

DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) is entered into as of the earliest of (a) the date on which Customer accepts the Services Agreement or an order that incorporates this DPA, (b) the date on which it is last signed by both Parties, and (c) the date on which the Services to which this DPA applies become effective (the “**Effective Date**”) by and between TQH Research and Development LLC, a Florida limited liability company, with a mailing address at 1576 Bella Cruz Drive, No. 319, The Villages, Florida 32159 (“**Company**”), and the individual or legal entity identified as the customer in the accepted order or account record associated with the Services (“**Customer**”). Company and Customer may each be a “**Party**” and together the “**Parties**.”

This DPA governs Company’s Processing of Customer Personal Data through the Connected Features and forms part of the TQH Brain Software License and Subscription Agreement accepted by Customer, together with Customer’s accepted order and any other agreement that expressly incorporates this DPA (collectively, the “**Services Agreement**”). The Services Agreement, including this DPA, governs Company’s provision of TQH Brain, the Customer Portal, and related Company online services.

ARTICLE 1 – Definitions

1.1. “Applicable Data Protection Law” means each law or regulation concerning privacy, data protection, data security, breach notification, or the Processing of Personal Data that applies to the relevant Processing under this DPA.

1.2. “Business,” “Business Associate,” “Consumer,” “Controller,” “Covered Entity,” “Personal Data,” “Personal Information,” “Processor,” “Sale,” “Service Provider,” “Share,” and “Targeted Advertising” shall have the meanings assigned to them under Applicable Data Protection Law, and “Personal Data” includes “Personal Information” as that term is used under Applicable Data Protection Law. “Protected Health Information” or “PHI” has the meaning assigned under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended. An applicable Business Associate Agreement governs PHI only to the extent the PHI is created, received, maintained, or transmitted by Company on Customer’s behalf through an Approved PHI Feature within that agreement’s activated scope.

1.3. “Connected Feature” means a Company portal, secure form, document-exchange tool, email campaign, appointment reminder, Network Center function, support channel, or other Company online service through which Customer deliberately selects, enters, uploads, submits, displays, or transmits information, including through a feature configured by Customer to make scheduled transmissions.

1.4. “Connected-Feature Data” means information that Customer or its authorized users deliberately select, enter, upload, submit, display, or transmit through a Connected Feature. Connected-Feature Data may leave Customer’s local environment and may be received, Processed, stored, encrypted, decrypted, transmitted, or accessed by Company systems and designated service providers as necessary to provide the selected feature. The fact that a source record is also stored locally does not make a transmission of Connected-Feature Data local-only.

1.5. “Customer Personal Data” means Personal Data contained in Connected-Feature Data that Company Processes on Customer’s behalf under the Services Agreement. Customer Personal Data excludes:

1.5.1. Local Practice Records that Company does not receive or access;

1.5.2. information Company Processes independently as a Controller, including information reasonably necessary to administer Customer’s account, licensing, orders, payments, subscriptions, agreement acceptance, security, fraud prevention, or legal obligations; and

1.5.3. information Processed by a third party acting independently under its own terms and privacy notice, except to the extent that the third party acts as Company’s Subprocessor.

1.6. “Data Subject” means an identified or identifiable natural person to whom Customer Personal Data relates, including a Consumer where that term applies.

1.7. “Local Practice Records” means Customer’s client lists, profiles, schedules, session notes, client documents, sensitive health information, practice financial reports, revenue and sales records, inventory records, related databases, and backups maintained within equipment or storage controlled by Customer. The standard local installation does not automatically upload Customer’s primary practice database or document library to Company, and Company does not host or maintain a disaster-recovery copy of that database or provide Company cloud storage for it. Local Practice Records are distinct from Connected-Feature Data that Customer deliberately submits, or configures the software to transmit on a schedule, through a Connected Feature; a locally stored source record does not make such a transmission local-only.

1.8. “Process,” “Processing,” and “Processed” mean any operation or set of operations performed on Customer Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, access, adaptation, alteration, retrieval, consultation, use, encryption, decryption, transmission, disclosure, dissemination, combination, restriction, erasure, or destruction, and shall be interpreted consistently with the meaning given to such terms under Applicable Data Protection Law.

1.9. “Security Incident” means an actual unauthorized acquisition of, access to, use of, disclosure of, alteration of, or destruction of Customer Personal Data in Company’s possession or control. Security Incident excludes unsuccessful attempts or activities that do not compromise Customer Personal Data, such as unsuccessful login attempts, pings, port scans, denial-of-service attempts, and attacks blocked by Company’s safeguards.

1.10. “Services” means the Connected Features and related services that Company provides to Customer under the Services Agreement and that involve Company’s Processing of Customer Personal Data.

1.11. “Subprocessor” means a third party engaged by Company to Process Customer Personal Data on Customer’s behalf in connection with the Services.

ARTICLE 2 – Scope, Roles, and Processing Instructions

2.1. Scope. This DPA applies only to Customer Personal Data Processed by Company through Connected Features. It does not apply to a genuinely local-only installation or to Local Practice Records that remain solely within Customer's environment and are not provided, displayed, or transmitted to Company or a Company-managed service. Expressly authorized support may permit access to information visible or supplied within the agreed support scope, in which case this DPA applies to any Customer Personal Data Company Processes on Customer's behalf in providing that support.

2.2. Party roles. As between the Parties, Customer acts as the Controller or Business, and Company acts as the Processor or Service Provider, with respect to Customer Personal Data Processed by Company on Customer's behalf. The Parties acknowledge that their legal roles are determined by the relevant facts and Applicable Data Protection Law, rather than solely by the labels used in this DPA.

2.3. Documented instructions. Company shall Process Customer Personal Data only:

2.3.1. to provide, secure, maintain, and support the operation of the Services purchased or enabled by Customer;

2.3.2. in accordance with the Services Agreement, this DPA, Schedule 1, and Customer's documented configuration and use of the Services;

2.3.3. as necessary to prevent fraud, address security threats, enforce lawful service restrictions, or comply with applicable legal obligations; or

2.3.4. as otherwise instructed by Customer in writing and agreed to by Company.

2.4. Unlawful instructions. If Company reasonably believes that a Customer instruction violates Applicable Data Protection Law, Company may suspend the affected Processing and shall notify Customer unless prohibited by law. The Parties shall cooperate in good faith to modify the instruction so that Processing may continue lawfully.

2.5. Processing details. The subject matter, nature, purpose, duration, categories of Data Subjects, and categories of Customer Personal Data are described in Schedule 1. Customer shall not submit categories of Personal Data outside the permitted scope stated in Schedule 1.

2.6. No sale, advertising, or general-purpose AI use. Except as permitted by Applicable Data Protection Law and Customer's documented instructions, Company shall not sell Customer Personal Data, share it for cross-context behavioral advertising, use it for targeted advertising, or use it to train or improve a general-purpose artificial-intelligence or machine-learning model. Company shall not retain, use, or disclose Customer Personal Data outside the direct business relationship between Company and Customer except as permitted by Applicable Data Protection Law and Customer's documented instructions. Company-managed portal and Connected-Feature Processing is not used for targeted advertising.

2.7. No combining of data. Except as permitted by Applicable Data Protection Law, Company shall not combine Customer Personal Data received from or on behalf of Customer with Personal Data received from another person or collected from Company's own interactions with a Data Subject.

2.8. Processing required by law. If law requires Company to Process Customer Personal Data contrary to Customer's instructions, Company shall notify Customer before the Processing unless the law prohibits notice.

ARTICLE 3 – Customer Obligations

3.1. Lawful data and instructions. Customer is responsible for:

3.1.1. the legality, accuracy, quality, and content of Customer Personal Data;

3.1.2. establishing a lawful basis for the collection, use, disclosure, and Processing of Customer Personal Data;

3.1.3. providing legally required notices and obtaining legally required permissions or consents;

3.1.4. configuring and using the Services in accordance with the Services Agreement, this DPA, Schedule 1, and Applicable Data Protection Law;

3.1.5. selecting lawful recipients and limiting submitted data to what is reasonably necessary for the selected feature; and

3.1.6. responding to Data Subjects regarding Local Practice Records and other information controlled by Customer.

3.2. Customer safeguards. Customer shall maintain reasonable administrative, technical, and physical safeguards for its systems, credentials, Local Practice Records, exports, backups, and use of the Services. These safeguards include authorized staff access, strong individual credentials, available multifactor authentication, device locks, supported and patched systems, suitable malware protection, secure networks and physical access, full-drive encryption for volumes containing the database, keys, temporary staging files, exports, and backups, trusted HTTPS configured for each workstation without bypassing certificate warnings, staff training, tested backups, and secure disposal practices.

3.3. Restricted data. Customer shall not submit payment-card numbers, card security codes, passwords, or other authentication secrets through ordinary Company email, support forms, or support tickets. Customer shall remove unnecessary client identifiers from ordinary support email, tickets, screenshots, attachments, and logs.

3.4. Data Subject communications. Customer remains responsible for its communications with its clients and other Data Subjects, including obtaining communication consent, maintaining accurate recipient lists, providing required disclosures, and honoring applicable opt-out requests.

ARTICLE 4 – Confidentiality and Personnel

4.1. Confidential treatment. Company shall keep Customer Personal Data confidential and shall not disclose it except as permitted by this DPA, at Customer's documented direction, or as required by law.

4.2. Authorized personnel. Company shall limit access to Customer Personal Data to personnel and contractors who require access to perform the Services or satisfy Company's legal obligations.

4.3. Confidentiality obligations. Company shall ensure that personnel authorized to Process Customer Personal Data are subject to contractual, professional, or statutory confidentiality obligations appropriate to the nature of the information.

4.4. Required disclosure. If Company is legally required to disclose Customer Personal Data, Company shall, to the extent legally permitted, notify Customer before disclosure and reasonably cooperate with Customer's lawful efforts to limit or challenge the disclosure.

ARTICLE 5 – Security

5.1. Security program. Company shall implement and maintain reasonable administrative, technical, and physical safeguards designed to protect Customer Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, alteration, or disclosure. The measures applicable to the Services are described in Schedule 2.

5.2. Appropriate safeguards. In determining appropriate safeguards, Company may consider the nature, scope, context, and purposes of Processing; the sensitivity and quantity of Customer Personal Data; the state of available technology; implementation costs; and the risks to Data Subjects.

5.3. Service architecture. The Parties acknowledge that the Services use feature-specific security arrangements. Protected secure-form data is application-encrypted in managed database services, and attachments and protocol PDFs are application-encrypted in private storage and decrypted by authorized service code for the requested workflow. Other data, including Network Center text and metadata, uses provider-managed protection and access controls rather than the same application-level encryption arrangement.

5.4. Customer-controlled environments. Company's safeguards do not replace Customer's responsibility for systems, devices, mailboxes, Microsoft tenant settings, recipient systems, independently selected providers, Local Practice Records, exports, and backups within Customer's possession or control.

5.5. Security review. Company shall periodically evaluate its safeguards and modify them when reasonably necessary to address material changes in the Services, relevant threats, or Applicable Data Protection Law.

ARTICLE 6 – Security Incidents

6.1. Notification. Company shall notify Customer without undue delay after becoming aware of a Security Incident affecting Customer Personal Data and within any shorter period required by Applicable Data Protection Law. A Security Incident involving PHI is governed by the incident-notice requirements of the applicable Business Associate Agreement.

6.2. Content. To the extent known and legally permitted, Company's notice shall describe:

6.2.1. the nature of the Security Incident;

- 6.2.2. the categories of affected Customer Personal Data and Data Subjects;
- 6.2.3. the known or reasonably anticipated consequences;
- 6.2.4. the measures taken or proposed to contain, investigate, and remediate the Security Incident; and
- 6.2.5. a contact for reasonable follow-up inquiries.

6.3. Supplemental information. Company may provide available information in phases as its investigation proceeds and shall supplement its notice without undue delay as additional material information becomes available. An initial notice does not constitute an admission of fault or liability.

6.4. Cooperation. Company shall take reasonable steps to contain, investigate, and remediate a Security Incident and shall reasonably assist Customer with notifications or other actions that Applicable Data Protection Law requires, considering the nature of Processing and information available to Company.

6.5. Customer incidents. Customer shall notify Company promptly of an incident affecting Company credentials, Company-managed Services, or Customer's authorized users. Customer shall not include PHI, passwords, payment-card data, or unnecessary client records in an ordinary incident-notification email.

ARTICLE 7 - Data Subject Requests and Compliance Assistance

7.1. Requests received by Company. If Company receives a verified request from a Data Subject concerning Customer Personal Data Processed solely on Customer's behalf, Company shall, where legally permitted, refer the requester to Customer or notify Customer and await Customer's reasonable instructions.

7.2. Assistance. Taking into account the nature of the Processing and functionality available within the Services, Company shall reasonably assist Customer in responding to legally valid requests for access, correction, deletion, portability, consent withdrawal, or an applicable privacy opt-out.

7.3. Scope and limitations. Assistance and deletion obligations apply only to Customer Personal Data Company actually holds. They do not require Company to delete Local Practice Records, recipient copies, mailbox copies, suppression records, legally required records, legal-hold materials, or provider recovery copies that Company cannot reasonably control or that may lawfully be retained.

7.4. Regulatory assistance. Company shall reasonably assist Customer with legally required privacy assessments, security inquiries, and consultations concerning Company's Processing, taking into account the nature of the Processing and information available to Company.

7.5. Customer responsibility. Customer shall independently respond to requests concerning Local Practice Records because Company does not maintain or search Customer's local database under the standard local configuration.

ARTICLE 8 – Subprocessors

8.1. Authorization. Customer authorizes Company to engage each provider identified in Schedule 3 as a Subprocessor only to the extent that provider Processes Customer Personal Data on Company's behalf for the identified Services. Listing an independent provider or a customer-configured provider in Schedule 3 does not make that provider Company's Subprocessor.

8.2. Subprocessor obligations. Before permitting a Subprocessor to Process Customer Personal Data, Company shall enter into a written agreement requiring the Subprocessor to protect Customer Personal Data through obligations materially consistent with the applicable obligations imposed on Company under this DPA.

8.3. Responsibility. Company remains responsible for a Subprocessor's performance of the data-protection obligations Company delegates to that Subprocessor, subject to the limitations and exclusions in the Services Agreement and Applicable Data Protection Law.

8.4. Changes. Company shall provide reasonable prior written notice of a material addition or replacement of a Subprocessor that Processes Customer Personal Data, except where an emergency requires shorter notice to maintain the security or continuity of a Connected Feature. Customer may object on reasonable data-protection grounds by written notice within 15 days after notice. The Parties shall work in good faith to address the objection. If no commercially reasonable alternative is available, either Party may discontinue the affected Connected Feature without terminating unaffected Services. Company shall update Schedule 3 within a reasonable time after the new or replacement Subprocessor begins Processing Customer Personal Data.

8.5. Independent providers. A provider selected, contracted, or configured independently by Customer is not Company's Subprocessor merely because the Services interoperate with that provider. The optional Microsoft 365 mailbox integration connects Customer's Center server directly to the Microsoft tenant and mailbox configured by Customer and is not routed through Company's managed reminder or campaign store. Microsoft Graph is only the API/access mechanism used to authenticate to and interact with the configured Microsoft Entra ID and Exchange Online services; it is not treated under this DPA as a separately covered service.

ARTICLE 9 - Retention, Return, and Deletion

9.1. Feature-specific retention. Customer acknowledges that retention is feature-specific and that no single retention period applies to all Customer Personal Data. The applicable retention and deletion practices are stated in Schedule 1 and the Privacy Notice.

9.2. Termination instructions. Upon expiration or termination of the applicable Services, Company shall, at Customer's written direction and to the extent supported by the applicable Connected Feature, delete or return Customer Personal Data within Company's possession or control in accordance with Schedule 1 and the Privacy Notice, except to the extent:

9.2.1. retention is required or permitted by applicable law;

9.2.2. the data consists of security, fraud-prevention, agreement-acceptance, suppression, billing, transaction, audit, or dispute records that Company may lawfully retain;

9.2.3. the data remains in backups or provider recovery systems pending deletion through ordinary lifecycle processes, in which case Company shall continue to protect the data and shall not actively Process it except for security, recovery, or legal-compliance purposes; or

9.2.4. Company cannot control copies held by recipients, Customer-configured mailboxes, or independent providers.

9.3. Deletion safeguards. Customer Personal Data retained under Section 9.2 shall remain protected under this DPA, shall not be Processed for another purpose, and shall be deleted when the applicable retention basis ends.

9.4. Local records. Expiration, cancellation, suspension, or termination does not authorize Company to remotely delete Local Practice Records and does not transfer ownership of those records to Company.

9.5. Exports. Customer is responsible for preserving required readable exports, original-document downloads, backups, and recovery materials before access to a trial, plan, subscription, or Connected Feature ends or changes. Company does not promise a fixed post-closure retrieval window, a single export of all Local Practice Records, or export or retrieval of Connected-Feature Data that Company does not hold or that the applicable feature does not support.

ARTICLE 10 - Audits and Demonstration of Compliance

10.1. Compliance information. Upon Customer's reasonable written request, Company shall make available information reasonably necessary to demonstrate Company's compliance with this DPA.

10.2. Assessments. Company may satisfy an assessment request by providing then-current third-party assessment reports, certifications, summaries, policies, or responses to a reasonable written questionnaire, subject to appropriate confidentiality restrictions.

10.3. Additional audit. If the information provided under Section 10.2 is insufficient to address a reasonable and documented compliance concern, Customer may conduct an additional assessment no more than once during any twelve-month period, unless a Security Incident or regulator requires otherwise. The assessment shall:

10.3.1. occur on reasonable advance written notice and during normal business hours;

10.3.2. be limited to systems, records, and Processing relevant to Customer Personal Data;

10.3.3. avoid access to another customer's data, privileged material, security-sensitive testing details, and Company trade secrets unrelated to compliance;

10.3.4. not unreasonably interfere with Company's operations; and

10.3.5. be performed by Customer or a qualified independent assessor subject to confidentiality obligations.

10.4. Costs. Each Party shall bear its own assessment costs.

10.5. Remediation. Company shall address material deficiencies identified through an assessment within a reasonable period proportionate to the associated risk.

ARTICLE 11 - HIPAA and Protected Health Information

11.1. No default authorization. This DPA is not a Business Associate Agreement and does not, by itself, authorize Customer to submit PHI to Company or any Connected Feature. Features are not approved for PHI by default.

11.2. No-PHI restriction. Customer shall not enter, upload, submit, display, or transmit PHI or other identifiable client health information through a Connected Feature, online service, or support channel unless:

11.2.1. Company has expressly designated and enabled the specific feature as PHI-capable for Customer;

11.2.2. the Parties have executed a Business Associate Agreement applicable to the feature and Customer;

11.2.3. all required provider agreements and covered-service configurations have been confirmed, including, for any Microsoft-dependent PHI workflow, confirmation that the tenant used for Company-managed Processing is TQH's actual Microsoft tenant, the applicable tenant and subscription are active, Microsoft Entra ID and Exchange Online are the licensed services actually used, the sending mailbox and permissions are configured for that workflow, the contracting Microsoft customer has not opted out of Microsoft's HIPAA Business Associate Agreement, and the particular use is HIPAA-eligible under Microsoft's then-current terms; and

11.2.4. the feature is identified as PHI-permitted in a completed and mutually approved Schedule 1 entry to the applicable Business Associate Agreement.

11.3. Conditional BAA. If Customer is an eligible Covered Entity or Business Associate and Company approves a PHI-capable feature, the Parties shall execute the Conditional HIPAA Business Associate Addendum and complete and mutually approve the applicable Approved PHI Feature entry in its Schedule 1. That Business Associate Agreement shall apply only to the approved feature and PHI expressly within its scope after all applicable activation conditions are satisfied. Customer's unauthorized submission of PHI does not activate the Business Associate Agreement or expand the authorized scope of the Services, but does not relieve either Party of any nonwaivable duty imposed by applicable law with respect to PHI actually received. In the event of a conflict concerning the privacy, security, use, disclosure, return, or destruction of PHI, the Business Associate Agreement controls.

11.4. Prohibited features. Unless expressly approved under Section 11.2, Customer shall not submit identifiable client health information to the Network Center, Bulletin Board, referral directory, ordinary support email, campaigns, reminders, or any other feature not expressly authorized for that purpose.

11.5. Consumer health data. A Connected Feature may Process Personal Data that reveals or permits inferences about health, treatment interests, or services sought. Where Applicable Data Protection Law treats that information as consumer health data, the Parties shall use the feature only

after required disclosures, permissions, consents, and contractual safeguards are in place. Company shall use such data only to provide the selected feature and related operations and shall not sell it, share it for cross-context behavioral advertising, or use it for targeted advertising. Customer shall not use the affected feature for consumer health data in a jurisdiction where a required consent or disclosure framework is not in place.

11.6. No status determination. Nothing in this DPA determines whether either Party is a Covered Entity, Business Associate, or other regulated entity. Those roles depend on the Parties' actual activities and the applicable Processing.

ARTICLE 12 - Liability and Order of Precedence

12.1. Services Agreement controls remedies. The warranty disclaimers, exclusions of damages, liability limitations, indemnification provisions, and remedies in the Services Agreement apply to this DPA, except to the extent prohibited by Applicable Data Protection Law.

12.2. Connected-Feature Data. The Services Agreement does not disclaim Company's responsibility for loss or unauthorized disclosure of Connected-Feature Data to the extent such responsibility cannot be limited or disclaimed under Applicable Data Protection Law or other nonwaivable law.

12.3. Order of precedence. In the event of a conflict:

12.3.1. an executed Business Associate Agreement controls with respect to PHI within its scope;

12.3.2. the Terms and Privacy Notice control the descriptions of the Services, data flows, feature functionality, retention and deletion limits, and other matters they address;

12.3.3. this DPA supplements the Services Agreement and controls only with respect to Company's obligations as a Processor or Service Provider for Customer Personal Data, to the extent it does not conflict with the Terms, Privacy Notice, or an applicable Business Associate Agreement; and

12.3.4. Schedule 1 controls over a general description in this DPA only with respect to the expressly identified feature configuration, permitted data, and Processing details, but it may not expand a data flow, feature capability, retention or deletion commitment, or other representation beyond the Terms and Privacy Notice or reduce a protection required by this DPA or Applicable Data Protection Law.

ARTICLE 13 - Term and Termination

13.1. Term. This DPA begins on the Effective Date and remains effective while Company Processes Customer Personal Data under the Services Agreement.

13.2. Termination. This DPA terminates when Company no longer Processes Customer Personal Data. For Customer Personal Data retained after expiration or termination of the Services, the applicable protections and restrictions of this DPA remain in effect until the data is deleted or returned in accordance with Article 9.

13.3. Suspension. Company may suspend affected Processing when reasonably necessary to address an unlawful instruction, prohibited-data submission, serious security threat, material breach, or legal requirement. For a correctable material breach, Company shall ordinarily provide written notice and at least 10 days to cure before terminating the affected Processing. Company may act immediately when reasonably necessary to address fraud, a serious security risk, unlawful activity, or a legal obligation, shall promptly notify Customer unless prohibited by law, and shall use reasonable efforts to restore the affected Processing after the risk is addressed. Where reasonably practicable, Company shall limit the suspension to the affected feature.

13.4. Survival. Articles 4, 6, 9, 11, 12, and 14 survive termination to the extent necessary to protect retained Customer Personal Data or enforce accrued rights and obligations.

ARTICLE 14 - General Provisions

14.1. Governing law and venue. Florida law governs this DPA, without regard to conflict-of-law principles, subject to applicable federal law and mandatory protections that cannot lawfully be waived. Subject to those protections and nonwaivable venue rights, the Parties consent to exclusive jurisdiction in the state courts located in Lake County, Florida, and the federal courts serving that county.

14.2. Notices. Notices under this DPA must be in writing and delivered to the following contacts, as updated by written notice:

14.2.1. Company: TQH Research and Development LLC; 1576 Bella Cruz Drive, No. 319, The Villages, Florida 32159; Attention: Privacy and Security Contact; Email: support@tqhbrain.com.

14.2.2. Customer: the individual or legal entity identified as Customer in the accepted order or account record; Address: Customer's address in its then-current account record; Attention: Privacy Contact; Email: the email address designated by Customer for legal or privacy notices in its account record.

14.3. Amendments. An amendment to this DPA must be in writing and accepted by authorized representatives of both Parties, except that Company may update Schedule 3 in accordance with Article 8.

14.4. Assignment. Neither Party may assign this DPA separately from the Services Agreement. Any permitted assignment of the Services Agreement includes this DPA.

14.5. Severability. If a provision of this DPA is held unenforceable, it shall be modified to the minimum extent necessary to make it enforceable, and the remaining provisions shall remain effective.

14.6. Waiver. A waiver is effective only if in writing and signed by the waiving Party. A waiver on one occasion is not a waiver on another occasion.

14.7. Counterparts, acceptance, and electronic signatures. Customer accepts this DPA by accepting the Services Agreement or an order that incorporates this DPA. The Parties may also execute this DPA in counterparts and by electronic signature, each of which is deemed an original and all of which constitute one instrument.

14.8. Entire agreement concerning Processing. This DPA, the Services Agreement (including the Terms and Privacy Notice), its incorporated schedules, and any applicable Business Associate Agreement constitute the Parties' agreement concerning the Processing addressed here and supersede prior or contemporaneous understandings concerning that subject matter, subject to the order of precedence in Article 12.

14.9. Obligations limited to Applicable Data Protection Law. Company's obligations as a Processor or Service Provider under this DPA are intended to meet, and not to exceed, what Applicable Data Protection Law requires of a Processor or Service Provider with respect to the relevant Processing. Where a provision of this DPA can reasonably be read either to track or to exceed those requirements, it shall be read to track them, and nothing in this DPA shall be construed to impose on Company any duty, assistance, notification, deletion, audit, or other obligation beyond what Applicable Data Protection Law requires, except for the specific commitments the Parties have expressly agreed to in this DPA.

[SIGNATURE PAGE FOLLOWS]

SIGNATURE BLOCKS

TQH RESEARCH AND DEVELOPMENT LLC

By: _____

Name: _____

Title: _____

Date: _____

CUSTOMER IDENTIFIED IN THE ACCEPTED ORDER OR ACCOUNT RECORD

By: _____

Name: _____

Title: _____

Date: _____

Schedule 1 – Processing Details and Feature Schedule

Article 1 – General Processing Description

- 1.1. Subject matter.** Processing of Customer Personal Data through the Connected Features enabled and used by Customer.
- 1.2. Duration.** For the term of the applicable Services and any limited period afterward during which Company lawfully retains Customer Personal Data under Article 9.
- 1.3. Nature and purpose.** Receipt, access, storage, encryption, decryption, organization, transmission, retrieval, support, security monitoring, deletion, and other Processing reasonably necessary to provide the selected Connected Features.
- 1.4. Data Subjects.** Customer's account holders, authorized users, workforce members, clients, prospective clients, communication recipients, form recipients, directory participants, support contacts, and other individuals whose Personal Data Customer deliberately submits through an enabled Connected Feature.
- 1.5. Permitted Personal Data.** Business contact information; account, practice, installation, and user identifiers; recipient email addresses; appointment start time and time-zone information; practice name and contact information; delivery identifiers, timestamps, status, and outcomes; campaign subject, body, links, sender information, scheduling data, and delivery progress; form and document selections, attachments, request metadata, submitted content, and verification information approved for the applicable workflow; submitted network content and access metadata; support messages, technical logs, and material deliberately provided or displayed; authentication and session information; and other technical and security information expressly identified for the selected feature in the Privacy Notice and this Schedule 1.
- 1.6. Prohibited Personal Data.** PHI unless Article 11 has been satisfied for the specific feature; full payment-card numbers; card security codes; passwords; authentication secrets; and data outside the documented scope of the selected feature.

Article 2 – Feature Matrix

Connected Feature	Permitted Data and Purpose	Company Role and Processing	Retention and Deletion	DPA/BAA Status
Appointment reminders	Recipient email address, appointment start time, time zone, practice name, contact telephone number, and delivery identifier; treatment-detail fields are prohibited, although practice identity and appointment context	Company-managed cloud function uses Microsoft Graph as the API/access mechanism to authenticate through Microsoft Entra ID and send reminders through Exchange Online from the configured sender	Tracking retains identifiers, timestamps, and delivery status, not the recipient address or message body; Sent Items, recipient, and mail-system copies follow separate retention settings, and no immediate-deletion	DPA applies; not approved for PHI unless Company confirms the feature is PHI-capable and all BAA activation conditions are satisfied

	may reveal health-related information		or universal retention period is promised	
Email campaigns	Selected recipient information, campaign subject and body, links, sender information, scheduling information, and delivery progress; PHI is prohibited unless expressly approved	Company-managed processing stores an application-encrypted payload and decrypts it in authorized service code, then uses Microsoft Graph as the API/access mechanism to authenticate through Microsoft Entra ID and send messages through Exchange Online from the configured sender	Completion or cancellation records status and timestamp but does not automatically remove the encrypted payload; delivery and audit records, suppression entries, and unsubscribe tokens remain subject to distinct retention rules	DPA applies; not approved for PHI unless Company confirms the feature is PHI-capable and all BAA activation conditions are satisfied
Secure forms and document exchange	Recipient email, selected form or document information, attachments, request metadata, submitted content, and verification information	Company-managed services process protected form data and attachments for verified submission and retrieval workflows; where email is sent, Microsoft Graph is the API/access mechanism used with Microsoft Entra ID and Exchange Online to transmit request and verification emails from the configured sender under the applicable Microsoft service terms and provider coverage	Imported, Rejected, Revoked, and Expired requests enter terminal cleanup that removes protected request and submission content, disables prior access, and attempts attachment deletion; failed attachment deletion may require retries, limited status and cleanup metadata may remain, and submitted forms awaiting review are retained	DPA applies; BAA applies only after the secure-forms and document-exchange feature is activated under a completed and mutually approved BAA Schedule 1 entry
Network Center and protocol resources	Posts, replies, practice listings, advertisements, moderation reports, access metadata, and protocol files; client-identifying information is prohibited	Company hosts and displays submitted content according to audience, membership, and moderation settings	Content, files, moderation records, and audit records follow distinct lifecycles without a verified universal age-based deletion schedule; visibility changes or moderation do not immediately erase recipient copies, files, or audit records	DPA applies where Company Processes Personal Data on Customer's behalf; not approved for PHI

Authorized support	Contact details, support messages, technical logs, and information Customer deliberately provides or displays	Authorized remote support is limited to Customer's authorization and the agreed support scope; ordinary email and ticket channels are separate and are not approved for PHI	Support mail, tickets, logs, and remote-session artifacts follow distinct operational lifecycles without a verified universal age-based deletion schedule	DPA applies to Customer Personal Data Company Processes on Customer's behalf; ordinary support channels are not approved for PHI, and remote support is PHI-capable only after the required BAAs and a completed feature-specific approval are in effect
Microsoft 365 mailbox integration	Mailbox folders, messages, recipients, subjects, bodies, attachments, and message-state actions	Customer's Center server connects directly to Customer's configured Microsoft tenant and mailbox; content is not routed through Company's managed reminder or campaign store	Retention is controlled principally by Customer's mailbox configuration, Microsoft services, and recipients; Sent Items and recipient copies may remain, and background synchronization is not a complete local mailbox archive	DPA does not apply to mailbox content routed directly between Customer's Center server and Customer's Microsoft tenant unless Company separately accesses or Processes it on Customer's behalf; PHI use is not approved by default and requires Article 11 confirmation for Customer's actual tenant, subscription, licensed Exchange Online and Microsoft Entra ID services, mailbox and permissions configuration, non-opt-out status, and HIPAA-eligible use
Reserved—no additional Connected Feature approved	None	None	Not applicable	Not approved; update this Schedule before launch

Schedule 2 – Minimum Technical and Organizational Measures

Company shall maintain the following measures, as applicable to the Services and proportionate to the relevant risks:

2.1. Access control. Role-appropriate access restrictions, authentication controls, credential-management procedures, and periodic review of authorized access.

2.2. Encryption. Encryption of Customer Personal Data in transit using appropriate transport protections and encryption at rest where identified for the applicable feature, including application-level encryption for feature content expressly described as using that protection. For ePHI within an Approved PHI Feature, the encryption requirements of the applicable Business Associate Agreement control.

2.3. Infrastructure security. Reasonable hardening, patching, malware protection, logging, monitoring, vulnerability management, and environment-separation practices for Company-managed systems.

2.4. Secure development and change management. Procedures reasonably designed to evaluate material changes, restrict production access, address identified security defects, and prevent unauthorized deployment.

2.5. Incident response. Documented procedures for identifying, containing, investigating, remediating, and communicating Security Incidents.

2.6. Business continuity. Measures appropriate to Company-managed Services for backup, recovery, continuity, and restoration. Customer remains responsible for maintaining and testing backups of its primary Local Practice Records; Company does not maintain a disaster-recovery copy of those records.

2.7. Personnel safeguards. Confidentiality obligations, security awareness appropriate to personnel responsibilities, and access termination or modification when personnel roles change.

2.8. Provider management. Reasonable diligence and written data-protection obligations for Subprocessors with access to Customer Personal Data.

2.9. Additional confirmed measures. No additional certifications, testing commitments, recovery objectives, encryption arrangements, or retention controls are represented beyond those expressly stated in the Services Agreement, Privacy Notice, this DPA, and any applicable Business Associate Agreement or completed feature schedule.

Schedule 3 – Authorized Subprocessors and Other Service Providers

Provider and status	Service or Processing Function	Data Location	Categories of Customer Personal Data	Applicable Connected Features
Google Cloud and Firebase services – Subprocessor for applicable Company-managed features; PHI use requires confirmed provider coverage and covered-service configuration	Portal hosting, authentication, cloud processing, storage, database, logging, scheduling, and related infrastructure	United States for secure-form and document-exchange storage and processing; otherwise the region configured for the applicable Google Cloud or Firebase service, subject to applicable provider terms	Account, authentication, feature content, attachments, technical, security, and workflow data, as applicable	Customer Portal, secure forms, document exchange, Network Center, campaigns, and reminders, as applicable to the configured service
Microsoft – Subprocessor through Microsoft Entra ID and Exchange Online for Company-managed features and independent provider for Customer-configured mailbox integration. Microsoft Graph is the API/access mechanism, not a separately represented covered service. Microsoft identifies Microsoft Entra ID and Exchange Online as in-scope HIPAA services, and Microsoft's HIPAA Business Associate Agreement is incorporated through the Microsoft DPA by default for qualifying Covered Entity or Business Associate customers unless they opt out; PHI use remains subject to Article 11 and confirmation of the actual tenant, subscription, licensed services, mailbox and permissions configuration, non-	Microsoft Entra ID authentication and Exchange Online communications and mailbox operations, accessed through Microsoft Graph for reminders, campaigns, secure-form request and verification emails, sending, receiving, and mailbox operations	Microsoft infrastructure associated with TQH's actual Microsoft tenant for Company-managed features or Customer's actual Microsoft tenant for Customer-configured mailbox integration, as applicable, subject to the applicable Microsoft service terms and data-location commitments	Account identifiers, recipient information, message content, attachments, mailbox information, and delivery data	Reminders, campaigns, and secure-form request and verification emails; optional mailbox integration is customer-configured and direct to Customer's Microsoft tenant rather than Company-managed storage

opt-out status, and HIPAA-eligible use				
Stripe – independent provider for certain payment functions and Subprocessor only to the extent it Processes Customer Personal Data on Company's behalf	Payment and subscription processing	Stripe-controlled infrastructure associated with the configured account and services, subject to Stripe's applicable service terms and data-location commitments	Billing contacts, subscription and payment identifiers, payment status, invoices, and limited payment-method details	Account billing; Stripe's payment-card functions are governed by Stripe's own privacy notice, while any Subprocessor role is limited to Processing performed on Company's behalf
PC Planet – Company support provider; Company's BAA with PC Planet is in effect	Authorized support services	Locations and provider-controlled infrastructure used by PC Planet within the authorized support scope and subject to its agreement with Company	Support contact information, technical information, and information deliberately displayed or provided during authorized support	Authorized support
Reserved—no additional provider identified	None	Not applicable	None	Not applicable