Ensuring Secure Data Management and Patient Privacy

Inato's Patient Pre-Screening Tool is designed with comprehensive safeguards to protect patient privacy, support site compliance, and foster sponsor trust. Each party — Inato, the research site, and the sponsor — has a clearly defined role in safeguarding patient data, reinforced by legal agreements and industry-standard protocols. Inato processes patient data in compliance with HIPAA, GDPR, ISO 27001, and HDS (Hébergeur de Données de Santé).

Patient Authorization

- Before accessing any data, Inato ensures research sites have the requisite authorization to share patient data. Authorization is obtained via the site's standard workflow, with contractual assurance to Inato.
- In the U.S., a Business Associate Agreement (BAA) outlines data-handling responsibilities for both parties.
- Outside the U.S., Inato acts as a data processor on behalf of the site (data controller), under a Data Processing Agreement (DPA).

Data Handling & De-identification

- Medical Record Processing: Site CRCs upload patient records to Inato's platform. Records are de-identified using the Google Cloud Platform Data Loss Prevention (GCP DLP) API.
- De-identification Standards: Identifiers like names, addresses, and contact details are removed. Minimal data (e.g., month/year of relevant dates, patient age) is retained to ensure accurate eligibility assessments. Site users may add patient names for internal tracking; all such data is redacted for Sponsor and Inato staff.
- File Storage: The original file is never stored in viewable form. Only de-identified clinical data is retained, held under a random identifier in encrypted Google Cloud storage.
- Platform Isolation: Each site operates in its own isolated environment — data is completely invisible to any other site on the platform.

AI Infrastructure & HDS Compliance

- Patient data stays inside Inato's Google Cloud projects. We use Google's Gemini models to assess eligibility, so patient data never leaves our Google Cloud environment.
- This architecture enables HDS compliance — the highest French health-data hosting standard, required for processing patient data in France and many other jurisdictions.
- Higher accuracy: The Gemini-based pipeline handles more complex eligibility scenarios, with ~10% higher accuracy than the prior system on our internal benchmark of the most difficult cases.
- Built to scale: A robust orchestration layer (powered by Temporal, the same technology used by leading enterprises) supports clinical-scale patient volumes reliably.

Third-Party Vetting & Integration

- All vendors are vetted against HIPAA, GDPR, and ISO 27001 standards. Where applicable, only de-identified data is shared, and vendors may not use data beyond Inato's defined purpose.
- Google Cloud (incl. Gemini) — supports de-identification, secure storage, and eligibility assessment, with no identifiable data retained.
- Inato conducts daily security checks via Drata, annual third-party penetration tests, and maintains HIPAA and ISO 27001 certification renewed yearly.

Patient Data Security

- Data Encryption: All data is encrypted in transit and at rest using AES-256.
- Logical Access Control: Access is restricted to authorized site personnel. Inato employees cannot view identifying information.
- Network Security: Google Cloud Armor protects against external threats including DDoS attacks.

Risk Management

- Pseudonymization: All medical records are pseudonymized prior to processing and stored under random identifiers in a secure Google Cloud bucket.
- Risk Assessments: Ongoing assessments identify potential threats (e.g. unauthorized access), with safeguards including strict access controls and full logging.

inato

Ensuring Secure Data and Patient Privacy

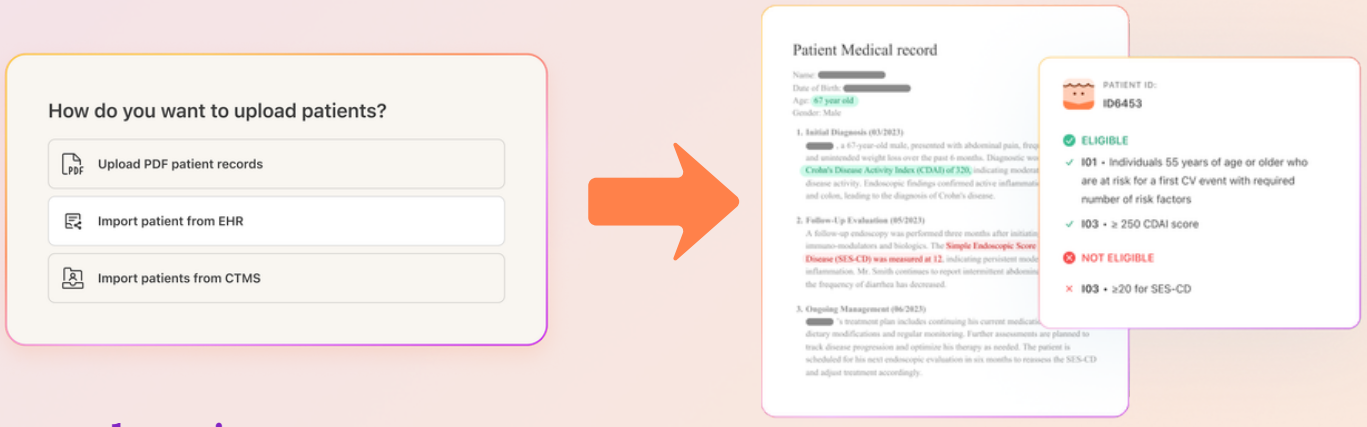
How you upload patient records:

Option 1: Manual Upload *(no integration required)*

- Site staff upload PDF patient chart, chart does not need to be redacted prior to upload
- Inato's AI redacts records as soon as they are uploaded and prior to being reviewed
- Patients who best match the trial needs are identified via Inato's AI review
- Only the site team decides which patients to contact or move to full screening

Option 2: EHR/CTMS Integration

- Inato securely connects to the site EHR/CTMS system to automatically pull redacted patient records
- Inato's AI redacts records as soon as they are pulled from the EHR/CTMS and prior to being reviewed
- Patients who best match the trial needs are identified via Inato's AI review
- Only the site team decides which patients to contact or move to full screening
- Inato can automatically sync and upload new patient records once EHR sync is turned on



How we keep it secure

- PHI Storage: Inato securely stores Protected Health Information (PHI), including structured data such as patient names and contact details. The system only retains de-identified clinical data extracted from the record, held in an encrypted Cloud storage environment.
- Medical Record Redaction: All records undergo automated redaction prior to any AI processing, ensuring data used for prescreening excludes identifiable information.
- AI Processing on Google Cloud: Eligibility is assessed by Google Gemini models running inside Inato's Google Cloud projects — patient data never leaves our cloud environment, enabling HDS compliance for France and beyond.
- Inato meets the same rigorous security and regulatory standards as an EHR/CTMS vendor.
- Inato complies with leading standards: HIPAA, ISO 27001, GDPR
- Inato uses providers and services in Europe that are HDS certified
- HIPAA-compliant de-identification via trusted tools (Google Cloud's DLP service).
- Patient data is encrypted at all times (in transit and at rest); site data is completely invisible to any other site on the platform.

Scan to view how we stay compliant