Data Protection Addendum

Last updated: January 2, 2025

This Data Protection Addendum ("Addendum") forms part of the agreement in place between Customer and Signant Health covering Customer's use of Signant Health's Products and/or Services ("Agreement"), unless otherwise agreed in the Agreement. Unless otherwise defined in this Addendum, all capitalized terms shall have the meanings given to them in the Agreement.

1. **Definitions.** For purposes of this Agreement, the following terms have the following meanings:

   The terms "Controller", "Data Subject", "Personal Data", "Process", "Processed", "Processes", "Processing", "Processor" and "Supervisory Authority" have the meaning set out under Applicable Data Protection Law, or where not specifically defined under Applicable Data Protection Law, the same meaning as analogous terms in Applicable Data Protection Law. For example: (i) where the EU GDPR or UK GDPR is applicable, "Controller" means the person or entity that determines the purposes and means of Processing Personal Data, and where the CCPA is applicable includes any "business" as that term is defined by the CCPA, and (ii) where the EU GDPR or UK GDPR is applicable, "Processor" means an entity that processes Personal Data on behalf of a Controller, and where the CCPA is applicable includes any "service provider" as that term is defined by the CCPA.

   "CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

   "Data Exporter" means a Controller or a Processor which is transferring Personal Data directly or via onward transfer to a country that triggers additional requirements for the protection of Personal Data being transferred in accordance with Applicable Data Protection Law.

   "Data Importer" means a Controller or a Processor which receives Personal Data directly from a Data Exporter, or via onward transfer, and that is in a country that triggers additional requirements for the protection of Personal Data being transferred in accordance with Applicable Data Protection Law.

   "Applicable Data Protection Law" means any applicable data protection laws, each as updated from time to time, of the European Union, the European Economic Area, Switzerland, the United Kingdom, the United States, or any other jurisdiction that governs or otherwise applies to In-Scope Personal Data Processed under the Agreement, including but not limited to, as applicable, European Data Protection Law, UK Data Protection Law and US Data Protection Law.

   "EU Standard Contractual Clauses" or "EU SCCs" means Module II, III and IV, as applicable to the Services, for the transfer of Personal Data to third countries pursuant to Regulation (EU)

2016/679 of the European Parliament and the Council as approved by EC Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

"UK Standard Contractual Clauses" or "UK SCCs" means the International Data Transfer Addendum to the European Commission's standard contractual clauses for international data transfers from the United Kingdom.

"EU GDPR" means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

"UK GDPR" means the Data Protection Act 2018, as amended from time to time, in the United Kingdom.

"European Data Protection Law" means the EU GDPR, any successor thereto, and any other Law relating to the data protection or privacy of individuals that applies in the European Economic Area.

"FADP" means the Federal Act on Data Protection of 19 June 1992 (SR 235.1).

"FDPIC" means the Swiss Federal Data Protection and Information Commissioner.

"In-Scope Personal Data" means any Personal Data provided to Signant Health by Customer in connection with the Agreement or that is acquired, collected, generated, or otherwise Processed by Signant Health on behalf of Customer in connection with the Agreement, as set forth in Annex I.B of the EU Standard Contractual Clauses.

"Security Incident" means any actual or reasonably suspected accidental, unlawful, or unauthorised loss, destruction, alteration, access, use, disclosure of, damage or corruption to In-Scope Personal Data.

"Subprocessor" means any person or entity contracting with Signant Health who Processes In-Scope Personal Data on behalf of Signant Health.

2. **Relationship of the parties**

2.1. The parties agree that with respect to the provision of the Services, if Customer is the Sponsor of the Study, Customer is the Controller of the In-Scope Personal Data and Signant Health is the Processor of such In-Scope Personal Data. If Customer is not the Sponsor, then Customer is the Processor of the In-Scope Personal Data and Signant Health is the Sub-Processor of such In-Scope Personal Data.

2.2. Each party represents, warrants, and undertakes to perform its obligations in connection with the Agreement, including the Processing of In-Scope Personal Data, in accordance with the Applicable Data Protection Law.

3. Scope and Operation

3.1. This Addendum applies to Signant Health's Processing of In-Scope Personal Data in providing the Services to Customer in accordance with the Agreement.

3.2. The details associated with Signant Health's Processing of In-Scope Personal Data in provision of the Services are set forth in Annex I.B of the EU Standard Contractual Clauses.

4. Signant Health Obligations

4.1. Signant Health shall not be entitled to use, sell or otherwise Process In-Scope Personal Data for any reason other than to provide to Customer the Services defined in the Agreement and only for the duration of time stipulated in the Agreement, as well as to comply with Customer's documented instructions, including with regard to transfers of In-Scope Personal Data to a third country or an international organization, unless otherwise required by Applicable Data Protection Law. In this case, Signant Health shall inform Customer of the relevant legal requirement prior to such Processing, unless Signant Health is legally prohibited from informing Customer of the requirement. Signant Health will notify Customer if it believes any instructions from Customer violate Applicable Data Protection Law.

4.2. Signant Health shall not disclose or transfer In-Scope Personal Data to any third party except as permitted by this Agreement or as required by Applicable Data Protection Law.

4.3. Signant Health shall implement appropriate technical and organisational measures to protect In-Scope Personal Data against accidental or unlawful destruction or accidental loss, including deletion, alteration, including corruption, unauthorised disclosure, use or access.

4.4. Signant Health shall ensure that In-Scope Personal Data are accessible only to Signant Health staff on a need-to-know basis and that such staff have been suitably trained, will only process In-Scope Personal Data on instructions from Customer and have committed themselves to confidentiality according to the nature of the In-Scope Personal Data they will be Processing.

5. Customer Obligations

5.1. To the extent required under Applicable Data Protection Law, Customer shall obtain explicit consent from Data Subjects with respect to the Processing of Personal Data and obtain

separate/unbundled explicit consent from Data Subjects with respect to the transfer of In-Scope Personal Data to Signant Health and comply with other requirements as required by the Applicable Data Protection Law.

5.2. Customer shall be solely responsible for compliance with any notification obligations to Data Subjects or Supervisory Authorities and for all related costs, except to the extent that a Security Incident was solely the fault of Signant Health. Signant Health shall never notify Data Subjects, Supervisory Authorities or any other third parties without the prior written consent of the Customer.

6. Subprocessors

6.1. Signant Health may use Subprocessors to carry out specific processing activities subject to the terms of this Section 6. Signant Health shall only engage Subprocessors which provide sufficient guarantees as to the protection of Personal Data.

6.2. Prior to giving any Subprocessor access to or responsibilities in relation to In-Scope Personal Data, Signant Health shall ensure that such Subprocessor has entered into a legally binding agreement with Signant Health requiring that the Subprocessor abide by terms for the protection of In-Scope Personal Data not less protective than those in this Addendum.

6.3. Customer consents to Signant Health engaging third party Subprocessors to process In-Scope Personal Data to the extent necessary to provide the Services provided that Signant Health maintains an up-to-date list of its Subprocessors available at this link. Signant Health will provide details of any change in Subprocessors to Customer as soon as reasonably practicable. Signant Health will give written notice no less than ten (10) days prior to any such change. If Customer reasonably protests the replacement or addition of a Subprocessor, the parties will work together in good faith to find a suitable solution to resolve the issue.

6.4. Signant Health shall remain fully liable for any In-Scope Personal Data Processed by its Subprocessors.

7. Security Incidents

7.1. Signant Health shall notify Customer without undue delay after becoming aware of any Security Incident and such notification will include, where possible, the categories and approximate number of Data Subjects concerned, and approximate number of In-Scope Personal Data records concerned.

7.2. Signant Health shall promptly implement, at Signant Health's expense, to the extent that the Security Incident was due to a breach of Signant Health obligations under this Addendum, corrective measures necessary remedy the causes of the Security Incident.

7.3. Signant Health shall inform Customer of all corrective measures implemented and remediation efforts undertaken.

8. <u>International Data Transfers</u>

8.1. The EU Standard Contractual Clauses will apply where In-Scope Personal Data that is subject to the EU GDPR is transferred from a Data Exporter to a Data Importer. The EU Standard Contractual Clauses can be accessed via https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en and are deemed to be incorporated into this Addendum in their entirety and without alteration, except as specified in this Addendum.

8.1.1. If Customer is the Data Controller and Customer, or a third party acting on behalf of Customer, transfers, under or in connection with the Agreement, any EU-originating In-Scope Personal Data to Signant Health or any of Signant Health's affiliates located outside the EEA in a country which has not been recognized by the EU Commission to ensure an adequate level of data protection pursuant to Art. 45(1) GDPR, the parties agree that such transfer shall be subject to Module 2 (Controller to Processor Transfer) of the EU Standard Contractual Clauses as specified in Attachment A to this Addendum.

8.1.2. If Signant Health or an affiliate of Signant Health located within the EEA transfers, under or in connection with the Agreement, any In-Scope Personal Data to a Customer that is a Data Controller and is located outside the EEA in a country which has not been recognized by the EU Commission to ensure an adequate level of data protection pursuant to Art. 45(1) GDPR, the parties agree that such transfer shall be subject to Module 4 (Processor to Controller Transfer) of the EU Transfer Clauses as specified in Attachment A to this Addendum.

8.1.3. A) If Customer is a Data Processor and Customer, or a third party acting on behalf of Customer, transfers, under or in connection with the Agreement, any EU-originating In-Scope Personal Data to Signant Health or any of Signant Health's affiliates located outside the EEA in a country which has not been recognized by the EU Commission to ensure an adequate level of data protection pursuant to Art. 45(1) GDPR, or

B) If Signant Health or any of its affiliates transfers, under or in connection with the Agreement, any EU-originating In-Scope Personal Data to a Data Processor Customer or to a third party acting on behalf of Customer that is located outside the EEA in a country which has not been recognized by the EU Commission to ensure an adequate level of data protection pursuant to Art. 45(1) GDPR, the parties agree that such transfer shall be subject to Module 3 (Processor to Processor Transfer) of the EU Standard Contractual Clauses as specified in Attachment A to this Addendum.

8.2. For transfers of In-Scope Personal Data from a UK Data Exporter to a country that has not been recognized by the UK Government to ensure an adequate level of data protection, the EU Standard Contractual Clauses (as referred to above in section 8.1) and the UK Standard Contractual Clauses Addendum, which can be accessed at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf are applicable as specified in Attachment A to this Addendum.

8.3. To the extent that the Data Exporter is established in Switzerland and transfers In-Scope Personal Data related only to Swiss data subjects to a country that has not been recognized by the Swiss Government to ensure an adequate level of data protection, the FADP applies to the transfers of In-Scope Personal Data therefore the EU Standard Contractual Clauses apply to the transfer with the adjustments specified in Attachment A to this Addendum.

8.4. In the event the EU Standard Contractual Clauses are amended, replaced, or repealed by the European Commission, the United Kingdom, or under Applicable Data Protection Law, the parties shall work together in good faith to enter into an updated version of the EU Standard Contractual Clauses, to the extent required, or negotiate in good faith a solution to enable a transfer of In-Scope Personal Data to be conducted in compliance with Applicable Data Protection Law.

8.5. If, at any time Data Protection Law requires any further steps to be taken in order to permit the transfer of In-Scope Personal Data to the Data Importer as envisaged under this Agreement, including, without limitation, executing or re-executing the EU Standard Contractual Clauses as separate documents setting out the proposed transfers, and entering into additional country-specific cross-border transfer clauses, then the parties shall work together in good faith to take all steps reasonably required to ensure that the transfer of In-Scope Personal Data meets the requirements of Applicable Data Protection Law.

8.6. In the event of any conflict between the EU Standard Contractual Clauses and the provisions of this Addendum and any other agreement between the parties existing at the time the EU Standard Contractual Clauses are agreed or entered into thereafter, the EU Standard Contractual Clauses shall prevail.

9. Cooperation and Assistance

9.1. Signant Health shall co-operate with Customer to assist Customer with its obligations under Applicable Data Protection Law, including without limitation security breach notification, privacy impact assessments or consultation obligations with Supervisory Authorities.

9.2. Signant Health shall also notify Customer within five (5) business days if it receives any communication from a Data Subject, Supervisory Authority, government authority or other party relating to In-Scope Personal Data. Signant Health shall not respond to any such

request unless obligated to do so under Applicable Data Protection Law or requested to do so by Customer. Signant Health shall provide reasonable and timely assistance to help Customer respond to any such requests related to In-Scope Personal Data where Customer has a legal obligation to respond within a given time limit.

9.3. Signant Health shall make available to Customer any information Customer may require for purposes of demonstrating compliance with Customer's obligations under Applicable Data Protection Law in connection with the Agreement.

10. Term and Termination

10.1. On any termination or expiry of the Agreement, completion of the Services, or when instructed by Customer in writing, Signant Health shall cease all operations on In-Scope Personal Data and shall, at Customer's direction, return and/or, to the extent feasible, delete all In-Scope Personal Data Processed by Signant Health under the Agreement and instruct its Subprocessors to do the same. Should deletion not be feasible, Signant Health shall keep the In-Scope Personal Data confidential and not Process the In-Scope Personal Data for any other purpose. Subject to the foregoing, Signant Health shall complete the return and/or erasure of In-Scope Personal Data within sixty (60) days of termination or expiry of the Agreement between the parties.

10.2. The obligations under this Addendum shall expressly survive termination or expiry of the Agreement.

11. Record Keeping and Audits

11.1. Each party shall maintain all records required by Applicable Data Protection Law, including in respect of its Processing of In-Scope Personal Data.

11.2. Upon reasonable written notice at mutually agreeable times and during regular business hours, subject to the confidentiality obligations set forth in the Agreement, Signant Health will permit Customer and its representatives access to Signant Health's premises, facilities, and personnel to conduct an audit of records Signant Health is required to create or maintain under this Agreement or Applicable Data Protection Law, for the purposes of evaluating and verifying: (i) compliance with the requirements of this Addendum; and/or (ii) compliance with Applicable Data Protection Law.

12. Miscellaneous

12.1. **Updates**. Signant Health may update the terms of this Addendum from time to time when an update is required as a result of (a) changes in Applicable Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material

changes to any of the existing Services. The updated terms will form part automatically of the Agreement. When material updates are made, Signant Health will notify Customer.

ATTACHMENT A

I. EU Standard Contractual Clauses (EU SCCs)

A. When **Module 2** applies:

i. Clause 7 of the EU SCCs - Docking Clause applies;

ii. the following provision under Clause 9(a) of Module 2 of the EU SCCs applies:
"*The data importer has the data exporter's general authorisation for the engagement of sub-Processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-Processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.*"

iii. the following provision under Clause 13(a) of Module 2 of the EU SCCs applies:
"The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority."

iv. the following provision under Clause 17 of Module 2 of the EU SCCs applies:
"*These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland."*

v. the following provision under Clause 18(b) of Module 2 of the EU SCCs applies:
"The parties agree that those shall be the courts of Ireland."

vi. See Annex I, Annex II and Annex III for the details of the data exporter and data importer, the description of the transfer and the technical and organisational security measures and the details of the sub-processors.

B. When **Module 3** applies:

i. Clause 7 of the EU SCCs - Docking Clause applies;

ii. the following provision under Clause 9(a) of Module 3 of the EU SCCs applies:
"*The data importer has the data exporter's general authorisation for the engagement of sub-Processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-Processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-*

processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object."

iii. the following provision under Clause 13(a) of Module 3 of the EU SCCs applies:
"The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority."

iv. the following provision under Clause 17 of Module 3 of the EU SCCs applies:
"*These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland."*

v. the following provision under Clause 18(b) of Module 3 of the EU SCCs applies:
"The parties agree that those shall be the courts of Ireland."

vi. See Annex I, Annex II and Annex III for the details of the data exporter and data importer, the description of the transfer and the technical and organisational security measures and the details of the sub-processors.

C. When **Module 4** applies:

i. Clause 7 of the EU SCCs - Docking Clause applies;

ii. the following provision under Clause 17 of Module 4 of the EU SCCs applies:
"*These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland."*

iii. the following provision under Clause 18 of Module 4 of the EU SCCs applies:
"Any dispute arising from these Clauses shall be resolved by the courts of Ireland."

iv. See Annex I, Annex II and Annex III for the details of the data exporter and data importer, the description of the transfer and the technical and organisational security measures and the details of the sub-processors.

II. UK Standard Contractual Clauses Addendum (UK SCCs)

With respect to the UK SCCs Addendum, the parties agree that:

(i) with respect to Table 1 of the UK SCC Addendum, the details of the data exporter and data importer are set forth in Annex I;

(ii) with respect to Table 2 of the UK SCC Addendum, the version of the SCCs in force at the date of execution of this Addendum applies;

(iii) with respect to Table 3 of the UK SCC Addendum, (a) the description of the parties is set forth in Annex I, (b) the details of the processing are set forth in Annex I, and (c) the description of the technical and organisational security measures are set forth in Annex II;

(iv) with respect to Table 4 of the UK SCC Addendum, no parties may end the UK SCC Addendum as set out in Section 19 of the UK SCC Addendum.

III. Adjustments to the EU Standard Contractual Clauses for In-Scope Personal Data transfers from Switzerland

A. To the extent that the Data Exporter is established in Switzerland and transfers In-Scope Personal Data related only to Swiss data subjects to a non-adequate country, the FADP applies to the transfers of In-Scope Personal Data and, therefore, the following adjustments to the EU SCCs shall apply:
(i) Annex I.C under Clause 13 of the SCCs:
"With regard to the Swiss entity as a data exporter, the competent supervisory authority is the Federal Data Protection and Information Commissioner ("FDPIC")";
(ii) Clause 17 of the SCCs:
"*The law governing the Standard Contractual Clauses is Swiss law*;"
(iii) The use of the term 'EU Member State' in the SCCs must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 of the SCCs;
(iv) References to the GDPR in the EU SCCs are to be understood as references to the FADP; and
(v) The EU SCCs also protect the data of legal entities until the entry into force of the revised FADP.

B. To the extent that the Data Exporter is established in Switzerland and transfers In-Scope Personal Data related also to EEA data subjects to a non-adequate country, or if the transfers of In-Scope Personal Data are otherwise subject to the extraterritoriality provisions of the EU GDPR (Article 3), the FADP and the GDPR apply in parallel to the transfers of In-Scope Personal Data. In this case, the Parties agree that the GDPR standard will apply to the transfers of In-Scope Personal Data because the GDPR provides adequate protection and data subjects are consequently not disadvantaged as a result of the transfers. The following adjustments to the SCCs shall apply:

(i) Annex I.C under Clause 13 of the EU SCCs: With regard to the Swiss entity as a data exporter, the competent supervisory authorities are the FDPIC, insofar as the transfers of In-Scope Personal Data are governed by the FADP, and the EEA competent supervisory authority as indicated in Annex I.C of the EU SCCs, insofar as the transfers of In-Scope Personal Data are governed by the GDPR;
(ii) the use of the term 'EU Member State' in the EU SCCs must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 of the EU SCCs;
(iii) the details of the data exporter and data importer are set forth in Annex I of this Addendum;
(iv) the description of the transfer are set forth in Annex I of this Addendum,
(v) the description of the technical and organisational security measures are set forth in Annex II;
(vi) the details of the sub-processors are set forth in Annex III of this Addendum;

ATTACHMENT B

ANNEX I

A. LIST OF PARTIES

Unless otherwise specified in the Agreement, the parties set forth the following:

Data exporter(s):
Name: Signant Health Global Solutions Limited, unless otherwise specified in the Agreement
Address: As described in the Agreement

Contact information: As described in the Agreement.

Activities relevant to the data transfer under these Clauses: to provide the Services as described in the Agreement

Signature and date: see Agreement signature

Role: data processor

Data importer(s): Customer

Name: As described in the Agreement

Address: As described in the Agreement

Contact information: As described in the Agreement.

Activities relevant to the data transfer under these Clauses: the reception of the Services provided by Signant Health, as described in the Agreement

Signature and date: see Agreement signature

Role: data controller or data processor, as described in the Agreement or in section 2.1. of the Addendum

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred

- Clinical trial participants / patients
- Investigator/investigator site staff
- Customer personnel and/or study sponsor personnel

Categories of personal data transferred

Depending on which Service Signant Health provides to the Customer, Signant Health may collect the following categories of Personal Data:

- From site personnel: name, contact information, job title, work address, education, certifications, work experience, video or audio image, username, password, account logs, information about trainings;
- From Customer and/or study sponsor personnel: name, contact information, job title, work address, username, password, account logs;
- From clinical trial participants: study subject ID, initials, name, signature, email address, phone number, home address, date of birth, health information, gender, video or audio image, visit dates, randomization data, username, password, account logs, device ID, if the device was provided by Signant Health. Some of the applications, e.g., the TrialMax application, may also collect location data to enable Bluetooth connections to study devices.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Key-coded/pseudonymised health related data of clinical trial participants

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)

Continuous basis.

Nature of the processing

Personal Data will be subject to the following basic processing activities:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organization, and structuring
- Using data, including analysing, and consultation
- Updating data, including correcting, adaptation, alteration, alignment, and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion

Purpose(s) of the data transfer and further processing

Provide Services in support of clinical studies sponsored by the study sponsor for the development and testing of medicines.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

For the duration of the Services under the Agreement unless otherwise instructed by Customer or to comply with applicable laws, including with tax or legal obligations or Applicable Data Protection Law to which Signant Health is subject.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing:

See Annex III.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

See Attachment A.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by Signant Health (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Signant Health implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the In-Scope Personal Data is Processed. This is accomplished by:

- establishing security areas;
- securing the data processing equipment;
- establishing access authorizations for staff and third parties, including the respective documentation;
- access to data centres is logged and monitored; and
- data centres are protected by appropriate security measures.

Access Control to Data Processing Systems

Signant Health implements suitable measures to prevent its data processing systems from being used by unauthorized persons. This is accomplished by:

- identification of the terminal and/or the terminal user to the data importer systems;
- automatic time-out of user terminal if left idle, identification and password required to reopen;
- automatic turn-off of the user ID when several erroneous passwords are entered, log file of events (monitoring of break-in-attempts);
- issuing and safeguarding of access/identification codes;
- staff policies and training in respect of each staff access rights to In-Scope Personal Data (if any), informing staff about their obligations; and
- utilisation of audit trail.

Access Control to Use Specific Areas of Data Processing Systems

Signant Health commits that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by its access permission (authorization) and that In-Scope Personal Data cannot be read, copied, or modified or removed without authorization. This shall be accomplished by:

- staff policies and training in respect of each staff member's access rights to the In-Scope Personal Data;
- allocation of individual user accounts;

- utilisation of audit trail;
- release of data to only authorized persons; and
- control of files, controlled and documented destruction of data.

Availability Control

Signant Health implements suitable measures to ensure that In-Scope Personal Data are protected from accidental destruction or loss. This is accomplished by:

- infrastructure redundancy; and
- data redundancy via data backup.

Transmission Control

Signant Health implements suitable measures to prevent the In-Scope Personal Data from being read, copied, altered, or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by:

- use of appropriate firewall and encryption technologies; and
- as far as possible, all data transmissions are logged and monitored.

Input Control

Signant Health implements suitable measures to ensure that it is possible to check and establish whether and by whom In-Scope Personal Data have been input into data processing systems or removed. This is accomplished by:

- an authorization policy for the input of data, as well as for the reading, alteration, and deletion of stored data (role-based access management rules);
- authentication of the authorized personnel;
- utilization of user codes (passwords);
- all users who have access to In-Scope Personal Data shall reset their passwords as specified in the relevant password policy; and
- areas housing the computer hardware and related equipment are capable of being locked.

Data Importer System Administrators

Signant Health implements suitable measures to monitor its system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs and keep them secure, accurate and unmodified for a reasonable period; and
- keeping an updated list with system administrators' identification details (e.g., name, surname, function, or organizational area) and tasks assigned.

Separation of Processing for Different Purposes

Signant Health implements suitable measures to ensure that data collected for different purposes and different customers can be Processed separately. This is accomplished by:

- access to data is separated through application security for the appropriate users; and
- modules within Signant Health's database separate which data is used for which purpose, i.e., by functionality and function.

ANNEX III

LIST OF SUBPROCESSORS

See list available here.

ATTACHMENT C

Additional Safeguards to the EU Standard Contractual Clauses

1. The Data Importer will assess whether the Laws applicable to it provide adequate protection under European Data Protection Law. To the extent that it determines that any such Laws are not in line with the requirements of the EU Standard Contractual Clauses and European Data Protection Law, it undertakes to comply with the safeguards set out in paragraphs 2 to 5 below.

2. The Data Importer undertakes to adopt supplementary measures to protect the In-Scope Personal Data transferred under the EU Standard Contractual Clauses from the Data Exporter ("**SCC Personal Data**") in accordance with the requirements of European Data Protection Law, including by implementing appropriate technical and organizational safeguards, such as encryption or similar technologies, access controls or other compensating controls, to protect SCC Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security.

3. The Data Importer warrants that:

(a) it has not purposefully created any means by which a public authority can bypass the Data Importer's security mechanisms, authentication procedures and/or software to gain access to and/or use its systems and/or the SCC Personal Data, such as a back door or similar programming;

(b) it has not purposefully created or changed its business processes, security mechanisms, software and/or authentication procedures in a manner that facilitates access to its systems and/or the SCC Personal Data by public authorities; and

(c) it is not required by national law or government policy to create or maintain any means to facilitate access to its systems and/or the SCC Personal Data by public authorities, such as a back door, or for the data importer to be in possession or to hand over the encryption key to access such data.

4. Any audits, including requests for reports or inspections, carried out by the Data Exporter or a qualified independent assessor selected by the Data Exporter (the "Independent Assessor") of the processing activities will include, at the choice of the Data Exporter and/or Independent Assessor, verification as to whether any SCC Personal Data has been disclosed to public authorities and, if so, the conditions under which such disclosure has been made.

5. If the Data Importer receives a legally binding request for access to the SCC Personal Data by a public authority, the Data Importer will:

(a) promptly notify the Data Exporter of such request to enable the Data Exporter to intervene and seek relief from such disclosure, unless the Data Importer is otherwise prohibited from providing such notice, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If the Data Importer is so prohibited and in the event that, despite having used its reasonable best efforts, the Data Importer is not permitted to notify the Data Exporter, it will make available on an annual basis general information on the requests it received to the Data Exporter and/or the competent Supervisory Authority of the Data Exporter;

(b) promptly inform the public authority if, in the Data Importer's opinion, such request is inconsistent and/or conflicts with its obligations pursuant to the Standard Contractual Clauses. The Data Importer will document any such communication with the public authorities relating to the inconsistency and/or conflict of such request with the Standard Contractual Clauses;

(c) not make any disclosures of the SCC Personal Data to any public authority that are determined to be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society; and

(d) upon request from the Data Exporter, provide general information on the requests from public authorities it received in the preceding 12-month period relating to SCC Personal Data. Where possible, such information will include the following:

(i) an overview of Laws that permit access to the SCC Personal Data in the jurisdiction to which the Data Importer is subject, to the extent the Data Importer is reasonably aware of such laws;

(ii) any measures taken to prevent access by public authorities to the SCC Personal Data;

(iii) information about the nature and number of such requests received by the Data Importer;

(iv) the type of data requested;

(v) the requesting body;

(vi) the legal basis to disclose the SCC Personal Data to the public authority; and

(vii) whether the Data Importer reasonably believes that it is legally prohibited to provide the information in subsections (i) to (vi) above and, if so, the extent to which such promotion applies.