

CONDITIONAL HIPAA BUSINESS ASSOCIATE ADDENDUM

This Conditional HIPAA Business Associate Addendum (this “**Addendum**”) is entered into as of the date on which the last Party executes or electronically accepts it (the “**Effective Date**”) by and between the individual or legal entity identified as the customer in the accepted order and execution record for this Addendum (“**Customer**”) and TQH Research and Development LLC, a Florida limited liability company (“**Company**”). Customer and Company are each a “**Party**” and collectively the “**Parties.**”

This Addendum supplements and is incorporated into the TQH Brain Terms and Conditions, Software License and Subscription Agreement accepted by Customer, together with Customer's accepted order, the TQH Brain Data Processing Addendum (the “DPA”), and any other agreement that expressly incorporates this Addendum (collectively, the “**Services Agreement**”), pursuant to which Company provides TQH Brain and its subscriptions, Customer Portal, connected features, and related Company online services to Customer.

The Parties intend this Addendum to apply only to an Approved PHI Feature for which Company creates, receives, maintains, or transmits Protected Health Information on behalf of Customer in the capacity of a Business Associate or subcontractor Business Associate. This Addendum does not apply to Local Practice Records that remain solely within Customer's environment and are not provided, displayed, transmitted, or made accessible to Company or a Company-managed service.

The Parties further intend that no Connected Feature may create, receive, maintain, or transmit Protected Health Information unless Company has expressly designated and enabled the specific feature as PHI-capable for Customer, the Parties have executed this Addendum, all required provider agreements and covered-service configurations have been confirmed, and the feature is identified as PHI-permitted in Schedule 1.

For good and valuable consideration, the receipt and sufficiency of which are acknowledged, the Parties agree as follows:

ARTICLE 1 – Definitions and Interpretation

1.1. Defined terms. For purposes of this Addendum:

1.1.1. “Activation Conditions” means all of the following conditions:

1.1.1.1. Company has expressly designated and enabled the specific Connected Feature as PHI-capable for Customer;

1.1.1.2. the Parties have executed this Addendum for the feature and Customer;

1.1.1.3. all required provider agreements and covered-service configurations have been confirmed, including for any Microsoft-supported workflow the actual tenant, subscription, licensed services, sending mailbox and related configuration, the continued effectiveness and non-opt-out status of the applicable provider business associate agreement, and the HIPAA-eligible use of the configured services; and

1.1.1.4. the feature is identified as PHI-permitted in Schedule 1.

1.1.2. “Approved PHI Feature” means a specific Connected Feature for which all Activation Conditions have been satisfied and that is expressly identified in a completed and mutually approved entry in Schedule 1 as authorized to create, receive, maintain, or transmit PHI. An Approved PHI Feature does not include any feature, integration, configuration, support channel, or service that is not expressly designated and enabled as PHI-capable for Customer.

1.1.3. “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 a feature configured by Customer to make scheduled transmissions.

1.1.4. “Connected-Feature Data” means information that Customer or its authorized users deliberately select, enter, upload, submit, display, or transmit through a Connected Feature and that leaves Customer’s local environment and is received, accessed, or processed by Company or a Company-managed service. Local storage of a source record does not make such a transmission local-only.

1.1.5. “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.

1.1.6. “Breach” has the meaning assigned to that term under HIPAA.

1.1.7. “Business Associate” has the meaning assigned to that term under HIPAA.

1.1.8. “Covered Entity” has the meaning assigned to that term under HIPAA.

1.1.9. “Designated Record Set” has the meaning assigned to that term under HIPAA.

1.1.10. “Electronic Protected Health Information” or “ePHI” means PHI that is transmitted by or maintained in electronic media.

1.1.11. “HIPAA” means the federal laws and implementing regulations governing the privacy, security, breach notification, and permitted use and disclosure of PHI, in each case as amended from time to time.

1.1.12. “Individual” has the meaning assigned to that term under HIPAA and includes a person who qualifies as an Individual’s personal representative.

1.1.13. “PHI” or “Protected Health Information” has the meaning assigned to that term under HIPAA and includes only PHI contained in Connected-Feature Data that Company creates, receives, maintains, or transmits from or on behalf of Customer through an Approved PHI Feature. PHI does not include Local Practice Records that Company does not receive or access. Solely for purposes of safeguards, mitigation, incident reporting, and return, deletion, or other

handling required by applicable law, PHI also includes protected health information that Company actually receives outside an Approved PHI Feature, without authorizing the submission or expanding the scope of the Services.

1.1.14. “Required by Law” has the meaning assigned to that term under HIPAA.

1.1.15. “Secretary” means the Secretary of the United States Department of Health and Human Services or the Secretary’s designee.

1.1.16. “Security Incident” has the meaning assigned to that term under HIPAA.

1.1.17. “Subcontractor” means a person or entity to whom Company delegates a function, activity, or service involving PHI, other than a member of Company’s workforce.

1.1.18. “Unsecured PHI” has the meaning assigned to that term under HIPAA.

1.2. HIPAA terminology. A term used but not otherwise defined in this Addendum has the meaning assigned to it under HIPAA. Any reference to HIPAA includes its applicable implementing regulations, as amended.

1.3. Interpretation. This Addendum shall be interpreted to permit the Parties to comply with HIPAA. No provision authorizes a use or disclosure of PHI that would violate HIPAA if undertaken by Customer, except to the extent HIPAA expressly permits a Business Associate to use or disclose PHI for its own management and administration or to carry out its legal responsibilities.

ARTICLE 2 – Conditional Application

2.1. Activation. This Addendum becomes operative with respect to an Approved PHI Feature only when all Activation Conditions applicable to that feature have been satisfied. The date on which all Activation Conditions are satisfied is the “Activation Date” for that Approved PHI Feature.

2.2. Feature-specific application. Each Approved PHI Feature shall be evaluated separately. Activation of this Addendum for one feature does not activate it for any other feature, service, integration, data flow, or configuration.

2.3. Inactive configurations. If the Activation Conditions are not satisfied, then:

2.3.1. Company is not authorized under the Services Agreement, the DPA, or this Addendum to create, receive, maintain, or transmit PHI through the applicable feature;

2.3.2. Customer shall not enter, upload, submit, display, disclose, transmit, or otherwise make PHI available to Company through that feature;

2.3.3. the applicable feature shall not be represented or treated by either Party as approved for PHI; and

2.3.4. except for the restrictions stated in this Section and provisions that expressly apply regardless of activation, this Addendum imposes no PHI-processing duties on Company with respect to that feature.

2.4. Deactivation. This Addendum ceases to be operative prospectively for an Approved PHI Feature when:

2.4.1. the Parties agree in writing to remove the feature from Schedule 1;

2.4.2. Company permanently disables the feature's ability to create, receive, maintain, or transmit PHI on Customer's behalf and provides written notice to Customer; or

2.4.3. the Services Agreement or this Addendum terminates.

2.5. Unauthorized submission. Customer's submission of PHI through a Connected Feature that is not an Approved PHI Feature does not activate this Addendum, expand the authorized scope of the Services Agreement or DPA, or constitute Company's agreement to process that PHI. Upon discovering such a submission, Company may suspend the affected feature and shall notify the Customer privacy and security contacts identified in Article 5 so that the Parties may arrange for secure deletion, return, or other appropriate handling without repeating PHI in ordinary email. Notwithstanding the conditional scope of this Addendum, Company shall safeguard any PHI it actually receives, mitigate any known harmful effect, provide any notice required by applicable law, and securely return, delete, or otherwise handle the PHI as required by HIPAA or other applicable law.

2.6. Changes to Approved PHI Features. A material change to an Approved PHI Feature's authorized data, purpose, Subcontractors, retention practices, or security configuration requires an updated Schedule 1 entry approved in writing by both Parties before the changed feature may process PHI.

ARTICLE 3 – Permitted Uses and Disclosures

3.1. Performance of services. During the active period for an Approved PHI Feature, Company may use or disclose PHI solely:

3.1.1. to perform the services described for that Approved PHI Feature in Schedule 1, the Services Agreement, and the DPA;

3.1.2. as permitted by this Addendum; or

3.1.3. as Required by Law.

3.2. Minimum necessary. Company shall request, use, and disclose only the minimum PHI reasonably necessary to perform its obligations, consistent with Customer's documented instructions, Schedule 1, and applicable HIPAA requirements.

3.3. Management and administration. Company may use PHI as necessary for its proper management and administration or to carry out its legal responsibilities. Company may disclose PHI for those purposes only if:

3.3.1. the disclosure is Required by Law; or

3.3.2. Company obtains reasonable assurances from the recipient that the PHI will remain confidential, will be used or further disclosed only as Required by Law or for the purpose for

which it was disclosed, and that the recipient will notify Company of any Breach or compromise of confidentiality of which the recipient becomes aware.

3.4. Data aggregation. Company may provide data-aggregation services relating to Customer's health-care operations only if expressly authorized in Schedule 1.

3.5. De-identification. Company may de-identify PHI only if expressly authorized in Schedule 1 and only in a manner that satisfies HIPAA. Company shall not use de-identified information for product development, analytics unrelated to the Approved PHI Feature, advertising, marketing, sale, licensing, model training, or disclosure to third parties unless Customer expressly authorizes the specific use in Schedule 1 and HIPAA permits it.

3.6. Prohibited conduct. Company shall not:

3.6.1. use or disclose PHI except as expressly permitted by this Addendum or Required by Law;

3.6.2. sell PHI or receive remuneration in exchange for PHI except as expressly authorized by Customer in writing and permitted by HIPAA;

3.6.3. use PHI for marketing, targeted advertising, profiling unrelated to the Services, or any independent commercial purpose;

3.6.4. use PHI to train or improve any general-purpose artificial intelligence or machine-learning model;

3.6.5. make any use or disclosure that would violate HIPAA if made by Customer, except as expressly permitted for a Business Associate's management, administration, or legal responsibilities; or

3.6.6. combine PHI received from Customer with information received from another source except as necessary to provide an Approved PHI Feature or as expressly authorized in Schedule 1.

ARTICLE 4 – Safeguards and Security

4.1. Safeguards. Company shall implement and maintain reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI and to prevent any use or disclosure not permitted by this Addendum.

4.2. Electronic PHI. With respect to ePHI, Company shall maintain a written security program reasonably designed to:

4.2.1. ensure the confidentiality, integrity, and availability of ePHI;

4.2.2. protect against reasonably anticipated threats or hazards;

4.2.3. protect against reasonably anticipated impermissible uses or disclosures; and

4.2.4. ensure compliance by Company's workforce.

4.3. Access controls. Company shall limit access to PHI to workforce members and Subcontractors who require access to perform authorized functions and shall apply appropriate authentication, authorization, and access-termination procedures.

4.4. Encryption. Company shall encrypt ePHI in transit and at rest using industry-standard encryption where reasonable and appropriate under the HIPAA Security Rule and appropriate to the nature and sensitivity of the information, except to the extent an alternative control is expressly documented in Schedule 1, approved by Customer, and permitted by HIPAA.

4.5. Risk management. Company shall conduct periodic risk assessments concerning systems that process ePHI and shall address identified risks through a documented risk-management process.

4.6. Personnel. Company shall train workforce members with access to PHI regarding their applicable privacy and security responsibilities and shall impose appropriate sanctions for violations.

4.7. Availability and recovery. To the extent Company is responsible under Schedule 1 for hosting or storing ePHI within an Approved PHI Feature, Company shall maintain reasonable backup, contingency, and recovery procedures consistent with the availability commitments in the Services Agreement. This obligation does not extend to Local Practice Records or Customer-controlled backups that Company does not receive or access.

4.8. Customer responsibilities. Customer remains responsible for:

4.8.1. determining whether its use of an Approved PHI Feature complies with HIPAA and other applicable law;

4.8.2. configuring and using the Approved PHI Feature in accordance with Company's documentation and the limitations in Schedule 1;

4.8.3. managing its users, credentials, devices, networks, and access permissions, and maintaining backups of its Local Practice Records and local databases;

4.8.4. obtaining any authorization, consent, notice, or other legal permission required for Customer's collection or disclosure of PHI; and

4.8.5. refraining from submitting types or categories of PHI identified as prohibited in Schedule 1.

ARTICLE 5 – Reporting and Incident Response

5.1. Impermissible uses and disclosures. Company shall report to Customer without unreasonable delay any use or disclosure of PHI not permitted by this Addendum of which Company becomes aware.

5.2. Breach of Unsecured PHI. Company shall notify Customer of a Breach of Unsecured PHI without unreasonable delay and in no event later than 60 calendar days after discovery.

5.3. Security Incidents. Company shall report a successful Security Incident involving Customer's ePHI without unreasonable delay after discovery and confirmation that Customer's ePHI was affected. The Parties acknowledge that routine unsuccessful attempts to access, use, disclose, modify, or destroy ePHI, including pings, port scans, unsuccessful log-in attempts, denial-of-service attempts, and blocked malicious traffic, occur regularly and need not be reported individually unless they result in unauthorized access to or compromise of ePHI. Company shall make aggregate information regarding such unsuccessful attempts available upon Customer's reasonable written request.

5.4. Discovery. A Breach or Security Incident is deemed discovered on the first day it is known to Company or, through the exercise of reasonable diligence, would have been known to Company.

5.5. Notice contents. To the extent known at the time of notice, Company's notice shall include:

5.5.1. a description of the event, including the date of occurrence and date of discovery;

5.5.2. the identity of each affected Individual or, if identities are not yet known, the affected population and estimated number of Individuals;

5.5.3. the categories and types of PHI involved;

5.5.4. the known or reasonably suspected source and recipient of the PHI;

5.5.5. the corrective and mitigating actions taken or proposed;

5.5.6. the measures Customer should consider taking to protect affected Individuals; and

5.5.7. the name and contact information of Company's incident-response representative.

5.6. Supplemental information. Company may provide available information in stages and shall supplement its notice without unreasonable delay as additional material information becomes available.

5.7. Mitigation and cooperation. Company shall take reasonable steps to mitigate harmful effects of an impermissible use or disclosure and shall reasonably cooperate with Customer's investigation, risk assessment, notifications, regulatory response, and remediation. Neither Party shall notify affected Individuals, regulators, or the media on behalf of the other Party without prior written authorization, except as Required by Law.

5.8. Notice delivery. Notices under this Article shall be delivered to:

5.8.1. **Customer privacy contact:** Customer's then-current privacy contact designated in the Customer Portal or by written notice to Company; if none is designated, Customer's account administrator at the current account email and mailing address in Company's records.

5.8.2. **Customer security contact:** Customer's then-current security contact designated in the Customer Portal or by written notice to Company; if none is designated, Customer's account administrator at the current account email and mailing address in Company's records.

5.8.3. Company privacy and security contact: TQH Research and Development LLC; support@tqhbrain.com; 1576 Bella Cruz Dr #319, The Villages, FL 32159. PHI must not be included in ordinary email; the Parties shall coordinate a secure transmission method.

ARTICLE 6 – Subcontractors

6.1. Permitted Subcontractors. Company may use Subcontractors to support an Approved PHI Feature only as expressly identified and authorized for that feature in Schedule 1, provided that each Subcontractor with access to PHI is covered by a compliant written business associate agreement and all applicable covered-service configurations have been confirmed before the Subcontractor processes PHI.

6.2. Written restrictions. Before permitting a Subcontractor to create, receive, maintain, or transmit PHI, Company shall enter into a written agreement requiring the Subcontractor to comply with restrictions and conditions that are at least as protective of PHI as those applicable to Company under this Addendum and HIPAA.

6.3. Responsibility. Company remains responsible for the performance of its obligations under this Addendum notwithstanding its use of a Subcontractor, subject to the limitations and exclusions in the Services Agreement and applicable law.

6.4. Material changes. A material addition or replacement of a Subcontractor that processes PHI requires at least 30 days' prior written notice to Customer before authorization, except where an emergency requires shorter notice to maintain the security or continuity of an Approved PHI 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 Approved PHI Feature without terminating unaffected Services.

ARTICLE 7 – Individual Rights and Regulatory Cooperation

7.1. Access. If Company maintains PHI in a Designated Record Set, Company shall, within a reasonable time after Customer's written request and in any event within the time necessary for Customer to meet its applicable HIPAA deadline, make the requested PHI available to Customer or, if directed by Customer, to the applicable Individual, in the form and format reasonably requested and as required by HIPAA. This obligation applies only to PHI Company actually holds within an Approved PHI Feature and not to Local Practice Records or copies outside Company's reasonable control.

7.2. Amendment. If Company maintains PHI in a Designated Record Set, Company shall make PHI available for amendment and incorporate amendments as directed by Customer within a reasonable time after receiving Customer's written request, and in any event within the time necessary for Customer to meet its applicable HIPAA deadline, to the extent Company actually holds and can technically amend the PHI within the Approved PHI Feature.

7.3. Accounting of disclosures. Company shall document disclosures of PHI and information relating to those disclosures as necessary for Customer to respond to a request for an accounting. Company shall provide the required information within a reasonable time after receiving Customer's

written request, and in any event within the time necessary for Customer to meet its applicable HIPAA deadline, limited to information available to Company concerning PHI within the Approved PHI Feature.

7.4. Restrictions and confidential communications. Company shall comply with any restriction on use or disclosure or any confidential-communications requirement that Customer notifies Company is applicable to the PHI, to the extent necessary for Customer to comply with HIPAA and technically feasible within the Approved PHI Feature.

7.5. Customer obligations delegated to Company. To the extent Company agrees in Schedule 1 to perform an obligation of Customer under HIPAA, Company shall comply with the requirements applicable to Customer in performing that obligation.

7.6. Records available to the Secretary. Company shall make its internal practices, books, records, policies, and procedures relating to the use and disclosure of PHI available to the Secretary for purposes of determining Customer's or Company's compliance with HIPAA.

7.7. Direct requests. Unless Required by Law or expressly directed by Customer, Company shall promptly forward to Customer any request received directly from an Individual concerning access, amendment, accounting, restriction, or confidential communications and shall not independently respond to the substantive request.

ARTICLE 8 – Customer Representations and Instructions

8.1. Authority to disclose. Customer represents that it has the right and authority to disclose PHI to Company for the purposes described in the Services Agreement, the DPA, and Schedule 1.

8.2. Notices and permissions. Customer shall not request Company to use or disclose PHI in a manner inconsistent with Customer's privacy notice, an applicable authorization, the Services Agreement, the DPA, or HIPAA.

8.3. Limitations. Customer shall notify Company of:

8.3.1. any limitation in Customer's privacy practices that materially affects Company's permitted use or disclosure of PHI;

8.3.2. any revocation or modification of an Individual's permission that materially affects Company's use or disclosure of PHI; and

8.3.3. any restriction on the use or disclosure of PHI that Company must observe.

8.4. Minimum-necessary configuration. Customer shall configure each Approved PHI Feature, assign user permissions, and limit submitted PHI in accordance with the minimum-necessary standard and Schedule 1.

ARTICLE 9 – Term and Termination

9.1. Term. This Addendum begins on the Effective Date but becomes operative for each Approved PHI Feature only as provided in Article 2. It remains in effect until the later of:

- 9.1.1. termination or expiration of the Services Agreement;
- 9.1.2. deactivation of every Approved PHI Feature; or
- 9.1.3. completion of Company's obligations concerning retained PHI.

9.2. Termination for cause. If either Party becomes aware of a material breach of this Addendum by the other Party, the nonbreaching Party shall provide written notice describing the breach. If cure is feasible, the applicable cure period expires 10 calendar days after the breaching Party receives the notice. If the breach is not cured within that period, or if cure is not feasible, the nonbreaching Party may terminate this Addendum and any affected Approved PHI Feature. If termination is not feasible, the nonbreaching Party may take any action required by HIPAA.

9.3. Immediate suspension. Company may immediately suspend access to an Approved PHI Feature to the extent reasonably necessary to prevent or contain an actual or reasonably suspected unauthorized use or disclosure of PHI, provided that Company promptly notifies Customer, limits the suspension to the affected feature where reasonably practicable, and uses reasonable efforts to restore access after the risk has been addressed.

9.4. Return or destruction. Upon termination or deactivation of an Approved PHI Feature, Company shall, at Customer's written direction and if feasible:

- 9.4.1. return or destroy all PHI within Company's possession or control that was received from Customer or created, received, maintained, or transmitted on Customer's behalf;
- 9.4.2. require its Subcontractors to return or destroy such PHI; and
- 9.4.3. retain no copies, except as Required by Law, as expressly authorized in writing by Customer, or temporarily in secure backups or provider recovery systems pending deletion through ordinary lifecycle processes.

9.5. Infeasibility. If Company determines that returning or destroying particular PHI is infeasible, Company shall notify Customer in writing of the conditions that make return or destruction infeasible. Company shall extend the protections of this Addendum to the retained PHI, limit further uses and disclosures to those purposes that make return or destruction infeasible, and delete the PHI when the applicable retention basis ends. Company is not required to delete copies outside its reasonable control that are held by recipients, Customer-configured mailboxes, or independent providers.

9.6. Backup media. PHI retained in secure backup media need not be immediately deleted if immediate deletion is technically infeasible, provided that the PHI remains protected under this Addendum, is not restored or used except for disaster recovery or security purposes, and is deleted in accordance with Company's applicable backup-retention cycle identified in Schedule 1.

9.7. Survival. Company's duties regarding PHI retained after termination or deactivation survive until that PHI is returned or destroyed.

ARTICLE 10 – Allocation of Responsibility

10.1. Services Agreement. Except as expressly modified by this Addendum, the Services Agreement and DPA remain in effect. The Services Agreement's provisions concerning confidentiality, indemnification, limitations of liability, insurance, dispute resolution, and remedies apply to this Addendum except to the extent prohibited by HIPAA or other applicable law. Schedule 1 may not alter liability allocation or remedies.

10.2. No expansion of services. This Addendum does not require Company to provide a feature, functionality, retention period, or service level not included in the Services Agreement, the DPA, or Schedule 1, but nothing in those documents reduces a safeguard or other obligation required by HIPAA or this Addendum.

10.3. No obligations beyond applicable law. Except where this Addendum expressly states a specific standard, timeframe, or commitment, nothing in this Addendum requires Company to undertake any obligation with respect to PHI that exceeds what HIPAA requires of a Business Associate. Any provision capable of more than one reasonable interpretation shall be construed so as not to impose obligations on Company greater than those required by HIPAA.

10.4. Order of precedence. In the event of a conflict: (a) this Addendum controls solely with respect to PHI within the scope of an Approved PHI Feature; (b) the controlling Terms and Privacy Notice control the descriptions of the Services, data flows, feature functionality, retention and deletion limits, and other matters they address; (c) the 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 controlling Terms and Privacy Notice or this Addendum; and (d) a completed Schedule 1 controls over a general description only for the expressly identified feature configuration, permitted data, and processing details, but may not expand a data flow, feature capability, retention or deletion commitment, or other representation beyond the controlling Terms and Privacy Notice, reduce a protection required by this Addendum, or alter liability allocation or remedies.

ARTICLE 11 – General Provisions

11.1. Amendment for compliance. The Parties shall amend this Addendum as reasonably necessary to maintain compliance with changes to HIPAA. Until an amendment becomes effective, the Parties shall interpret this Addendum in a manner consistent with applicable requirements.

11.2. Notices. Except for incident notices governed by Article 5, all notices under this Addendum shall be given in accordance with the notice provisions of the Services Agreement. Notices shall be delivered to the following contacts, as updated by written notice:

11.2.1. Company: TQH Research and Development LLC; 1576 Bella Cruz Dr #319, The Villages, FL 32159; Email: support@tqhbrain.com.

11.2.2. Customer: the Customer identified in the accepted order and execution record; Attention: Customer's then-current privacy contact designated in the Customer Portal or by written notice, or, if none, Customer's account administrator at the current account email and mailing address in Company's records.

11.3. Governing law. Federal law governs matters arising under HIPAA. To the extent state law applies and is not preempted, this Addendum shall be governed by the laws of the State of Florida, without regard to conflict-of-laws principles.

11.4. Venue. Subject to applicable federal law, mandatory protections, and nonwaivable venue rights, any action arising from this Addendum shall be brought in the state courts located in Lake County, Florida, or the federal courts serving that county. Each Party consents to the exclusive jurisdiction of those courts.

11.5. No third-party beneficiaries. This Addendum is solely for the benefit of the Parties and their permitted successors and assigns. It creates no rights in any other person, including any Individual.

11.6. Assignment. A Party may assign this Addendum only together with a permitted assignment of the Services Agreement, unless the other Party consents in writing.

11.7. Severability. If any provision of this Addendum is held invalid or unenforceable, the remaining provisions shall remain in effect, and the invalid or unenforceable provision shall be construed or modified to the minimum extent necessary to make it enforceable while preserving its intended purpose.

11.8. Waiver. A waiver is effective only if in writing and signed by the waiving Party. A waiver of one breach does not waive any other breach.

11.9. Entire agreement. This Addendum, the Services Agreement, the DPA, and each completed Schedule 1 entry constitute the entire agreement between the Parties concerning Company's creation, receipt, maintenance, or transmission of PHI on Customer's behalf and supersede prior discussions concerning that subject, subject to the order of precedence stated in this Addendum.

11.10. Counterparts and electronic signatures. This Addendum may be executed in counterparts, each of which is deemed an original and all of which constitute one instrument. Signatures transmitted or applied electronically shall have the same effect as original signatures.

11.11. Authority. Each person signing this Addendum represents that the person is authorized to execute it on behalf of the identified Party.

[SIGNATURE PAGE FOLLOWS]

SIGNATURE BLOCKS

TQH RESEARCH AND DEVELOPMENT LLC

By: _____

Name: _____

Title: _____

Date: _____

CUSTOMER IDENTIFIED IN THE ACCEPTED ORDER

By: _____

Name: _____

Title: _____

Date: _____

SCHEDULE 1 – APPROVED PHI FEATURE SCHEDULE

This Schedule 1 is incorporated into the Conditional HIPAA Business Associate Addendum between the Customer identified in the accepted order and execution record and TQH Research and Development LLC. A separate entry shall be completed for each feature proposed for use with PHI.

Article 1 – Feature Identification

1. **Feature name.** Secure forms and document exchange.
2. **Feature description.** Company-managed services that process protected form data and attachments for verified submission and retrieval workflows, including the related request and verification emails.
3. **Activation Date.** The date on which Company provides Customer written confirmation that all Activation Conditions for this feature have been satisfied.
4. **Company HIPAA role.** Business Associate when Customer acts as a Covered Entity for the approved workflow; subcontractor Business Associate when Customer acts as a Business Associate for the approved workflow.
5. **Customer role.** Covered Entity or Business Associate, as determined by Customer's actual legal status and activities for the approved workflow.
6. **Subject to BAA:** Yes, only after all Activation Conditions are satisfied.
7. **Subject to DPA:** Yes, for Customer Personal Data processed by Company on Customer's behalf; this Addendum controls in-scope PHI conflicts.
8. **Additional activation conditions.** Completion and mutual approval of this Schedule 1 entry; Company's written designation and enablement of the feature as PHI-capable for Customer; and confirmation, before PHI processing, of all required provider agreements and covered-service configurations, including the actual TQH Microsoft tenant and subscription, the licensed Exchange Online and Microsoft Entra ID services, the sending mailbox and application permissions and configuration, TQH's qualifying covered-entity or business-associate status and HIPAA-eligible use, and the continued effectiveness of the Microsoft HIPAA BAA through the Microsoft DPA without an applicable opt-out.

Article 2 – Authorized Data and Purposes

1. **Permitted PHI.** Recipient email, selected form or document information, attachments, request metadata, submitted content, and verification information, in each case only to the extent constituting PHI authorized for the secure-form workflow.
2. **Prohibited data.** Full payment-card numbers; card security codes; passwords; authentication secrets; and data outside the documented scope of the feature.
3. **Permitted Individuals or populations.** Individuals whose PHI Customer is legally authorized to submit through the approved secure-form or document-exchange workflow.
4. **Permitted purposes.** Customer's treatment, payment, health-care operations, or other HIPAA-permitted purpose specifically configured and documented for the approved workflow.

5. **Authorized users.** Customer workforce members and authorized recipients whom Customer has approved for the workflow, subject to role-based access and minimum-necessary restrictions.
6. **Data sources.** Customer, Customer's authorized users, and authorized recipients who submit information through the approved secure workflow.
7. **Recipients.** Customer, Customer's authorized users, the intended authorized recipient, Company, and approved Subcontractors only as necessary to provide the workflow.
8. **Data aggregation authorized:** No.
9. **De-identification authorized:** No.

Article 3 – Data Flow and Storage

1. **Collection method.** PHI enters the feature when Customer or an authorized recipient submits a secure form, document, or attachment through the Company-managed workflow.
2. **Processing operations.** Receipt, access, storage, encryption, decryption, organization, transmission, retrieval, and deletion reasonably necessary to provide the secure-form and document-exchange workflow.
3. **Storage locations.** Google Cloud and Firebase services (managed database and private storage) are configured for processing in the United States. Microsoft Entra ID and Exchange Online use provider-controlled infrastructure for the configured identity and email services, subject to the applicable Microsoft service terms; Microsoft Graph is used as an access/API mechanism and is not identified here as a separate storage service. Company shall not authorize a material change to these processing-location parameters unless the Parties approve the change in writing before it takes effect and all required HIPAA safeguards and provider agreements are in place.
4. **Transmission methods.** Encrypted transmission through Company-managed services; request email containing a secure link and instructions rather than completed answers or attachments; and a separate email containing the verification code. Microsoft Entra ID authenticates and authorizes Company's configured application access, Microsoft Graph is the access/API mechanism by which the application submits the messages, and Exchange Online sends the request and verification emails through the confirmed TQH mailbox. Microsoft Graph is not represented as independently covered under Microsoft's HIPAA BAA.
5. **Encryption.** form data is application-encrypted in Firestore, attachments are application-encrypted in private Cloud Storage and decrypted by authorized service code for the verified workflow and retrieval, and ePHI is encrypted in transit and at rest.
6. **Customer-controlled components.** Customer devices, networks, user accounts, recipient systems, and access permissions.
7. **Company-managed components.** Company-managed cloud functions, database, and storage used to process the secure-form and document-exchange workflow, together with Company-configured connections to approved provider services used to send request and verification emails.
8. **Backup responsibilities.** Company maintains backup, recovery, continuity, and restoration measures appropriate to Company-managed systems. Customer remains responsible for backing

up its primary Local Practice Records and local databases; Company does not host or maintain a disaster-recovery copy of those records or databases.

Article 4 – Subcontractors

1. Feature Subcontractors (subject to Activation Conditions):

Google Cloud and Firebase services — Function: portal hosting, authentication, cloud processing, storage, database, logging, and scheduling — PHI Access or Processing: stores and processes application-encrypted form data and attachments for the feature — Processing Location: United States, unless the Parties approve another location in writing before processing begins there and all required HIPAA safeguards and provider agreements are in place — Current Status: provider-agreement and HIPAA-eligible covered-service confirmation pending — Activation Condition: the applicable written business associate agreement or other required provider agreement must be in effect, and the services must be configured as HIPAA-eligible covered services, before Activation.

Microsoft Corporation — Services and Function: Microsoft Entra ID authenticates and authorizes Company's configured application access; Microsoft Graph is the access/API mechanism used to submit send requests to the relevant configured Microsoft services; and Exchange Online sends secure-form request and verification emails through the confirmed TQH mailbox — HIPAA Scope: Microsoft identifies Exchange Online and Microsoft Entra ID as in-scope services. Microsoft Graph is not represented as independently covered and may be used for PHI only as the access/API mechanism for the confirmed covered services and configuration — PHI Access or Processing: recipient email addresses and request or verification message content and metadata may be processed, but completed answers and attachments are not intended to be included in those emails — Processing Location: provider-controlled infrastructure used for the configured services, subject to the applicable Microsoft service terms — Provider Agreement: for a qualifying covered-entity or business-associate customer that includes PHI in Customer Data, Microsoft's standard HIPAA BAA is incorporated by default through the Microsoft DPA unless the customer opts out — Current Status: confirmation pending for TQH's actual Microsoft tenant and subscription, licensed Exchange Online and Microsoft Entra ID services, sending mailbox, application permissions and configuration, qualifying status and HIPAA-eligible use, and non-opt-out status — Activation Condition: each listed confirmation must be documented and the Microsoft HIPAA BAA must remain effective before Activation and throughout PHI processing.

2. Subcontractor-specific limitations. No Subcontractor may process PHI for this feature until its role, location, PHI access, covered-service configuration, and required written business associate agreement have been confirmed in this Schedule 1. Company confirms that its separate business associate agreement with PC Planet has been executed; however, PC Planet is not identified or authorized as a Subcontractor for this feature, and its separate agreement does not satisfy or replace any agreement or covered-service configuration required for an application provider.

Article 5 – Retention and Deletion

1. Active retention period. Submitted forms awaiting review are retained while active; Imported, Rejected, Revoked, and Expired requests enter terminal cleanup as described below. No single

fixed retention period applies unless stated in Company's then-current feature documentation or a mutually approved update to this Schedule 1.

2. **Termination deletion period.** Return or deletion occurs in accordance with Article 9 of the Addendum and the feature's ordinary lifecycle processes, subject to infeasibility, legal retention, provider recovery copies, and copies outside Company's reasonable control.
3. **Backup retention.** Secure backup or provider recovery copies are deleted through ordinary lifecycle processes; no fixed period is promised unless documented in a mutually approved update to this Schedule 1.
4. **Legally required retention.** Company may retain PHI only to the extent Required by Law or otherwise permitted by this Addendum, with continued protection and use limited to the applicable retention basis.
5. **Return format.** The then-available secure export or retrieval format supported by the feature, if technically feasible; Customer is responsible for preserving required readable exports and original-document downloads before access ends.
6. **Deletion verification.** Upon reasonable written request, Company will provide written confirmation of deletion completed within Company's possession or control, subject to the retention and control limitations in the Addendum.
7. **Known limitations.** Imported, Rejected, Revoked, and Expired requests enter terminal cleanup; attachment deletion may require retries, and limited metadata may remain.

Article 6 – Operational Requirements

1. **Individual-rights support.** Company will provide the access, amendment, accounting, restriction, and confidential-communications assistance described in Article 7, limited to PHI Company actually holds and functionality available within the feature.
2. **Logging and audit capabilities.** Available request, verification, access, status, transmission, and deletion-event metadata reasonably necessary to operate and secure the workflow and support Customer's HIPAA obligations.
3. **Feature-specific security controls.** Application-level encryption of form data and attachments, access controls, and authentication for the workflow.
4. **Customer configuration requirements.** Customer shall configure the feature, assign user permissions, and limit submitted PHI in accordance with the minimum-necessary standard.
5. **Feature-specific incident instructions.** Article 5 applies. Incident notices must not include PHI in ordinary email; the Parties shall coordinate secure transmission of sensitive details.
6. **Additional limitations or conditions.** Approval is limited to the secure-forms and document-exchange workflow described in this Schedule 1 and does not authorize PHI in appointment reminders, campaigns, Network Center, Bulletin Board, referral directory, ordinary support email, mailbox integrations, or any other Connected Feature not separately approved in writing.

Approved and incorporated into the Addendum by the authorized representatives of the Parties:

CUSTOMER

CUSTOMER IDENTIFIED IN THE ACCEPTED ORDER

By: _____
Name: _____
Title: _____
Date: _____

COMPANY

TQH Research and Development LLC

By: _____
Name: _____
Title: _____
Date: _____