This Supplier Data Sharing Agreement (the "DSA") sets out how “we” (also “us”; “our”; Medigold Health) and “you” (also the Supplier) will act with respect to the processing of Personal Data by each of us in connection with the Services provided under the Contract.

This DSA is supplemental to the Contract but is maintained separately and may be updated by us from time to time. It has effect upon the creation of the Contract and the term of this DSA will mirror the term of the Contract (subject to any obligations that may extend beyond the term of the Contract).

In case of any conflict or inconsistency between this DSA, part of the Contract or a Data Processing Addendum, unless otherwise expressly agreed between the parties in writing, the following order of precedence will apply:

(a)a Data Processing Addendum;

(b)the Data Processing Particulars;

(c)this DSA;

(d)the Order (not including the Data Processing Particulars); and

(e)the Purchasing Terms and Conditions.

1. Definitions

1.1 In this DSA:

"Business Data" means Personal Data processed by the Supplier as Controller for general business administration purposes in connection with the Contract.

"Contract" has the meaning given in the Purchasing Terms and Conditions.

"Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processor", "process", "processing", "Data Subject" and "Special Category Data" each have the meaning given to them in UK GDPR (as defined below).

"Customer Data" means Personal Data relating to Medigold Health's customers and their staff that may be processed by the Supplier.

"Data Processing Addendum" means a separate addendum executed between the parties that specifies data processing details.

"Data Processing Particulars" means the data processing particulars applicable to the processing contemplated by this DSA and the Order, in the form set out in Appendix 1.

"Data Protection Laws" means all applicable data protection and privacy legislation, regulations and guidance including:

(a) Regulation (EU) 2016/679) (as incorporated into UK legislation by way of the European Union (Withdrawal Agreement) Act 2020 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020, together forming the "UK GDPR") and the Privacy and Electronic Communications (EC Directive) Regulations 2003;

(b)the Data Protection Act 2018; and

(c)all applicable law about the processing of Personal Data and privacy; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data.

"International Transfer" means any transfer of Personal Data from the UK to a third country or international organisation.

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of Personal Data to third countries that do not benefit from an adequacy decision which are approved by the ICO under UK GDPR (for the avoidance of doubt this includes an "International Data Transfer Agreement (IDTA)" per s119A DPA 2018).

"ICO" means the UK Information Commissioner's Office (including any successor or replacement body).

"Order" means any Order or Goods Specification or Services Specification (as defined in the Contract).

"Purchasing Terms and Conditions" means our Purchasing Terms and Conditions located at https://legal.medigold-health.com/suppliers#purchasing-terms-and-conditions from time to time.

1.2 Defined terms not otherwise defined in this DSA will have the meanings given in the Contract.

2. Processing relationships and applicable provisions

2.1 The parties acknowledge that Medigold Health is a Controller and the Supplier's role as one or more of Controller, Processor, or Sub-Processor is determined by the specific Services being provided and the purposes for which Personal Data is processed by it in connection with those Services, and as specified in the applicable Order or Data Processing Addendum.

2.2 Unless otherwise specified in a Data Processing Addendum, the following processing scenarios shall apply:

2.2.1Controller Processing: Where the Supplier processes Personal Data as an independent Controller for its own business purposes (including Business Data for general business administration and Customer Data for the Supplier's own purposes); and/or

2.2.2Processor/Sub-Processor Processing: Where the Supplier acts as a Processor or Sub-Processor processing Business Data and/or Customer Data on behalf of Medigold Health, where Medigold Health is the Controller or is the Processor (on behalf of its customers) respectively.

2.3 Joint controllership is not anticipated; if it arises, the parties shall enter into a written arrangement under Article 26 UK GDPR.

2.4 The Order will set out the Data Processing Particulars applicable to the Order in the form set out in Appendix 1 – Data Processing Particulars Template. The applicable processing scenarios will be identified in the Data Processing Particulars but for the avoidance of doubt the facts and circumstances will dictate the relationship. Both processing scenarios may apply to a single Service where different types of processing occur.

2.5 Where the Order specifies that a separate Data Processing Addendum applies, the terms of that addendum shall take precedence over the standard processing provisions for the relevant processing activities.

3. Controller processing provisions

3.1 Where the Supplier acts as an independent Controller in respect of Personal Data, the Supplier shall:

3.1.1process Personal Data lawfully, fairly and transparently and only for the purposes disclosed to Data Subjects;

3.1.2ensure it has a lawful basis for processing Personal Data under the Data Protection Laws;

3.1.3implement appropriate technical and organisational measures to ensure data security;

3.1.4provide clear privacy notices to Data Subjects regarding its processing of Personal Data;

3.1.5respond to requests from Data Subjects to exercise their rights in respect of Personal Data;

3.1.6retain Personal Data for no longer than necessary for the purposes for which it is processed;

3.1.7where processing is likely to result in a high risk to the rights and freedoms of Data Subjects, conduct Data Protection Impact Assessments and prior consultations with the ICO as required under UK GDPR;

3.1.8notify Medigold Health within 48 hours of the Supplier becoming aware of any Personal Data Breach and comply with Data Protection Laws regarding notification to relevant Data Subjects;

3.1.9only appoint processors with Medigold Health's prior written approval and shall remain fully liable for their acts and omissions;

3.1.10not transfer Personal Data outside the UK without appropriate safeguards in place;

3.1.11not use Personal Data for purposes incompatible with those disclosed to Data Subjects;

3.1.12 coordinate with Medigold Health regarding any overlapping Data Subject requests or regulatory inquiries; and

3.1.13 provide contact details for its Data Protection Officer (if appointed) or designated data protection contact.

4. Processor/Sub-Processor processing provisions

4.1 Where the Supplier acts as a Processor or Sub-Processor in respect of Personal Data, Medigold Health will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of Personal Data to the Supplier.

4.2 The Supplier shall, in relation to Personal Data processed as a Processor or Sub-Processor:

4.2.1 process Personal Data only in accordance with documented written instructions from Medigold Health, only for the specific purposes set out in the Order or Data Processing Addendum, and only to the extent necessary for the performance of the Services;

4.2.2 maintain the confidentiality of Personal Data and not disclose it to third parties without Medigold Health's prior written consent, except as required by law;

4.2.3 only appoint sub-processors with Medigold Health's prior written approval and shall remain fully liable for their acts and omissions;

4.2.4 implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to protect against unauthorised processing and accidental loss or destruction of Personal Data, including encryption of data at rest and in transit where appropriate;

4.2.5 not transfer Personal Data outside the UK or EEA without Medigold Health's prior written consent and appropriate safeguards;

4.2.6 assist Medigold Health in responding to Data Subject requests and compliance obligations;

4.2.7 notify Medigold Health within 24 hours of the Supplier becoming aware of any Personal Data Breach;

4.2.8 inform Medigold Health immediately if, in its opinion, any instruction infringes the Data Protection Laws;

4.2.9 assist Medigold Health in ensuring compliance with its obligations under Articles 32 to 36 of the UK GDPR (including security, breach notification, data protection impact assessments and consultations with supervisory authorities);

4.2.10 delete or return Personal Data upon termination unless required by law to retain it; and

4.2.11 maintain records demonstrating compliance, make available to Medigold Health all information necessary to demonstrate compliance with Data Protection Laws, and permit audits by Medigold Health.

5. Mutual obligations

5.1 Both parties will comply with all applicable requirements of the Data Protection Laws. This DSA is in addition to, and does not relieve, remove or replace, a party's obligations or rights under the Data Protection Laws.

5.2 Both parties agree that they will at all times respect medical confidentiality and comply with all relevant Data Protection Laws.

5.3 Where both parties process the same Personal Data as independent Controllers, they shall reasonably assist each other to ensure Data Subjects can effectively exercise their rights.

5.4 Both parties shall maintain records of processing activities under their responsibility in accordance with Article 30 of UK GDPR and make such records available to the ICO upon request.

5.5 Any International Transfer of Personal Data by either party must comply with Chapter V of UK GDPR and be based on an adequacy decision or appropriate safeguards such as a Standard Contractual Clauses.

6. Notices

6.1 Notifications to the Supplier in relation to this DSA should be sent to the contact specified in the Order or otherwise notified to Medigold Health.

6.2 Notifications to Medigold Health will be sent to dpo@medigold-health.com.

6.3 Notice requirements shall otherwise be governed by the Contract.

7. Variation

7.1 Subject to clause 7.2, no variation of this DSA will be effective unless signed in writing by both parties.

7.2 Either party may propose to update this DSA on 30 days' written notice to reflect changes in Data Protection Laws or regulatory guidance.

8. Indemnification

8.1 The Supplier shall indemnify, defend, and hold Medigold Health harmless from and against any and all claims, damages, losses, costs, and expenses (including reasonable fees) arising out of or resulting from:

8.1.1the Supplier's breach of this DSA;

8.1.2the Supplier's violation of Data Protection Laws;

8.1.3any claim by a Data Subject relating to the Supplier's processing of Personal Data; or

8.1.4any regulatory action or penalty imposed by the ICO or other supervisory authority on Medigold Health relating to the Supplier's processing activities.

9. Severability

9.1 If any provision of this DSA is held to be invalid, illegal, or unenforceable, the validity, legality, and enforceability of the remaining provisions shall not be affected or impaired thereby, and such provision shall be deemed modified to the minimum extent necessary to make such provision valid, legal, and enforceable.

10. Governing law and jurisdiction

10.1 This DSA shall be governed by and construed in accordance with the laws of England and Wales.

10.2 Any disputes arising out of or in connection with this DSA shall be subject to the exclusive jurisdiction of the courts of England and Wales.

• • •

Appendix 1 – Data Processing Particulars

Please fill out the following form with regard to the relationship scenarios set out in clause 2 of the DSA:

Data Processing Role:

☐ Data Controller ☐ Data Processor ☐ Both (if both you must provide a copy of this form for each role)

Data Subjects (tick all that apply):

☐ Medigold Health staff and contractors

☐ Medigold Health's Customers' staff and contractors (i.e. Medigold Health service users)

☐ Members of the public

☐ Applicants / Candidates

☐ Private patients / service users

☐ Supplier staff and contractors

☐ Prospective customer staff

☐ Other (specify): _____

Personal Data Categories:

☐ Contact details and identifiers

☐ Employment details

☐ Financial information

☐ Communication records

☐ Other (specify): _____

Special Category Data Categories:

☐ Data concerning health ☐ Racial or ethnic origin ☐ Sex life or sexual orientation ☐ Trade Union membership ☐ None ☐ Other (specify): _____

Processing Purposes:

☐ Contact management and communication

☐ Invoice processing and payment

☐ Provision of Services

☐ Compliance and audit purposes

☐ Other (specify): _____

Lawful Basis:

☐ Consent ☐ Legitimate interests ☐ Legal obligation

☐ Other (specify): _____

Retention Period / Deletion Trigger:

☐ For the duration of the contract only (DEFAULT)

☐ _____ months/years after contract termination or service completion

☐ Until data are returned or deleted upon written instruction

☐ As required by applicable law or regulation (specify)

☐ Other (specify): _____

Data Protection Contact: _____

Data Location:

☐ UK only ☐ EEA ☐ Other (specify): _____

DPIA Required (Controller only): ☐ Yes ☐ No (rationale): _____