Data Processing Agreement (DPA)

This Data Processing Agreement ("DPA") is entered into by and between:

1. **_____** ("**Controller**"), a healthcare organization or technical supplier subject to the General Data Protection Regulation (GDPR), with its principal place of business at _____,

   and

2. **Inquira Technologies B.V.** ("**Processor**" or "**InquiraHealth**"), a Dutch private limited liability company with its principal place of business at Spangesekade 97D, 3027 GR, Rotterdam, The Netherlands registered with the Dutch Chamber of Commerce under number **95495460**,

(each a "**Party**" and collectively the "**Parties**").

This DPA is annexed to and forms an integral part of any underlying agreement or contract for services ("**Master Agreement**" or "**Service Agreement**") between the Parties. In the event of conflict between this DPA and any other agreement, **this DPA** shall prevail with regard to data protection and privacy obligations.

1. Purpose and Scope

1.1 **Purpose**. This DPA sets forth the terms under which Processor will process Personal Data (defined below) on behalf of Controller for the purpose of providing **Conversational AI services** and related functionalities (the "**Services**").

1.2 **GDPR Compliance**. This DPA is intended to fulfill the requirements of Article 28 of the **General Data Protection Regulation (EU) 2016/679 ("GDPR")**, as well as any applicable national laws.

2. Definitions

For the purposes of this DPA, the following definitions apply:

- **"GDPR"**: Regulation (EU) 2016/679, including any implementing and related national legislation.

- **"Personal Data"**: Any information relating to an identified or identifiable natural person, as defined in GDPR Article 4(1).

- **“Processing”** (and its variations “Process,” “Processes,” “Processed”): Any operation or set of operations performed on Personal Data, whether or not by automated means (GDPR Article 4(2)).

- **“Data Subject”**: An identified or identifiable natural person about whom Personal Data is processed.

- **“Sub-Processor”**: Any third party engaged by Processor who receives Personal Data from Processor for the purpose of Processor’s provision of the Services to Controller.

- **“EEA”**: European Economic Area.

Any capitalized terms not defined herein shall have the meaning given to them under the GDPR.

3. Subject Matter and Duration

3.1 **Subject Matter**. Processor will process Personal Data solely for the purpose of performing the Services described in the Master Agreement, including but not limited to scheduling, voice or chat interactions and other Conversational AI workflows.

3.2 **Duration**. The Processing will continue until the Master Agreement expires or is terminated, or until all Personal Data is deleted in accordance with Section 13 below.

4. Categories of Data and Data Subjects

4.1 **Categories of Personal Data**. The types of Personal Data that Controller may submit to the Services (depending on the workflow configuration) may include, but are not limited to:

- **Patient Identifiers**: Name, phone number, date of birth, national ID number, patient ID, email address, etc.

- **Appointment Details**: Scheduled times, dates, locations, clinics/doctors, department names, appointment notes.

- **Medical Information**: Collected symptoms, triage data, medication adherence, diagnostic details, or other health-related information if provided by Controller or the Data Subject.

- **Interaction Data**: Call recordings, chat messages, transcripts, uploaded files (e.g. medical documents).

4.2 **Data Subjects**. The Data Subjects may include:

- Patients (including prospective or former patients)
- Healthcare staff or other individuals, as relevant to the workflows

4.3 **Controller Responsibility**. Controller acknowledges that it determines the scope and purpose of the Personal Data collected. Processor has no control over the types of Personal Data submitted by Controller, nor the extent to which such data is shared.

5. Obligations of Controller

5.1 **Lawfulness of Processing**. Controller warrants that it has obtained and maintains all necessary consents or other lawful bases required under the GDPR (and any other applicable laws) to collect and process Personal Data via the Services.

5.2 **Instructions**. Controller will provide documented instructions to Processor, and Processor shall process Personal Data only in accordance with these instructions. Controller shall ensure that such instructions comply with GDPR and any other applicable laws.

5.3 **Accuracy and Minimization**. Controller is responsible for ensuring the Personal Data it provides is accurate, up to date, and limited to what is necessary for the defined purposes.

6. Obligations of Processor

6.1 **Processing Only on Instructions**. Processor shall process Personal Data solely for the purposes set forth in this DPA and the Master Agreement, and strictly in accordance with Controller's instructions, unless required otherwise by law.

6.2 **Confidentiality**. Processor shall ensure that all persons authorized to process Personal Data are bound by appropriate confidentiality obligations.

6.3 **Technical and Organizational Measures**. Processor shall implement and maintain appropriate technical and organizational measures (TOMs) to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. These measures are further detailed in **Annex 2** (Security Measures), which may be attached or referenced via the Processor's Trust Center.

6.4 **Assistance**. Processor shall assist Controller, insofar as feasible, in meeting Controller's obligations under GDPR Articles 32 to 36, taking into account the nature of the processing and the information available to Processor.

6.5 **Data Subject Requests**. Processor shall, to the extent legally permitted, promptly notify Controller if it receives a request from a Data Subject to exercise rights under GDPR (e.g., access, rectification, erasure). Processor shall not respond to such requests directly unless authorized by Controller.

6.6 **Deletion or Return of Data**. Upon termination or expiration of the Master Agreement, Processor shall, at Controller's choice, either return or securely delete all Personal Data in its possession, unless further storage is required by law.

7. Sub-Processors

7.1 **Authorized Sub-Processors**. Controller provides a general authorization for Processor to use Sub-Processors to fulfill the Services. A list of current Sub-Processors is maintained at: inquira.health/en/legal/sub-processors
This list includes the identity of each Sub-Processor and its location.

7.2 **Notification of Changes**. Processor will update its Sub-Processor list in a timely manner. Controller may sign up for notifications or periodically review the list for updates. Controller's continued use of the Services is deemed acceptance of the new Sub-Processors.

7.3 **Sub-Processor Obligations**. Processor shall ensure that any Sub-Processor is bound by contractual obligations no less stringent than those set forth in this DPA, including appropriate data protection and confidentiality obligations.

8. International Data Transfers

8.1 **Data Hosting Location**. Processor shall store and process all Personal Data within the European Economic Area (EEA) (or such other agreed hosting region in Europe) and shall not transfer or allow access to any Personal Data (including any patient or sensitive information) from outside that region unless specifically authorized in writing by Controller. For the avoidance of doubt, patient or sensitive information shall remain in the EEA at all times, except as expressly permitted by this Agreement or required by Union or Member State law.

8.2 **Limited Exceptions**. Controller acknowledges that Processor may transfer non-patient data (e.g., billing or customer account information) outside the EEA solely for legitimate business purposes (e.g., invoicing through Stripe in the U.S.). Any such transfers shall be strictly limited to the minimum necessary data required for such services.

8.3 **Safeguards**. Where any transfer of Personal Data outside the EEA is necessary (and lawfully authorized under Clause 8.2 or otherwise), Processor shall ensure appropriate safeguards are in place, such as Standard Contractual Clauses (SCCs) or another lawful transfer mechanism in compliance with GDPR. Processor shall provide evidence of such safeguards to Controller upon request.

8.4 **Sub-processor Obligations**. Processor shall require all Sub-Processors who may handle Personal Data (whether within or outside the EEA) to abide by equivalent data protection obligations as set forth in this DPA. In particular, no Sub-Processor is authorized to transfer Personal Data outside the EEA (or other agreed region) without Processor's prior written approval and compliance with GDPR transfer requirements.

8.5 **Notification of changes**. If Processor intends to make any material change to its data transfer practices that could affect Controller's data (e.g. engage a new Sub-Processor located outside the EEA), Processor shall notify Controller in advance. Controller may object to such changes if it reasonably believes they violate applicable data protection laws or this DPA.

9. Security and Personal Data Breach Notification

9.1 **Security Measures**. Processor shall implement and maintain security measures in accordance with **Annex 2 (Security Measures)**.

9.2 **Personal Data Breach**. In the event Processor becomes aware of a **Personal Data Breach** (as defined in GDPR), Processor shall notify Controller **without undue delay**. Processor's notification shall at least:

- Describe the nature of the breach
- Indicate the likely consequences
- Propose the measures taken or proposed to address the breach

Controller is responsible for complying with any notification obligations toward supervisory authorities and Data Subjects under GDPR Articles 33 and 34.

10. Audit Rights

10.1 **Audits**. Controller (or an appointed auditor) has the right to audit Processor's compliance with this DPA, subject to reasonable prior notice (e.g. at least 30 days) and during normal business hours.

10.2 **Limitations**. Audits shall not unreasonably interfere with Processor's business operations. Controller is responsible for any costs associated with the audit. Audits will not exceed one per year, unless required by a competent data protection authority or there has been a material data breach.

10.3 **Results**. Processor shall cooperate in good faith and provide all necessary documentation or assistance. Any audit results shall be treated as confidential information.

11. Liability

11.1 **Liability Cap**. Each Party's liability, taken together in the aggregate, arising out of or related to this DPA, shall be subject to any exclusions and limitations set forth in the Master Agreement, except to the extent prohibited by applicable law.

11.2 **Data Subject Claims**. In the event of a claim by a Data Subject under GDPR Articles 82(1) or 82(2), the Parties agree to cooperate in good faith to identify the responsible Party.

Each Party will be liable only for the damage caused by its own processing activities that infringe GDPR.

12. Governing Law and Jurisdiction

12.1 **Governing Law**. This DPA and any dispute or claim arising out of or in connection with it shall be governed by the laws of the **Netherlands** (or as specified in the Master Agreement), without regard to conflict of laws principles.

12.2 **Jurisdiction**. The courts of **Rotterdam, the Netherlands**, shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this DPA, unless mandatory laws dictate otherwise.

13. Return or Deletion of Personal Data

13.1 **Controller's Choice**. Upon termination or expiration of the Master Agreement, Controller may request that Processor either:

- Return all Personal Data, or
- Securely delete/anonymize all Personal Data

13.2 **Survival**. Processor may retain Personal Data if required by law or if it has a legitimate interest recognized by GDPR, but only to the extent and duration required. Any retained data remains subject to this DPA's confidentiality and security obligations.

14. Miscellaneous

14.1 **Entire Agreement**. This DPA forms part of the Master Agreement and constitutes the Parties' entire agreement with respect to processing of Personal Data.

14.2 **Variations**. Any modifications or amendments to this DPA must be in writing and signed by both Parties.

14.3 **Severability**. If any provision of this DPA is held invalid or unenforceable, such provision will be enforced to the maximum extent permissible, and the remaining provisions will remain in full force and effect.

15. Signatures

By signing below, each Party warrants that it has the authority to enter into this DPA and agrees to be bound by its terms.

For the Controller:

Company Name: _____

Name & Title: _____

Signature: _____

Date: _____

For Processor (Inquira Technologies B.V.):

Name & Title: _____

Signature: _____

Date: _____

Annex 1: Description of Processing

1. Nature and Purpose of Processing

- **Conversational AI Services**:
  Provide call or chat-based interactions for scheduling appointments, sending reminders, gathering patient intake information or feedback, and other administrative workflows.

- **LLM-Powered Interactions**:
  Integrate third-party large language models (e.g. Azure OpenAI) with prompt control to facilitate natural language dialogues.

- **Workflow Customization**:
  Offer prompt engineering, workflow building, or consulting services to configure the AI system for the Controller's specified administrative use cases (e.g. appointment reminders, inbound call routing).

- **Analytics & Quality Assurance**:
  Maintain logs (transcripts, metadata) for performance monitoring, error tracking, and compliance purposes.

- **Data Processing on Behalf of Controller**:
  Only process Personal Data in line with the Controller's instructions and as specified in the Master Agreement or this DPA.

2. Categories of Data Subjects

- **Patients** (prospective, current, or discharged)

- **Healthcare Staff** (administrators, clinicians, nurses, front-desk personnel)

- **Other Individuals** as directed by the Controller's workflows (e.g. guardians, caregivers)

3. Categories of Personal Data

- **Identifiers**: Name, phone number, date of birth, national ID or patient ID, email address

- **Appointment Details**: Dates, times, locations, specific clinics/doctors, or internal scheduling codes

- **Medical Information (Non-Clinical)**: Symptoms or triage data, medication adherence, patient feedback relevant to administrative tasks (e.g., clarifying symptom details for scheduling or triage forms); no direct clinical decisions or diagnostic data is processed unless otherwise explicitly instructed

- **Interaction Data**: Chat logs, call recordings, transcripts, uploaded files (documents, images), metadata (timestamps, caller IDs)

4. Data Retention

- **Controller Instructions**: Personal Data is retained for as long as instructed by the Controller in accordance with the Master Agreement or relevant service-level terms.

- **Deletion or Return**: At the termination or expiry of the Master Agreement, Processor will delete or return all Personal Data upon the Controller's request, unless further retention is required by law or regulatory obligations.

- **Product Privacy Policy Reference**: For specific retention practices (e.g., how long transcripts or logs are kept), please refer to the Inquira Health Product Privacy Policy or relevant sections of the Master Agreement.

5. Special Notes

- **Non-Clinical Use**: By default, the system is geared towards administrative and scheduling workflows. If the Controller configures any workflow to capture diagnostic-level data, that usage may trigger additional data protection or regulatory obligations, which remain the Controller's responsibility.

- **Geographic Restriction**: Except for narrow exceptions (e.g., billing data to Stripe), patient or sensitive data remains hosted within the agreed region (e.g., Europe).

Annex 2: Technical and Organizational Measures

Processor implements the following **technical and organizational measures** at a minimum:

1. Encryption

- **In Transit**: TLS 1.2+ (or higher) for data transmission, including chat messages, call transcripts, and API calls.
- **At Rest**: AES-256 (or equivalent) for stored data. Keys are managed with secure key management systems (e.g. KMS).

2. Access Controls

- **Role-Based Access**: Only authorized personnel with a valid business need can access Personal Data.
- **Multi-Factor Authentication (MFA)**: Required for administrative and privileged accounts.
- **Strict Logging**: User activities are logged, including access attempts, configuration changes, and data exports.

3. Network Security

- **Segmentation**: Production environments are isolated from development/staging environments.
- **VPN / Private Networking**: Servers utilize secure VPN tunnels (e.g., WireGuard via Tailscale) for internal communications.
- **Firewall & IDS/IPS**: Use of firewalls and intrusion detection/prevention systems to monitor and block suspicious traffic.
- **Periodic Vulnerability Scans**: Regular scans of infrastructure (Hetzner, AWS, Azure environments) to detect potential security issues.

4. Monitoring & Auditing

- **Application Monitoring**: Tools like Sentry, PostHog, or similar for error tracking, performance metrics, and anomaly detection.

- **System Logs**: Retained to facilitate audits, incident investigations, and ensure compliance with data protection obligations.

- **Automated Alerts**: Alerts for unusual activity or threshold breaches (e.g. suspicious login attempts) to trigger immediate review.

5. Physical Security

- **Data Center Standards**: Hosting with reputable providers (Hetzner, AWS, Azure) that adhere to ISO 27001 or similar certifications.

- **24/7 Security**: Physical access controls, surveillance, and on-site staff ensure data centers are secured against unauthorized entry.

6. Incident Response

- **Documented Process**: Maintain an Incident Response Plan outlining roles, responsibilities, and escalation paths.

- **Notification**: In the event of a Personal Data Breach, Processor will notify the Controller **without undue delay**, providing details on the breach scope, impact, and remediation steps.

- **Containment & Recovery**: Immediate measures to isolate affected systems, restore backups, and secure data integrity.

7. Business Continuity & Disaster Recovery

- **Regular Backups**: Encrypted backups stored in geographically redundant locations (e.g., AWS, Hetzner).

- **DR Testing**: Periodic disaster recovery drills to verify the effectiveness of recovery time objectives (RTO) and recovery point objectives (RPO).

- **Availability Commitments**: Target a minimum of 99.9% uptime for production systems under normal operating conditions.

8. LLM Governance

- **Prompt Control**: Custom workflow engine that constrains Large Language Model interactions to authorized topics or instructions.

- **Content Moderation**: Azure OpenAI content filtering to block or flag disallowed content (e.g., harmful, hateful, or out-of-scope queries).

- **Transparency & Traceability**: Chat/call transcripts are stored alongside any extracted data to provide a clear audit trail of AI outputs.

9. Sub-Processor Compliance

- **Equivalent Safeguards**: All Sub-Processors must adhere to equivalent or stronger TOMs, ensuring data protection obligations pass down the chain.

- **Periodic Review**: Sub-Processor compliance is reviewed periodically to confirm alignment with GDPR and this DPA.