

Plinical Data Protection Impact Assessment

Public Summary

Version 1.0 | Document date 15 September 2026

This summary explains the privacy risks assessed for Plinical, the safeguards required to address them, and the responsibilities of MTX STUDIO Ltd and its clinic customers. Health-data processing requires effective safeguards and appropriate supplier permissions. This publication does not itself authorise that processing.

1 Purpose and assessment scope

Plinical is a clinic-management service operated by **MTX STUDIO Ltd**, company number **15856187**. It supports UK clinics and self-employed professionals, including those in Northern Ireland, with patients, appointments, clinical records, consent, referrals, invoicing, reports and communications.

The assessment covers the shared application, database, files, staff accounts, imports and exports, communications, suppliers, security, support, retention and data-rights assistance. It also covers MTX's separate business-contact, account-security and subscription-billing processing. Use is routine during the subscription and continues only for the applicable return, deletion or lawful retention period.

A DPIA is warranted because the platform is designed to hold confidential health records across multiple clinics, including records about children and other vulnerable people. Disclosure, alteration or unavailability can cause distress, discrimination, financial loss, loss of control or harm to care. Actual volumes, clinic workflows and patient populations affect the risk and must inform each deployment.

2 Who is responsible

Clinics are controllers of patient and clinical records: they decide why those records are used, who may access them, their clinical content and applicable retention. Each clinic must identify its Article 6 lawful basis and Article 9 condition for health data, provide privacy information and assess its own use of the service. Consent to treatment is not automatically data-protection consent.

MTX is a processor for hosted and automated functions carried out on clinic instructions under the [Data Processing Agreement](#). MTX is separately a controller for its own enquiries, account administration, subscription billing, security and legal-compliance processing, described in the [Privacy Notice](#).

Patients have no Plinical account, portal or self-booking facility in the assessed scope. Patients do not pay through Plinical; clinics record payments made elsewhere. Stripe supports clinic subscription billing. Automated clinical decisions, biometric identification, sale of clinic data, advertising use of clinic records and general-purpose AI training are outside the permitted scope.

3 Information and processing lifecycle

Information	Purpose and limits
Patient identity and contacts	Names, contact details, demographics and clinic identifiers support identification, scheduling and clinic communications. Clinics should collect only what their work requires.
Health and care records	Histories, medication, allergies, assessments, treatment plans, clinical notes, referrals and attachments support care documentation. These are special category data.
Consent and signatures	Forms, recorded choices and signature images document clinic processes. Signature images are not used for biometric identification.
Appointments and invoices	Scheduling, services, invoices and records of payments made elsewhere support clinic administration. Even without a diagnosis, context may reveal a health relationship.
Clinic staff and account data	Names, business emails, role assignments, authentication and security records support authorised access and service administration.
MTX subscription and operational data	Business identity, billing details, subscription status and minimised technical records support MTX's own service, billing and security duties. Patient records must not be sent to Stripe.

Collection and use. Authorised clinic users enter information, import CSV files and upload documents. The application processes these records within the clinic's workspace for scheduling, care documentation and administration. Imports must preserve the correct clinic, patient and source and be checked for errors and excessive information.

Storage and sharing. Structured records are stored in the database; files and generated documents use object storage. Authorised clinic users may view or export records. Clinic-selected recipients may receive communications, referrals or time-limited invoice links. Downloads create copies that the clinic must protect and manage.

Support and access. Under the stated operating model, MTX staff do not enter clinic workspaces or read patient records. Support is provided by ticket and reply with guidance. Clinics must use synthetic or fully redacted examples and must not send patient records, passwords or keys in support requests.

The automated service processes records to provide its functions. Encryption does not make this processing anonymous, and the assessment does not establish encryption controlled exclusively by the clinic. Key custody, automated decryption and supplier capabilities remain part of the security assessment.

4 Suppliers and international processing

The following map records the service architecture and owner-confirmed configuration. Optional services apply only when enabled. Locations identify the recorded main processing route; supplier access, metadata, backups and onward processing also require assessment.

Service	Recorded function and location
Vercel application	Application and server functions in London. The service processes clinic data to deliver the software.
Neon database	Structured clinic records in London. Tenant separation, access and recovery controls apply.
Vercel Blob	Files, PDFs and signature images in Washington DC, United States. Private storage and expiring delivery links are owner-confirmed.
Resend	Email dispatch in Ireland; metadata, logs, API and account records in the United States. Message context may reveal health information.
The SMS Works	Optional SMS delivery. The telecom route, location, retention and contractual scope must be established before use. The owner confirms AI Optimiser and overrides are disabled.
Sentry	Optional diagnostics with EU storage in Germany. The owner confirms clinical-data scrubbing; health payloads and session replay are excluded from the assessed use.
Upstash	Optional technical counters in Ireland. The owner confirms region configuration. Clinical payloads are excluded and retention must be limited to operational need.
Cloudflare Turnstile	Public-registration anti-abuse checks involving global browser and network signals. No clinical or form contents are intended. MTX is controller; Cloudflare has processor and separate controller functions.
Stripe	Clinic subscription billing, separate from patient invoicing and external patient payments. Provider payment operations may involve international processing. Its roles and transfers must be assessed for the actual service.

Auth.js is a self-hosted software library, rather than a separate hosting supplier. The assessed Fresha route is clinic-controlled CSV import, with no live API integration.

For restricted transfers, MTX must establish an applicable adequacy basis or valid contractual safeguards and complete the required transfer assessment or data protection test. A London application region does not make all processing UK-only. Supplier permission to handle health data is a separate requirement from transfer safeguards; section 9 explains the assessment finding.

5 Necessity and proportionality

Patient identity, care and scheduling information support the clinic's administration and recordkeeping. Eliminating all health data would prevent the assessed clinical-record function. This does not justify unrestricted collection: clinics must limit fields, attachments, messages and access to the relevant purpose and keep records accurate.

The assessment identifies less intrusive choices: use minimal message text and neutral subject lines; omit diagnoses and clinical narratives from operational telemetry; keep patient data out of subscription billing; use private, expiring document delivery; and use synthetic data for demonstrations and testing. Patient portals, patient payment processing and automated clinical decisions are excluded and require reassessment before introduction.

Clinic access must follow least privilege, separating administrative and clinical roles and promptly disabling leavers. Exports require authorisation and secure handling. Technical evidence must establish tenant isolation, file and link access, logging, secret protection, vulnerability management and recovery. These controls must be tested against the version and configuration used in service.

6 Retention rights and incidents

Retention. During a subscription, clinics determine lawful patient-record retention requirements and issue instructions under the DPA. On termination, DPA version 2.0 provides 30 days for retrieval or a return request, followed by active deletion without undue delay as specified there. Protected backup copies must be deleted no later than 90 days after active deletion. Restoration must reapply deletion restrictions and must not restart that period. Legally required retention is limited to the applicable duty and protected from other use.

Deletion must cover structured data, documents, generated files and relevant downstream copies. MTX's own billing, security and legal records follow the separate purposes and retention criteria in its Privacy Notice. The platform's exit periods do not replace a clinic's professional or statutory record-retention duties.

Individual rights. Patients should contact their clinic for access, correction, restriction, deletion or other requests concerning clinic records. MTX must route requests and assist the clinic under the DPA, using identity and tenant checks. Export and assisted workflows must cover relevant records and attachments while protecting other people's information. Rights concerning MTX's own controller processing may be raised directly with MTX.

Incidents. Under DPA version 2.0, MTX must notify an affected clinic without undue delay and within 24 hours of becoming aware of a personal-data breach, providing available facts and further information as it becomes available. MTX must support the clinic's assessment and response. The clinic remains responsible for its controller notifications, including any applicable regulator and affected-person notifications.

Supplier changes. DPA version 2.0 requires at least 15 calendar days' advance notice of a new or replacement Sub-processor and an opportunity to object. Supplier notice periods and technical switching arrangements must allow MTX to meet that obligation before the affected processing changes.

7 Risks and required safeguards

The register assesses harm to individuals. Likelihood and impact are each rated from 1 to 5 and multiplied: Low 1-4, Moderate 5-9, High 10-14 and Very High 15-25. A control may lower likelihood while leaving the severity of a possible disclosure or care failure unchanged.

The rows below preserve risks R1-R24 from the original assessment and add R25-R26. They summarise the measures needed to address each risk. They do not state that every measure has been independently verified. Original forecast scores are not presented as measured or accepted residual scores.

Risk	Potential harm	Required safeguards
R1 Tenant separation	One clinic receives another clinic's records.	Enforce clinic scope in queries, APIs, files and exports; perform negative access tests and independent checks.
R2 User accounts	Stolen credentials or excessive permissions expose records.	Least privilege, strong authentication and session controls, rate limiting, access reviews and rapid leaver removal.
R3 Record integrity	Wrong, missing or altered data affects care.	Validate records, preserve provenance and audit trails, support correction, test concurrent changes and recovery.
R4 Exports	Downloaded records reach unauthorised people.	Restrict and log exports, minimise scope and provide secure-download and local-retention guidance.
R5 Communications	Wrong recipients or excess detail expose confidential care.	Verify recipients, minimise content, use safe templates and check referral and retry workflows.
R6 Document links	A shared, guessed or persistent link exposes documents.	Private storage, strong link tokens, enforced expiry, authorisation, revocation and access testing.
R7 Diagnostics	Logs or support tickets disclose clinical data or secrets.	Allowlist or scrub diagnostic fields; exclude clinical content, credentials and replay; test actual payloads.
R8 Technical cache	Cached content or region changes widen exposure.	Use short-lived technical counters, exclude health data and verify regions, expiry and failover.
R9 Imports	Wrong-patient, wrong-clinic or excessive records affect privacy or care.	Validate files and schema, bind imports to the clinic, preview content and support duplicate checks and rollback.
R10 Signatures	Images are reused, over-retained or used for identification.	Limit purpose, access and retention; prohibit biometric matching in the assessed service.
R11 Availability	Outage or failed recovery interrupts access to care records.	Test backups and restoration, define recovery objectives and provide clinic downtime and reconciliation procedures.
R12 Retention	Records remain beyond the permitted purpose or period.	Apply clinic instructions, verified active deletion, backup expiry and narrowly controlled legal-retention exceptions.
R13 Rights	Requests fail or disclose another person's records.	Verify identity and clinic, route requests promptly and test complete, controlled export and correction workflows.

7 Risks and required safeguards continued

Risk	Potential harm	Required safeguards
R14 Operational access	Misuse of infrastructure, credentials or keys bypasses access boundaries.	Maintain the no-staff-access support model; establish actual key and service capabilities; restrict and monitor operational privileges.
R15 Test material	Real patient data appears in demonstrations or screenshots.	Use synthetic or irreversibly anonymised material; separate environments and inspect public and test assets.
R16 Secondary use	Records are reused for advertising, sale or AI training.	Enforce contractual and technical purpose limits, disable conflicting vendor features and assess any proposed new use.
R17 Breach response	Delayed detection or notice prevents timely protection.	Monitor incidents, maintain escalation contacts, preserve evidence and test the 24-hour notification process.
R18 Vulnerable people	Disclosure or confusing access harms children or vulnerable patients.	Use accessible notices, clinic-led representative checks, minimal communications and appropriate access controls.
R19 Transfers	International processing lacks effective protection or lawful coverage.	Establish the actual route, supplier health-data permission, transfer basis, assessment and necessary supplementary controls.
R20 Supplier changes	New locations, features or recipients alter protection.	Maintain the supplier inventory, monitor changes, reassess risk and make the 15-day clinic notice process workable.
R21 Bot protection	Registration checks collect excessive information.	Limit Turnstile to necessary signals, exclude form contents, assess global processing and explain the roles and purposes.
R22 Email metadata	Logs and delivery records reveal patient relationships.	Minimise content and metadata, restrict retention and access, and match supplier contracts to the actual data.
R23 Security flaws	Vulnerabilities or leaked secrets enable unauthorised access.	Review code and dependencies, scan for secrets, patch promptly, rotate credentials and test the deployed service.
R24 Clinical reliance	Users rely on incomplete records or software instead of professional judgement.	Explain the service boundary, support data-quality checks and train users in downtime and reconciliation procedures.
R25 Subscription billing	Billing errors or excess metadata expose identity or financial details.	Keep patient data out of Stripe, restrict billing roles, verify subscription linkage and assess payment-provider processing.
R26 Privacy governance	Conflicting duties weaken challenge, risk decisions or rights handling.	Separate operational decisions from independent DPO advice; document duties, implementation, advice and accountable decisions.

Risk acceptance must rely on actual configurations, contracts, tests and operating evidence. A forecast cannot establish that risk has fallen. Severe potential harm must remain in the impact assessment unless a specific, supported reason demonstrates that the harm itself has been reduced.

8 Accountability and consultation

MTX management is responsible for operational decisions, implementation and lawful risk acceptance. The role of the Data Protection Officer, **Theodoros Mentis**, is to advise and monitor independently. The company has selected a role allocation placing product, hosting, security and supplier decisions with **Christos Mentis**, CEO and Director. Its operation in practice and the independence of advice must be evidenced separately from adoption of the allocation.

Clinic, clinician, reception and patient or representative perspectives should inform the assessment where appropriate. Consultation should address access, confidentiality, messages, rights, accessibility and continuity of care. Actual feedback and resulting decisions must be recorded; a decision not to consult a group needs a specific reason. This publication does not report completed stakeholder consultation or independent DPO advice.

9 Assessment findings and processing conditions

The assessment identifies a credible need for the service and material risks requiring effective safeguards. Owner confirmations cover private files and expiring links, EU diagnostics and scrubbing, Ireland cache configuration, disabled SMS AI features and the contractual notification and deletion capabilities. These confirmations are part of the evidence; they are distinct from current production test results and account-specific contractual records.

Health-data permission remains a material issue. Vercel's published DPA restricts sensitive or special category customer data, while Resend's published DPA describes sensitive-data transfers as not applicable. Account-specific permission or a verified alternative processing route must resolve the actual health-data use. Encryption, generic supplier terms and the availability of transfer clauses do not by themselves resolve that issue.

The assessment record does not establish a completed, evidence-backed residual-risk acceptance for live clinical processing. Supplier health-data coverage, the applicable transfer arrangements, control effectiveness and independent privacy advice must support that decision. Affected live health-data processing must not begin until the mandatory prerequisites are satisfied. Publishing this summary does not record a management signature or regulatory approval.

Where a required DPIA identifies high risk remaining despite mitigation, the relevant controller must consult the ICO before the processing proceeds. MTX must assist clinic controllers and fulfil that obligation for its own controller processing where applicable. An internal acceptance decision cannot waive prior consultation. See ICO guidance on concluding a DPIA.

10 Maintenance and contact

This public summary accompanies the original assessment dated 19 August 2026 and subsequent updates. It replaces the public information at this page on publication; the underlying assessment and decision history remain retained. Reassessment is required before material changes to features, data, scale, suppliers or locations, following significant incidents, and no later than 19 August 2027.

Privacy, security and assessment enquiries: support@mtxstudio.com. **DPO:** th.mentis@mtxstudio.com. Clinics may request supporting information through the DPA information and audit process. Patients should direct clinic-record requests to their clinic and may raise privacy concerns with the ICO.

Registered office: MTX STUDIO Ltd, Princess House The Square, 3rd Floor, Shrewsbury, Shropshire, England, SY1 1JZ.