

## MASTER SUBSCRIPTION AGREEMENT

<b>Customer Full Legal Name:</b>	
<b>Customer Address:</b>	

This Master Subscription Agreement (**Agreement**) is between Tympa Health Technologies Limited a limited liability company having its registered office at Landmark, 33 Cavendish Square, London W1G 0PW ("**Supplier**") and the customer named above. This Agreement is effective as of the last date beneath the parties' signatures below (the "**Effective Date**"). The parties agree as follows:

### 1. DEFINITIONS

**Captured Data:** means data and information entered into the Service or captured via the Hardware including all images and procedure results generated by the Software or otherwise produced through use of the Service.

**Confidential Information:** information of commercial value which has been kept confidential by the party from whom the information originates and which has not come into the public domain during the term of this Agreement in breach of any obligation of confidentiality.

**Defect:** an error in the Hardware that causes it to fail to operate substantially in accordance with the relevant Documentation and not caused due to any fault or negligence of the Customer.

**Derived Data:** means data and information created by Supplier using all or part of the pseudonymised Captured Data together with the results of Research and Development.

**Documentation:** the operating manuals, user instructions, technical literature and all other related materials in human-readable and/or machine-readable form supplied to the Customer by the Supplier for aiding the use and application of the Online Service.

**Hardware:** the equipment provided by the Supplier to the Customer and on which the Software is loaded or through which it is accessed and via which the Online Service is accessed.

**Intellectual Property Rights:** all vested contingent and future intellectual property rights including but not limited to copyright, trademarks, service marks, design rights (whether registered or unregistered), patents, know-how, trade secrets, inventions, get-up, database rights and any applications for the protection or registration of these rights and all renewals and extensions thereof existing in any part of the world whether now known or in the future created to which the Supplier may be entitled.

**Location:** the location(s) at which the Hardware is to be installed as specified in the relevant Order Form.

**Research and Development:** the activities described in clause 6.7(a) and clause 6.7(b).

**Software:** the software applications specified in the Order Form and all operating software which is loaded onto or accessed from the Hardware.

**Order Form:** means an ordering document or online order specifying the Service to be provided hereunder that is entered into between Customer and Supplier including any addenda and supplements thereto.

**Online Service:** the provision of access to Customer and its customers to the online database where Captured Data is stored.

**Service:** means provision of the Hardware, the Software and the Online Service.

**Subscription Term:** means the period of time for which the Service is purchased as indicated in the applicable Order Form.

## **2. PROVISION OF SERVICE**

2.1 The Supplier shall, during the Subscription Term, provide the Service to the Customer in accordance with the terms of this Agreement.

2.2 Unless otherwise specified in an Order Form, the Supplier shall use commercially reasonable endeavours to make the Service available 24 hours a day, seven days a week, except for:

- (a) planned maintenance carried out with at least forty-eight (48) hours' notice; and
- (b) unscheduled maintenance performed outside of normal business hours, provided that the Supplier has used reasonable endeavours to give the Customer at least twenty-four (24) hours' notice in advance;
- (c) any unavailability caused by circumstances beyond Supplier's reasonable control, including, for example, an act of God, act of government, flood, fire, earthquake, civil unrest, act of terror, strike or other labour problem (other than one involving Supplier's employees), Internet service provider failure or delay, denial of service attack, or any third party application.

2.3 The Supplier shall provide training to the Customer if, and as, specified in the Order Form.

## **3. SUPPORT SERVICES**

3.1 The Supplier shall ensure that support is available by telephone and e-mail during normal business hours to provide assistance to the Customer in respect of the following:

- (a) remedying Defects in the Hardware;
- (b) provision of bug fixes and patches and online troubleshooting for the Online Services; and
- (c) providing advice on the use of the Service.

3.2 Where the Supplier is required to attend to faults or fix the Hardware and, in the Supplier's reasonable opinion, there is no Defect, or due to fault or negligence of the Customer, including but not limited to breach by Customer of any of its obligations under this Agreement, Supplier shall charge Customer on a time and materials basis at its standard rates then applicable and Customer shall be liable for all associated costs and expenses such as travel, cost of replacement parts or spares, installation costs, which shall be invoiced to Customer by Supplier at cost.

## **4. CUSTOMER OBLIGATIONS**

4.1 The Customer shall:

- (a) use the Service only in accordance with this Agreement, the Documentation, Order Forms and applicable laws and government regulations with respect to its activities under this Agreement;
- (b) use commercially reasonable efforts to prevent unauthorised access to or use of the Service, and shall notify the Supplier promptly of any such unauthorised access or use;

- (c) be responsible for the accuracy, quality and legality of Captured Data and the means by which Customer acquired Captured Data which Customer inputs into the Service including obtaining applicable consent for the transfer of the Captured Data to the Supplier via the Services;
- (d) inspect the Hardware on delivery and notify the Supplier immediately in writing of any Defects in the Hardware;
- (e) be responsible for installing the Hardware at the Location in accordance with the Supplier's instructions unless otherwise agreed with the Supplier;
- (f) use the Hardware in a proper manner and in accordance with any operating instructions issued for it and shall ensure that its staff are properly trained to supervise the use of the Hardware;
- (g) not, without Supplier's prior written approval, allow any person other than a representative of the Supplier to modify, repair or maintain any part of the Hardware;
- (h) not transfer, sell, assign, sub-licence, pledge or otherwise dispose of, encumber or suffer a lien or encumbrance upon or against any interest in the Hardware;
- (i) insure the Hardware for the duration of the Subscription Term;
- (j) notify the Supplier in writing immediately of any loss of or damage to the Hardware and shall indemnify the Supplier against any loss or damage to the Hardware while in the possession of the Customer, ordinary wear and tear excepted;
- (k) remove all Captured Data from Hardware before returning Hardware to Supplier;
- (l) be solely responsible for procuring and maintaining its network connections and telecommunications links from its systems to the Online Service and Supplier's data centres, and all problems, conditions, delays, delivery failures and all other loss or damage arising from or relating to the Customer's network connections or telecommunications links or caused by the internet.

4.2 The Customer shall not access, store, distribute or transmit any harmful software or material including but not limited to Viruses, or any other material during the course of its use of the Service that:

- (a) is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;
- (b) facilitates illegal activity;
- (c) depicts sexually explicit images;
- (d) promotes unlawful violence;
- (e) is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability, or any other illegal activity; or
- (f) causes damage or injury to any person or property.

4.3 The Customer shall not:

- (a) except as may be allowed by any applicable law which is incapable of exclusion by Agreement between the parties:
  - (i) attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Hardware, Software and/or Documentation (as applicable) in any form or media or by any means; or
  - (ii) attempt to reverse compile, disassemble, reverse engineer or otherwise reduce to human-perceivable form all or any part of the Hardware or Software; or
- (b) access all or any part of the Service and Documentation in order to build a product or service which competes with the Service and/or the Documentation; or
- (c) use the Service and/or Documentation to provide services to third parties; or
- (d) license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Service and/or Documentation available to any third party; or
- (e) attempt to obtain, or assist third parties in obtaining, access to the Service and/or Documentation, other than as provided under this Agreement or any Order Form.

4.4 In the event of a Customer's use of any Service in breach of this clause 4 or any other provision of this Agreement, the Documentation or applicable Order Form, without prejudice to any other rights and remedies including the right to terminate, Supplier may suspend the Service until Customer remedies the breach.

4.5 Subject to the Supplier complying with reasonable applicable policies of the Customer, as notified to the Supplier from time to time, the Customer shall allow the Supplier's personnel such access to the Customer's premises as is reasonably necessary for the Supplier to carry out its obligations to the Customer pursuant to this Agreement. The Customer shall provide to the Supplier all permissions necessary to obtain such access.

## **5. CHARGES AND PAYMENT**

5.1 The charges for the Service ordered are set out the Order Form and Customer is responsible for paying all charges as set out in the applicable Order Form. Quantities purchased cannot be decreased during the relevant subscription term.

5.2 Charges will be invoiced in advance and are due thirty (30) days from the date of invoice, unless otherwise specified in the applicable Order Form.

5.3 Customer is responsible for providing complete and accurate billing and contact information to the Supplier and for notifying the Supplier of any changes to such information.

5.4 If the Supplier has not received payment within 30 days after the due date, unless the Customer is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute, without prejudice to any other rights and remedies it may have, the Supplier may, without liability to the Customer, suspend access to the Service while the invoice(s) concerned remain unpaid.

## **6. PROPRIETARY RIGHTS**

6.1 The Customer acknowledges and agrees that the Supplier and/or its licensors own all intellectual property rights in the Service and the Documentation. Except as expressly stated herein, this Agreement does not grant the Customer any rights to, or in, patents, copyrights, database rights, trade secrets, trade names, trademarks (whether registered or unregistered), or any other rights or licences in respect of the Service or the Documentation.

6.2 The Customer shall own all rights, title and interest in and to all of the Captured Data and grants a licence to the Supplier to use such Captured Data in the Derived Data subject to all personal identifiers in such Captured Data having been removed.

6.3 The Supplier shall own all rights, title and interest in and to all of the Derived Data, subject to the Customer's rights in the Captured Data.

6.4 Supplier will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Captured Data. Those safeguards will include, but will not be limited to, measures for preventing access, use, modification or disclosure of Captured Data by Supplier personnel except (a) to provide the Service and prevent or address service or technical problems, (b) as compelled by law in accordance with the "Confidentiality" section below, or (c) as expressly permitted in writing by Customer, and for backing-up Captured Data in accordance with established archiving procedures.

6.5 To the extent that Personal Data is included in Captured Data and Supplier processes any Personal Data contained in Captured Data, on Customer's behalf, within the scope of rendering the Service, the Supplier and Customer agree to such processing in accordance

with the terms of the data processing addendum (**DPA**) attached to this Agreement as Schedule A.

- 6.6 Supplier does not provide a storage or back-up service to the Customer for the Captured Data and does not keep copies of Captured Data. The Supplier shall not be responsible for any loss, destruction, alteration or disclosure of Captured Data.
- 6.7 Subject to compliance with the DPA, Supplier will retain a copy of Captured Data in pseudonymised form for research and statistical analysis for the purpose of:
- (a) developing and improving the Service; and
  - (b) generating anonymised and aggregated data on trends within Captured Data and Supplier may use such anonymised and aggregated data in Supplier's sole discretion, provided that in so doing Supplier does not reveal any information that would enable any third party to identify Customer.

**7. WARRANTIES**

- 7.1 The Supplier warrants that during an applicable Subscription Term the Service will perform materially in accordance with the applicable Documentation. For any breach of this warranty above, Customer's exclusive remedies are repair of Defects or replacement of defective Hardware, or termination in accordance with clause 10.2(b) and refund in accordance with clause 10.3(c).
- 7.2 The warranty in clause 7.1 shall not apply to the extent of any non-conformance which is caused by use of the Service contrary to the Supplier's instructions, or modification or alteration of the Service by any party other than the Supplier or the Supplier's duly authorised contractors or agents.
- 7.3 The Supplier:
- (a) does not warrant that the Customer's use of the Service will be uninterrupted or error-free; nor that the Service, Documentation and/or the information obtained by the Customer through the Service will meet the Customer's requirements; and
  - (b) is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the internet, and the Customer acknowledges that the Service and Documentation may be subject to limitations, delays and other problems inherent in the use of such communications facilities.
- 7.4 In no event shall Supplier be liable for unavailability, inaccuracies, incompleteness or errors in: the data captured or input by the Customer or its customers using the Service; or results provided through Service.
- 7.5 Except as expressly provided herein, each party excludes all warranties, representations, terms, conditions or other commitments of any kind, whether express or implied, statutory or otherwise, and each party specifically disclaims all implied warranties, including (without limitation) any warranties, representations, terms, conditions or other commitments of merchantability or fitness for a particular purpose or of satisfactory quality or of reasonable skill and care, in each case, to the maximum extent permitted by applicable law.
- 7.6 Each party disclaims all liability and indemnification obligations for any harm, damages or other liability caused by any third-party hosting providers.

**8. LIMITATION OF LIABILITY**

- 8.1 This clause 8 sets out the entire financial liability of the Supplier (including any liability for the acts or omissions of its employees, agents and sub-contractors) to the Customer in respect of: (a) any breach of this Agreement; (b) any use made by the Customer of the Service and Documentation or any part of them; and (c) any representation, statement or tortious act or omission (including negligence) arising under or in connection with this Agreement.
- 8.2 Nothing in this Agreement excludes the liability of the Supplier: (a) for death or personal injury caused by the Supplier's negligence; or (b) for fraud or fraudulent misrepresentation.
- 8.3 Subject to clause 8.2:
- (a) the Supplier shall not be liable whether in tort (including for negligence or breach of statutory duty), contract, misrepresentation, restitution or otherwise for any loss of profits, loss of business, depletion of goodwill and/or similar losses or loss or corruption of data or information, or pure economic loss, or for any special, indirect or consequential loss, costs, damages, charges or expenses however arising under this Agreement; and
  - (b) the Supplier's total aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise, arising in connection with the performance or contemplated performance of this Agreement shall be limited to the total fees paid hereunder for the Service giving rise to the liability in the twelve months preceding the first incident out of which the liability arose.

**9. CONFIDENTIALITY**

- 9.1 Each party may be given access to Confidential Information from the other party in order to perform its obligations under this Agreement. A party's Confidential Information shall not be deemed to include information that:
- (a) is or becomes publicly known other than through any act or omission of the receiving party;
  - (b) was in the other party's lawful possession before the disclosure;
  - (c) is lawfully disclosed to the receiving party by a third party without restriction on disclosure; or
  - (d) is independently developed by the receiving party, which independent development can be shown by written evidence.
- 9.2 Each party will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care) to (i) not use any Confidential Information of the other party for any purpose outside the scope of this Agreement and (ii) except as otherwise authorised by the other party in writing, limit access to Confidential Information of the other party to those of its employees and contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements containing protections not materially less protective of the Confidential Information than those herein.
- 9.3 A party may disclose Confidential Information of the other party to the extent compelled by law to do so, provided the party called on to make the compelled disclosure gives the other party prior notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at the other party's cost, if the other party wishes to contest the disclosure.
- 9.4 This clause 9 shall survive termination of this Agreement, however arising.

## 10. TERM AND TERMINATION

- 10.1 This Agreement commences on the Effective Date and continues until the Service ordered hereunder has expired, unless otherwise terminated in accordance with the provisions of this Agreement. The Service shall automatically renew on expiry of the original or preceding Subscription Term for a subsequent term of equal duration to the original Subscription Term at pricing agreed on such renewal unless either party has given notice of non-renewal to the other at least thirty (30) days prior to the expiry of the applicable Subscription Term.
- 10.2 Without prejudice to any other rights or remedies to which the parties may be entitled, either party may terminate this Agreement without liability to the other:
- (a) upon thirty (30) days written notice issued after 12 months of subscription payments have been made, or
  - (b) upon thirty (30) days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period; or
  - (c) immediately on written notice if the other party becomes the subject of a petition in bankruptcy or any other proceeding (whether voluntary or involuntary), relating to insolvency, administration, receivership, administrative receivership, liquidation or assignment for the benefit of creditors or takes or suffers any similar or analogous procedure, action or event in consequence of debt in any jurisdiction.
- 10.3 On termination of this Agreement for any reason:
- (a) all licences granted under this Agreement and the right to use the Service shall immediately terminate;
  - (b) each party shall return and make no further use of any equipment (including Hardware), property, Documentation and other items (and all copies of them) belonging to the other party;
  - (c) Supplier will refund Customer any prepaid fees covering the remainder of the Subscription Term of all Order Forms after the effective date of termination where the Customer has terminated pursuant to clause 10.2;
  - (d) Customer will return all Hardware after having removed all Captured Data from the Hardware;
  - (e) the accrued rights of the parties as at termination, or the continuation after termination of any provision expressly stated to survive or implicitly surviving termination, shall not be affected or prejudiced. In no event will termination relieve Customer of its obligation to pay any fees payable to Supplier for the period prior to the effective date of termination.
- 10.4 Unless the Supplier receives, no later than 25 days after the expiry or termination of this Agreement for any reason, a written request from Customer for the delivery to Customer of the then most recent back-up of the Captured Data, all Captured Data shall be deleted. Upon such request, Supplier shall deliver, to a secure location provided by the Customer (for example SFTP server or cloud repository), a copy of such back-up within 60 days of Supplier's receipt of such request and thereafter delete Supplier's copy of Captured Data, provided that Customer has, at that time, paid all fees and charges outstanding at and resulting from expiry or termination. Customer acknowledges that such data may be in an unstructured format.
- 10.5 Subject to clause 10.4, all Captured Data will be deleted 31 days after contract expiry or termination. Prior to expiry or termination, Customer will be able to extract Captured Data in accordance with this Agreement.

## 11. GENERAL

- 11.1 **Assignment.** Neither party shall, without the prior written consent of the other, assign, transfer, charge, sub-contract or deal in any other manner with all or any of its rights or obligations under this Agreement; provided, however, either party may assign this

Agreement in its entirety (including all Order Forms), without the other party's consent to its affiliate (that is majority owned or controller or under common control) or in connection with a merger, acquisition, corporate reorganisation, or sale of all or substantially all of its assets. Notwithstanding the foregoing, if a party is acquired by, sells substantially all of its assets to, or undergoes a change of control in favour of, a direct competitor of the other party, then such other party may terminate this Agreement upon written notice.

- 11.2 **Force Majeure.** The Supplier shall have no liability to the Customer under this Agreement if it is prevented from or delayed in performing its obligations under this Agreement, or from carrying on its business, by acts, events, omissions or accidents beyond its reasonable control, including, without limitation, strikes, lock-outs or other industrial disputes (whether involving the workforce of the Supplier or any other party), failure of a utility service or transport or telecommunications network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or sub-contractors, provided that the Customer is notified of such an event and its expected duration.
- 11.3 **Notices.** Any notice required to be given under this Agreement shall be in writing and shall be delivered by hand or sent by pre-paid first-class post or recorded delivery post to the other party at its address set out in this Agreement, or such other address as may have been notified by that party for such purposes, or sent by email save that formal legal notices will also be sent by post. Invoices and billing notices shall be sent by email to the address given for such by the Customer in the Order Form.
- 11.4 A notice delivered by hand shall be deemed to have been received when delivered (or if delivery is not in business hours, at 9 am on the first business day following delivery). A correctly addressed notice sent by pre-paid first-class post or recorded delivery post shall be deemed to have been received at the time at which it would have been delivered in the normal course of post. A notice sent by email shall be deemed to have been received at the time of transmission (as shown by the copy of the sent email obtained by the sender).
- 11.5 **Waiver.** A waiver of any right under this Agreement is only effective if it is in writing and signed by the waiving party, and it applies only to the person to whom the waiver is addressed and the circumstances for which it is given. Unless specifically provided otherwise, rights arising under this Agreement are cumulative and do not exclude rights provided by law.
- 11.6 **Severance.** If any provision of this Agreement (or part of a provision) is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions shall remain in force. If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision shall apply with whatever modification is necessary to give effect to the commercial intention of the parties.
- 11.7 **Publicity.** The Customer agrees that Supplier may publicise that the Customer is a customer of Supplier and the Customer agrees to provide Supplier, on Supplier's reasonable request, with testimonials, statements for press releases and to participate in case studies.
- 11.8 **Third Party Rights.** This Agreement, and the documents referred to in it, are made for the benefit of the parties to them and their successors and permitted assigns and are not intended to benefit, or be enforceable by, anyone else.
- 11.9 **Entire Agreement.** The parties agree that this Agreement constitutes the complete and exclusive statement of the Agreement between them with respect to the subject matter of this Agreement, which supersedes all proposals, oral or written, and all other communications between them relating to it. In the event of any conflict between this Agreement and an Order Form, the Order Form shall prevail.



11.10 **Governing law.** This Agreement and any disputes or claims arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) are governed by, and construed in accordance with, the law of England and Wales.

11.11 **Jurisdiction.** The parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that arises out of, or in connection with, this Agreement or its subject matter or formation.

Signed by each party's authorised representative:

**TYMPA HEALTH TECHNOLOGIES LIMITED**

**CUSTOMER**

By: \_\_\_\_\_

By: \_\_\_\_\_

Print Name: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

## SCHEDULE A

### DATA PROCESSING ADDENDUM

The purpose of this Data Processing Addendum (“**DPA**”) is to set out each party's obligations relating to the personal data processed by the parties pursuant to the agreement for the provision of certain services (“**Agreement**”) entered into between them and to which this DPA is attached and incorporated.

#### 1. DEFINITIONS

Defined terms in this DPA shall have the same meaning as set out in the Agreement unless otherwise defined below.

<b>Appropriate Safeguards</b>	means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time.
<b>Applicable Law</b>	means as applicable and binding on Customer, the Supplier and/or the Services:  (a) any law, statute, regulation, by-law or subordinate legislation in force from time to time to which a party is subject;  (b) any court order, judgment or decree; or  (c) any direction, policy, rule or order that is made or given by any regulatory body having jurisdiction over a party.
<b>Controller</b>	means the entity which determines the purposes and means of the Processing of Personal Data.
<b>Customer</b>	means the party named or identified as such in the Agreement being the recipient of the Services.
<b>Data Subject</b>	means the identified or identifiable person to whom Personal Data relates.
<b>Data Subject Request</b>	means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws.
<b>Data Protection Laws</b>	means as applicable and binding on Supplier and the Customer in relation to the Services:  (a) in the United Kingdom the Data Protection Act 2018; and  (b) in member states of the European Union the GDPR and all relevant member state laws or regulations transposing or giving effect to or corresponding with GDPR.
<b>Data Protection Losses</b>	means all losses and liabilities, including all:  (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, expenses, losses and damages; and  (b) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; and

- (c) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and
- (d) the reasonable costs of compliance with investigations by a Supervisory Authority;
- (e) costs of investigation including forensic investigation;
- (f) cost of breach notification including notifications to the Data Subjects; and
- (g) cost of complaints handling including providing Data Subjects with credit reference checks, setting up contact centres (e.g. call centres), producing end customer communication materials, provision of insurance to end customers (e.g. identity theft), and reimbursement of costs incurred by end customers (e.g. changing locks).

**GDPR** means the General Data Protection Regulation (EU) 2016/679.

**Personal Data** means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws.

**Personal Data Breach** means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data.

**Processor** means the entity which Processes Personal Data on behalf of the Controller.

**processing** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (and related terms such as **process** have corresponding meanings).

**Processing Instructions** has the meaning given to that term in clause 3.2.

**Protected Data** means Personal Data in Captured Data provided to the Supplier by the Customer, or otherwise received by the Supplier in connection with the Services, pursuant to the Agreement.

**Services** means the services provided to Customer by the Supplier pursuant to the Agreement.

**Sub-Processor** means another Processor engaged by the Supplier for carrying out processing activities in respect of the Protected Data on behalf of the Supplier.

**Supervisory Authority** means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.

**Supplier** means the party named or identified as such in the Agreement being the provider of the Services.

## 2. ROLES AND OBLIGATIONS

- 2.1 The parties agree that, for the Protected Data, Customer shall be the Controller and the Supplier shall be the Processor.
- 2.2 The parties acknowledge that Supplier also uses some of the Protected Data which is in Derived Data for its own purposes. This is considered to be “Shared Personal Data” of which the parties are Controllers in common. The categories of Shared Personal Data are set out in Exhibit 3 together with the parties' agreement on how to handle the Shared Personal Data.
- 2.3 The Supplier shall process the Protected Data in compliance with:
- (a) the obligations of Processors under Data Protection Laws and so as always not to place Customer in breach of Customer's obligations as a Controller of that Protected Data (subject to Customer complying with Data Protection Laws); and
  - (b) the terms of this DPA.
- 2.4 Customer shall ensure all data it provides to the Supplier for use in connection with the Services shall be collected and transferred to the Supplier in accordance with Data Protection Laws. For the avoidance of doubt, it shall be Customer's responsibility to (i) ensure the terms of use it supplies to the Data Subjects of the Protected Data comply with Data Protection Laws including in particular any fair processing information requirements relating to the processing of the Protected Data by the Supplier and (ii) to ensure it has a legal basis for the processing of the Protected Data by the Supplier.
- 2.5 Customer shall have sole responsibility for the accuracy, quality, and legality of Protected Data and the means by which Customer acquired Personal Data.
- 2.6 Customer shall obtain valid consents from Data Subject in advance for the collection and transfer of Protected Data to the Supplier for processing as contemplated under the Agreement including for use of the Shared Personal Data in accordance with Exhibit 3.

## 3. INSTRUCTIONS

- 3.1 Customer's instructions for the Processing of Protected Data shall comply with Data Protection Law.
- 3.2 Insofar as the Supplier processes Protected Data, the Supplier:
- (a) shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with Customer's documented instructions from time to time and in accordance with Exhibit 1 (Data Processing Particulars), as updated from time to time by written agreement of the parties or as otherwise detailed in the Agreement (“**Processing Instructions**”);
  - (b) shall inform Customer if the Supplier is aware of a Processing Instruction that, in its opinion, infringes Data Protection Laws.

## 4. TECHNICAL AND ORGANISATIONAL MEASURES

- 4.1 The Supplier shall implement and maintain, at its cost and expense:
- (a) the technical and organisational measures prescribed by Data Protection Laws; and
  - (b) taking into account the nature of the processing, the technical and organisational measures necessary to assist Customer insofar as is reasonably possible in the fulfilment of Customer's obligations to respond to Data Subject Requests relating to Protected Data.

4.2 Current data flows and security for the Protected Data are set out at Exhibit 2.

#### **5. SUB PROCESSORS AND STAFF**

5.1 The Supplier has appointed those Sub-Processor(s) listed in Exhibit 1 to this DPA under a written contract containing materially equivalent obligations to those in this DPA. Supplier shall provide Customer with a copy of the agreements with Sub-Processors if requested to do so by Customer. Supplier may redact commercial terms from such agreements before disclosing them to Customer.

5.2 The Supplier shall ensure that all of its personnel and contractors processing Protected Data are subject to a binding written contractual obligation with the Supplier or under professional obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Supplier shall, where practicable and not prohibited by Applicable Law, notify Customer of any such requirement before such disclosure).

5.3 Supplier may not change or add new Sub-Processors without first notifying the Customer and giving the Customer ten days (from date of receipt of the notice) to object to the change or addition in Sub-Processor on reasonable and objectively justifiable grounds.

#### **6. DATA SUBJECT REQUEST ASSISTANCE**

6.1 Supplier shall promptly refer all Data Subject Requests it receives to Customer (wherever practicable within two working days of receipt of the request).

6.2 The Supplier shall provide such assistance to Customer as Customer reasonably requires (taking into account the nature of processing and the information available to the Supplier) to ensure compliance with each party's obligations under Data Protection Laws with respect to:

- (a) Data Subject Requests;
- (b) security of processing;
- (c) data protection impact assessments (as such term is defined in Data Protection Laws);
- (d) prior consultation with a Supervisory Authority regarding high risk processing; and
- (e) notifications to the Supervisory Authority and/or communications to Data Subjects by Customer in response to any Personal Data Breach and for the avoidance of doubt the Supplier must promptly notify Customer in writing of any communications received by it from Data Subjects or Supervisory Authorities relating to the Protected Data without responding to either of the same unless it has been expressly authorised to do so by Customer.

#### **7. OVERSEAS TRANSFERS**

7.1 To the extent required under Data Protection Laws, Supplier shall ensure that any transfers (and any onward transfers) of Protected Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws of the foregoing territories, are effected by way of Appropriate Safeguards and in accordance with such Data Protection Laws.

#### **8. RECORDS AND AUDITS**

8.1 The Supplier shall maintain written records of all categories of processing activities carried out on behalf of Customer.

8.2 The Supplier shall make available to Customer such information as is reasonably necessary to demonstrate its compliance with the obligations of Processors under Data Protection Laws, and shall allow for and contribute to audits, including inspections, by Customer (or another auditor mandated by Customer) for this purpose, subject to Customer:

- (a) giving the Supplier at least 30 days' advance notice of such information request, audit and/or inspection being required; and
- (b) Customer and Supplier mutually agreeing the scope, timing, and duration of the audit; and
- (c) ensuring that all information obtained or generated by Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law). Customer shall provide a copy of such information and audit reports to the Supplier following an inspection or audit pursuant to this clause 8.

## **9. BREACH NOTIFICATION**

9.1 In respect of any Personal Data Breach involving Protected Data, the Supplier shall without undue delay and within 24 hours of becoming aware of the Personal Data Breach:

- (a) notify Customer of the Personal Data Breach; and
- (b) so far as possible without prejudicing the continued security of the Protected Data or any investigation into the Personal Data Breach, provide Customer with details of the Personal Data Breach.

## **10. DELETION OR RETURN OF DATA**

10.1 The Supplier shall return all the Protected Data to Customer in accordance with clause 10.4 and clause 10.5 of the Agreement.

10.2 Following termination, Customer acknowledges and agrees that Supplier may anonymise a copy of Protected Data (to the extent it has not already been anonymised prior to termination) and Supplier may continue to use such anonymised Protected Data for its own business purposes including Research and Development.

## **11. LIABILITY**

11.1 If a party receives a compensation claim from a person (including but not limited to a Data Subject) relating to processing of Protected Data processed by the Supplier under this Agreement, it shall promptly provide the other party with notice and full details of such claim. The Supplier shall make no admission of liability nor agree to any settlement or compromise of the relevant claim in relation to its processing activity without the prior written consent of Customer.

11.2 This clause 11 does not affect the liability of the Supplier to any Data Subject or Supervisory Authority pursuant to a claim made directly against the Supplier by either of them.

11.3 As between the Supplier and the Customer liability for all Data Protection Losses arising out of any breach of this Data Processing Addendum including for any loss or damage arising out of a Personal Data Breach, and for the mutual indemnity in respect of Shared Personal Data as set out in Exhibit 3, shall be subject to the same caps and exclusions on liability as set out in the Agreement.

## **12. CHANGE IN LAW**

Notwithstanding anything to the contrary in this DPA, in the event: (i) of a change in any law or regulation or (ii) a regulator issues a binding instruction, order or requirement which

changes the basis on which the Protected Data can be processed, transferred or stored pursuant to this DPA, the parties agree to negotiate in good faith to agree an amendment to this DPA and that Agreement (to the extent necessary) to address change in law or regulation or to comply a binding instruction, order or requirement as applicable.

**EXHIBIT 1  
DATA PROCESSING PARTICULARS**

**1. Subject-matter of processing:**

Data of customers of Customer and electronic images and media of Tympanic Membrane (ear drum) and ear canal for analysis of hearing health.

**2. Duration of the processing:**

Subject to Clause 10 of this DPA, Supplier will Process Personal Data for so long as necessary to perform the Services, unless otherwise agreed upon in writing.

**3. Nature and purpose of the processing:**

To use the Protected Data for the purpose of providing the Services and as otherwise detailed in the Agreement, and as further instructed by Customer in its use of the Services.

**4. Categories of Personal Data:**

- Name or unique patient reference number
- Date of birth
- Electronic media of Tympanic Membrane (ear drum) and ear canal
- Medical appointment times and dates

Special Category Data:

- current medication
- health status
- medical history

**5. Categories of Data Subjects:**

- Individuals undergoing hearing health clinic

**6. Processing Instructions**

To use the Protected Data for the purpose of providing the Services and as otherwise detailed in the Agreement.

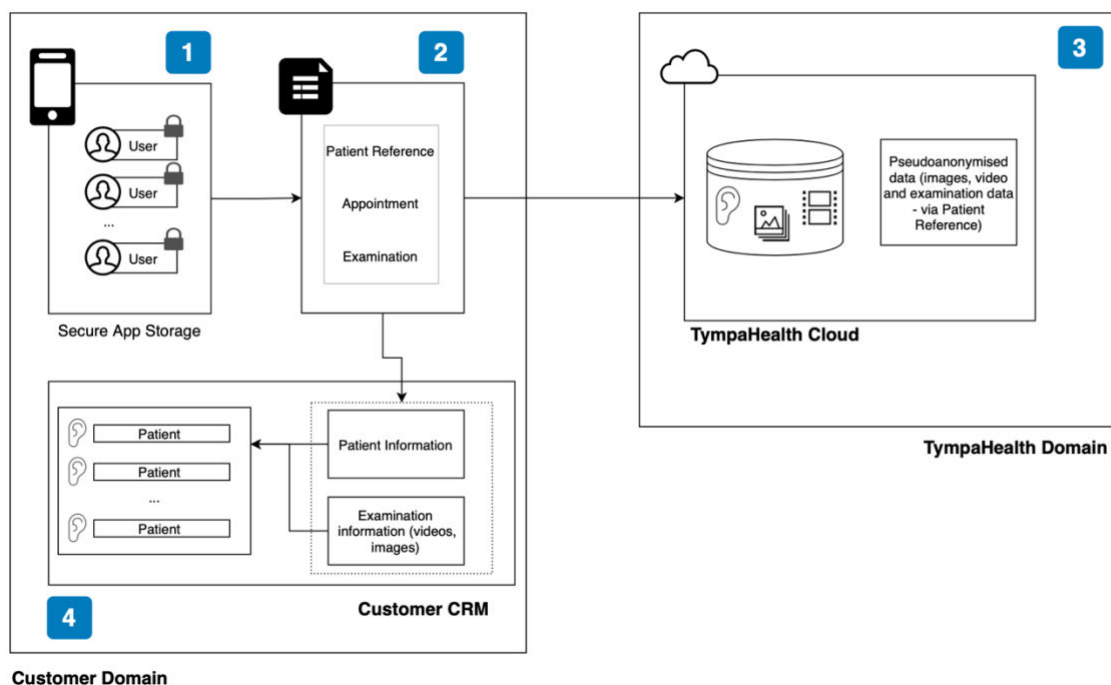
**7. Sub-Processors**

<b>Name</b>	<b>Location</b>	<b>Processing Activity</b>
Google Inc (Google Cloud)	London, United Kingdom	Cloud hosting provider (with no logical access to data)



**EXHIBIT 2****TympaHealth Data Flows and Security**

Customer Data



- 1** All information captured in the app is stored in either database or files in the secure app storage area of the mobile operating system which is only accessible by the app (no additional encryption at rest is required). The files are separate for each logged in user in the app and loaded to phone memory upon user login (with pin or password).
- 2** The data stored contains patient details, appointment details, examinations performed. All media (photos and videos) captured during examination are also stored in the secure app documents storage area and are referenced to appointments and examinations by file name.
- 3** Data upload is performed using REST API using HTTPS protocol with latest TLS versions. When logging in, users are granted tokens which must be supplied when making calls to the APIs in request header. Without tokens the requests will fail. API uses Nginx web server with PHP running as fpm and stores information in Postgresql database. All internal traffic within cloud server infrastructure is internal and cannot be eavesdropped (see infrastructure diagram).
- 4** Data is retrieved using REST API using https protocol with latest TLS versions. Every request requires a valid token in the header. The token defines the scope of access to data. Tokens are granted by an Oath2 compatible authentication server. Supplying valid credentials creates and provides a JWS token which must be

version 17.08.21

supplied in each API request. The tokens have limited lifespan and must be renewed when expired.

**EXHIBIT 3**  
**SHARED PERSONAL DATA**

**1. Categories of Shared Personal Data**

The following are categories of Shared Personal Data and the identified purposes for which each party uses the Shared Personal Data (“**Agreed Purposes**”).

Category of Data	Customer Purpose	Supplier Purpose
<ul style="list-style-type: none"> <li>• Patient reference number</li> <li>• Electronic media of Tympanic Membrane (ear drum) and ear canal;</li> </ul>	Use of the Services	Research and Development

**2. Particular obligations relating to Shared Personal Data.**

Each party shall:

- (a) ensure that it has all necessary notices and consents in place to enable lawful collection and use and transfer of the Shared Personal Data to Permitted Recipients (as defined in sub-clause 2(d) below for the Agreed Purposes;
- (b) give full information to any data subject whose personal data may be processed under this Agreement of the nature such processing. This includes giving notice that, on the termination of this Agreement, personal data relating to them may be retained by or, as the case may be, transferred to one or more of the parties, their successors and assignees;
- (c) process the Shared Personal Data only for the Agreed Purposes;
- (d) not disclose or allow access to the Shared Personal Data to anyone other than the parties to this Agreement, the employees of each party, any third parties engaged to perform obligations in connection with the Agreement, the specialist consultants engaged by the Supplier to review the electronic media of Tympanic Membrane (ear drum) and ear canal (“**Permitted Recipients**”);
- (e) ensure that all Permitted Recipients are subject to written contractual obligations concerning the Shared Personal Data (including obligations of confidentiality) which are no less onerous than those imposed by this DPA;
- (f) ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- (g) not transfer any Shared Personal Data outside the EEA unless the party doing so ensures that Appropriate Safeguards are in place;

- (i) only retain Shared Personal Data for so long as necessary to fulfil the Agreed Purpose and applying the criteria for determining retention as set out in any privacy notice or other information notice given to data subjects of such Shared Personal Data.

**3. Mutual assistance.**

Each party shall assist the other in complying with all applicable requirements of the Data Protection Laws. In particular, each party shall:

- (a) consult with the other party about any notices given to data subjects in relation to the Shared Personal Data;
- (b) promptly inform the other party about the receipt of any data subject access request;
- (c) provide the other party with reasonable assistance in complying with any data subject access request;
- (d) not disclose or release any Shared Personal Data in response to a data subject access request without first consulting the other party wherever possible;
- (e) assist the other party, at the cost of the other party, in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Laws with respect to security, Personal Data Breach notifications, data protection impact assessments and consultations with supervisory authorities or regulators;
- (f) notify the other party without undue delay on becoming aware of any breach of the Data Protection Laws;
- (g) use compatible technology for the processing of Shared Personal Data to ensure that there is no lack of accuracy (i) maintain complete and accurate records and information to demonstrate its compliance with this clause 3(g) and allow for audits by the other party or the other party's designated auditor in accordance with the terms of clause 8 of the DPA which shall apply mutatis mutandi to the Customer for the purposes of Shared Personal Data; and
- (h) provide the other party with contact details of at least one employee as point of contact and responsible manager for all issues arising out of the Data Protection Laws, including the joint training of relevant staff (as applicable), the procedures to be followed in the event of a Personal Data Breach, and the regular review of the parties' compliance with the Data Protection Laws.

**4. Indemnity.**

Each party shall indemnify the other against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred by the indemnified party arising out of or in connection with the breach of this Exhibit 3 affecting Shared Personal Data, provided that the indemnified party gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend and/or settle it.

version 17.08.21