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, and other applicable privacy laws, as well as contractual agreements established with research sites.

Patient Security

- Before accessing any data, Inato ensures research sites have the requisite authorization to share patient data with Inato. Such authorization may be obtained via the site's standard authorization workflow. Research sites must provide contractual assurance to Inato that appropriate authorization is in place before disclosing any data to Inato.
- In the U.S., a Business Associate Agreement (BAA) may be executed outlining the data handling responsibilities of both parties.
- Outside the U.S., Inato acts as a data processor on behalf of the site as data controller. The parties execute a data processing agreement (DPA) outlining processing instructions for Inato.

Data Handling and De-identification

Inato processes data solely in accordance with the research site's instructions and limits processing to the minimum necessary to achieve the project's objectives. We adhere to the following process:

- **Medical Record Processing**: A site's CRCs upload patient medical records to Inato's platform. These records are de-identified using the Google Cloud Platform's Data Loss Prevention (GCP DLP) API.
- **De-identification Standards**: Identifying information such as names, addresses, and contact details are removed. We retain the minimal necessary data (e.g., month/year of relevant dates and patients' exact ages) to ensure accurate trial eligibility assessments.
- **Data Minimization**: Only the data necessary for evaluating trial eligibility is processed. All identifying information, medical records, and patient comments are fully redacted for Inato employees and sponsors

Site users can add patient names for easy internal tracking and follow up. For authorized Sponsor and Inato staff who require visibility into site usage, all data is redacted.

Third-Party Vetting and Integration

Inato uses trusted third-party vendors to support data processing. All vendors are carefully vetted and required to meet security, privacy, and compliance standards, including HIPAA and ISO 27001. When applicable, only de-identified data is shared, and vendors are prohibited from using the data for any purpose beyond what Inato defines.
Examples include (but are not limited to):

- OpenAI – Processes de-identified records to assess trial eligibility, with no identifying data stored or retained.
- Google Cloud – Supports de-identification and secure storage, without retaining identifiable information.

Inato conducts daily security checks via Drata, annual third-party penetration tests, and maintains HIPAA and ISO 27001 certification renewed yearly to ensure continuous data protection.

Patient Data Security

Inato employs industry-standard measures to ensure the secure handling of de-identified patient data throughout its lifecycle:

- **Data Encryption**: All data is encrypted both at rest and in transit using AES-256 encryption.
- **Logical Access Control**: Access to patient data is restricted to authorized personnel at clinical research sites. Inato employees do not have access to view identifying information.
- **Network Security**: We utilize Google Cloud's security features, such as Cloud Armor, to defend against external threats like DDoS attacks.

Risk Management

Inato takes a proactive approach to identifying and mitigating risks associated with patient data processing:

- **Pseudonymization of Medical Records**: To further protect patient privacy, all medical records are pseudonymized before being processed. These records are stored under random identifiers in a secure Google Cloud storage bucket.
- **Risk Assessments**: We conduct ongoing risk assessments to identify potential threats, such as unauthorized access, and implement appropriate safeguards, including strict access controls and logging.

inato

Ensuring Secure Data and Patient Privacy

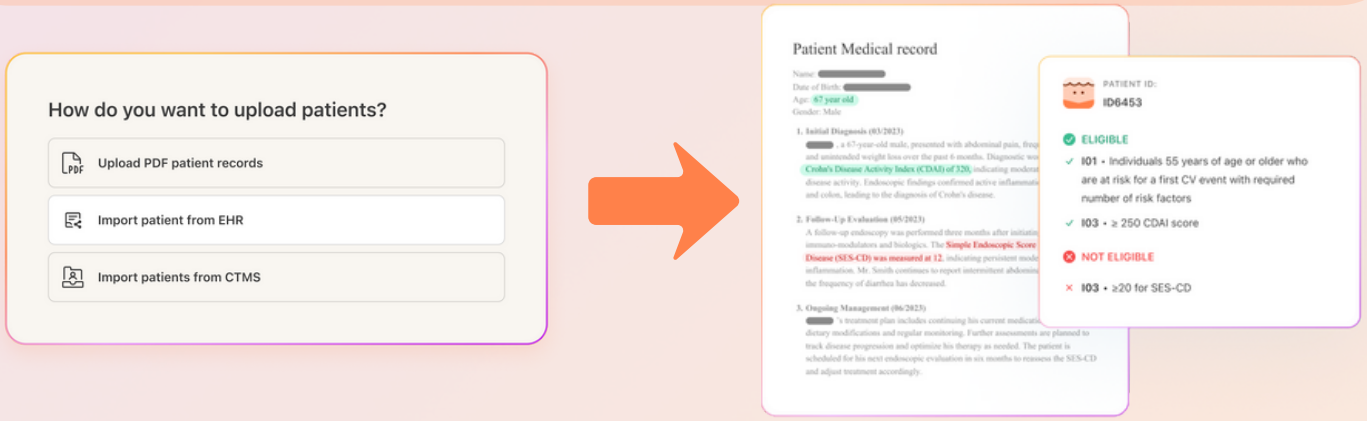
How you upload patient records:

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 Integration

- Inato securely connects to the site EHR system to automatically pull redacted patient records
- Inato's AI redacts records as soon as they are pulled from the EHR 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, when provided via EHR integration and with site authorization
  - PHI is automatically redacted and never visible to Inato employees or sponsors. This is enforced through system-level safeguards and user access restrictions.
- **Medical Record Redaction:** All medical records undergo automated redaction prior to any AI processing, ensuring that data used for prescreening excludes identifiable information
- Inato meets the same rigorous security and regulatory standards as an EHR vendor
- Inato complies with leading standards (HIPAA, ISO 27001, GDPR)
- HIPAA-compliant de-identification via trusted tools (Google Cloud's DLP service)
- Patient data is encrypted at all times (in transit and at rest)

What we never do

- Inato employees and sponsor users can not view or share personal health information (PHI)
- Inato does not use site patient data for anything beyond the site's trial
- Inato does not let unauthorized users (including sponsors) access patient names or contact info

HIPAA ISO 27001 Certified GDPR COMPLIANT

Click to view how we stay compliant

inato