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 alignment with HIPAA, other applicable privacy laws, and in accordance with 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 would act as a data processor on behalf of the site as data controller. The parties would 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. No identifying information is stored by Inato after processing. No medical records are retained by Inato.

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.

We regularly review our vendors to ensure continued compliance. A full list is available upon request.

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 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