where a required DPIA identifies high residual risk that cannot be reduced, the responsible controller must consult the ICO before the affected processing begins. MTX assists clinic controllers under the DPA.

6.2 The internal release record must identify the decision-maker, date, build, environment, permitted features and data, evidence relied upon, supplier and transfer arrangements, relevant DPO advice, DPIA outcome and any restrictions. It must distinguish completed actions from restrictions that still prevent particular processing. Any application setting used to enable a release must reflect that recorded decision.

6.3 For each clinic, the clinic remains controller of its clinical and patient records. It determines its lawful bases, clinical purposes, retention requirements and staff permissions. MTX acts as processor for hosted and automated operations on its instructions. Company completion records do not take over a clinic's own accountability or clinical decisions.

7 Public documents and customer acceptance

The public documents explain the following parts of the service. Each document identifies its own version and relevant date.

Document	Purpose
<u>SaaS Terms</u>	Subscription, trial, charges, renewal, cancellation and service responsibilities, together with the accepted Order.
<u>Data Processing Agreement</u>	Processing of clinic data, security, suppliers, transfers, assistance and return or deletion.
<u>Privacy Notice</u>	How personal data is used and shared, retention, individual rights and complaints.
<u>Cookie Policy</u>	Public website storage and access technologies, their purposes, duration and available controls.
<u>Legal Release Statement</u>	How legal documents, customer acceptance and service responsibilities fit together.
<u>DPIA Public Summary</u>	Public information about the service's data-protection impact assessment and safeguards.

7.1 Document publication, a company release decision and a customer's acceptance are separate events. The accepting person must have authority to bind the identified clinic business. Acceptance records must identify the legal customer, accepted document versions and date, and allow the customer to retain the agreement. Publishing a new document does not automatically replace an existing customer's accepted terms.

7.2 Privacy information must be supplied where required and technology choices must work where the relevant technology operates. A privacy or cookie notice does not itself provide consent or an objection mechanism. The public Cookie Policy describes the existing theme-storage controls; the light/dark toggle does not disable storage. Any required additional control must be implemented before relying on the relevant exception.

8 Changes and continuing accountability

8.1 Changes to features, data, providers, locations or controls require reassessment proportionate to their effect. The company updates the relevant records, instructions and public information, and follows contractual notice and variation requirements. Controls and obligations continue after a release; a previous decision does not cover materially different processing automatically.

8.2 Version 1.0. Document date: 16 September 2026. This statement replaces the earlier public information at this page when published. Original governance evidence and decision records are retained separately. Publication does not create a signature, DPO acknowledgement, implementation date or service-release decision.

9 Contact

9.1 For company, legal, privacy, security and support enquiries, contact support@mtxstudio.com or write to our registered office. Our ICO registration reference is ZC226522.

9.2 You may contact the DPO, Theodoros Mentis, directly at th.mentis@mtxstudio.com. Patients seeking action concerning their clinic records should contact their clinic. The [Privacy Notice](#) explains rights and how to raise a privacy complaint.