Data Processing Exhibit to Medidata Services Agreement

This Data Processing Exhibit (the "**Exhibit**") forms part of the underlying Agreement, inclusive of any amendments to the Agreement, by which Medidata Solutions, Inc. (together with any of its Affiliates that provide Services, collectively, "**Medidata**") provides the Services to Customer and reflects the parties' agreement with regard to the Processing of Personal Data (as defined below) in accordance with the requirements of the applicable Privacy Laws. The parties agree to comply with the provisions of this Exhibit with respect to any Personal Data. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1 DEFINITIONS

1.1 **Definitions in Privacy Laws.** Without limitation, the definitions in this Section 1 shall be construed as informed by their corresponding defined terms in Privacy Laws, where available. In the event these definitions restrict or reduce the scope of related definitions under Privacy Laws, the definition shall be expanded to match the definition under that Privacy Law. In the absence of a definition under this Section 1, a term shall be interpreted in a manner compliant with Privacy Laws.

1.2 "**Additional Products**" means products, services and applications (whether made available by Medidata or a third party) that are not part of the Services.

1.3 "**Customer**" means the relevant entity that has entered into an Agreement with Medidata to receive the Services, and if applicable, any of its Authorized Affiliates that have signed the Agreement or any Sales Orders related thereto, whether referred to in that Agreement as a Customer, Business Partner and/or Partner.

1.4 "**Customer Data**" has the same meaning as in the Agreement (whether referred to as Customer Data or Partner Data). Customer Data excludes User Registration Data (as defined in Section 3.2 herein).

1.5 "**Data Controller**" means the entity that determines the purposes and means of the Processing of Personal Data.

1.6 "**Data Processor**" means the entity that Processes Personal Data on behalf of the Data Controller.

1.7 "**Data Subject**" means the individual to whom Personal Data relates (including clinical subjects, customer users or other clinical personnel).

1.8 **"Data Subject Request**" means a Data Subject's request to access, correct, amend, transfer, block or delete that person's Personal Data consistent with that person's rights under Privacy Laws.

1.9 "**Instructions**" has the same meaning as in the Agreement; where not set forth in the Agreement, "Instructions" means all provisions of the Agreement, any Sales Orders, and any written amendments to either, concerning the Processing of Customer Data.

1.10 "**Personal Data**" has the meaning set forth in Privacy Laws, namely (and without limitation) any information relating to an identified or identifiable person, including sensitive data, where such data is submitted to Medidata as part of Customer Data for Processing pursuant to the Instructions.

1.11 "**Personal Data Breach**" has the meaning set forth in Privacy Laws, namely (and without limitation) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed. For clarity, any reference in the Agreement to the defined term "Security Incident" shall mean Personal Data Breach as defined in this Exhibit.

1.12 "**Privacy Assistance Materials**" means those materials Medidata provides to its general customer base as information on the Services' Processing of Customer's Personal Data and, where required under Privacy Laws, as assistance for Customer's data protection impact assessment(s), data transfer impact assessment(s), and/or prior consultations with Regulators. Privacy Assistance Materials will include, at a minimum, Medidata's current security certifications and reports, such as its SOC 1 and/or SOC 2 audit reports (or comparable industry-standard successor reports) and ISO/IEC 27001:2013 Certification available at Medidata's Trust & Transparency Center (www.medidata.com/trust).

1.13 "**Privacy Laws**" has the same meaning as in the Agreement; where not set forth in the Agreement, "Privacy Laws" means all applicable laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, applicable to the Processing of Personal Data under the Agreement, and including the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**"), all as amended from time to time.

1.14 "**Process**", "**Processes**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, including the collection, recording, organization, storage, updating, modification, retrieval, consultation, use, transfer, dissemination by means of transmission, distribution or otherwise making available, merging, linking as well as blocking, erasure or destruction.

1.15 "**Regulator**" means any supervisory authority with authority under Privacy Laws over all or any part of the provision or receipt of the Services or the Processing of Personal Data.

1.16 "**Security Program**" means the administrative, organisational and technical controls as set out in the Privacy Assistance Materials and in **Attachment B** to this Exhibit.

1.17 "**Services**" has the same meaning as in the Agreement.

1.18 "**Standard Contractual Clauses**" means, to the extent each applies as required by Privacy Laws, (a) the Standard Contractual Clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council pursuant to Commission implementing decision (EU) 2021/914 of 4 June 2021, as set out in **Attachment C** to this Exhibit (together with its Annexes, which are incorporated as **Attachments A and B** of this Exhibit) by and between Customer and Medidata, which the parties agree may be replaced or updated in accordance with a relevant European Commission decision (as applicable to the EU) or Swiss Federal Data Protection and Information Commissioner (FDPIC) decision (as applicable to Switzerland), and (b) the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses under S119A(1) of the Data Protection Act 2018, as set out at https://www.medidata.com/wp-content/uploads/2022/09/Medidata_UK-Addendum-for-International-Transfer_2022.pdf, by and between Customer and Medidata, which the parties agree may be replaced or updated in accordance with a relevant Information Commissioner's Office decision.

1.19 "**Subprocessor**" means any Data Processor engaged by Medidata for Processing or having authorized access to Personal Data as part of the subcontractor's role in delivering the Services.

1.20 "**Transfer Impact Assessment**" means the transfer impact assessment required pursuant to Clause 14 of the Standard Contractual Clauses, as set out in **Attachment D** to this Exhibit.

2 SUBJECT-MATTER, DURATION, NATURE AND PURPOSE OF THE PROCESSING, TYPE OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

2.1 **Subject-matter of the Processing**. The Processing is carried out in an automated Process using Medidata's IT systems and procedures. The Processing operations are further set out in **Attachment A** (Details of Data Processing).

2.2 **Duration of the Processing**. The Processing begins and ends with performance of the Services for Customer, as specified in the Instructions.

2.3 **Nature and Purpose of the Processing**. The purpose and object of the Processing of Personal Data by Medidata is to perform and provide the Services pursuant to the Instructions, as specified in the Agreement and this Exhibit, on behalf of and for the benefit of Customer.

2.4 **Type of Personal Data and Categories of Data Subjects**. The type of Personal Data and categories of affected Data Subjects are set out in **Attachment A** (Details of Data Processing).

3 INSTRUCTIONS, COMMITMENT TO CONFIDENTIALITY

3.1 **Controller Processor Relationship**. Other than as set forth in Section 3.2 below, Medidata shall only Process Personal Data on behalf of the Customer. The parties acknowledge that with respect to the Processing of Personal Data, and as between the parties, Customer acts as the Data Controller and Medidata acts as the Data Processor (e.g., even where Customer is a data processor on behalf of another data controller, as between the parties to this Agreement, Customer will act as the Data Controller).

3.2 **Independent Controller Relationship for Authorized Users**. Medidata, Customer and other Medidata customers are each independent controllers with respect to the registration data provided by site-based investigators and other Authorized Users of Medidata's hosted portal application, including without limitation, name, email, address, and training records ("**User Registration Data**"). Nothing in this Section 3.2 shall relieve Medidata or Customer of its obligations as otherwise set forth in the Agreement.

3.3 **Business Contact Data**. Each party may receive names, mailing addresses, email addresses and/or phone numbers of the personnel of the other party that are necessary to the ordinary business relationship with that other party ("**Business Contact Data**"). Each party will ensure that it is legally entitled to and has taken the necessary steps to enable it to: (a) provide such Business Contact Data to the other party; and (b) authorise the other party to Process such Business Contact Data for the purpose of maintaining the parties' business relationship, including the provision or receipt of Services under the Agreement. Each party will only process Business Contact Data for the purposes of their relationship and the Agreement.

3.4 **Customer's Processing of Personal Data**. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Privacy Laws, including any applicable requirement to provide notice to Data Subjects of the use of Medidata as Processor (and where Customer is a Processor, by ensuring that the ultimate Controller does so). Customer is responsible for assessing the sufficiency of Medidata's Security Program, including determining whether the Services are appropriate for Processing of Personal Data subject to Privacy Laws, and for using the Services in a manner consistent with Customer's legal and regulatory obligations. Customer shall ensure that its Instructions to Medidata comply with Privacy Laws, and that its use of the Services will not violate the rights of any Data Subject. Customer has sole responsibility for the accuracy, quality, and legality of Personal Data made available for Medidata's Processing pursuant to the Instructions.

3.5 **Instructions**. Other than User Registration Data (as set forth in Section 3.2 above), Medidata shall only Process Personal Data on behalf of Customer and in accordance with the Instructions. Medidata shall protect Personal Data as Confidential Information. The Instructions are Customer's complete and final instructions to Medidata for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately with prior written agreement between Customer and Medidata. For the purposes of Clause 8.1 (a) of the Standard Contractual Clauses, the following is included as an instruction in the Instructions by Customer to Process Personal Data: (a) Processing in accordance with the Agreement, applicable Sales Order(s), and this Exhibit; and (b) processing initiated by Authorized Users in their use of the Services. Where Medidata believes that compliance with any Customer's Instructions infringes Privacy Law, Medidata shall immediately notify Customer thereof.

3.6 **Commitment to Confidentiality**. Medidata shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have committed themselves to confidentiality. Medidata shall ensure that such confidentiality obligations survive the termination of the personnel engagement. Medidata restricts its personnel from Processing Data without authorization as described in the Security Program and ensures that access to Personal Data is limited to those personnel who require such access to perform the Agreement.

3.7 **Compliance with Laws**. Each party will comply with all laws, regulations and rules applicable to it in the performance of this Exhibit, including Privacy Laws.

4 SECURITY OF PERSONAL DATA

4.1 **Security Controls**. At all times during the Processing of the Personal Data, Medidata will take and implement the appropriate administrative, organizational and technical controls as set out in the Security Program. These controls are designed to ensure an appropriate level of security of the Personal Data, taking into account the state of the art, the costs of

implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects. Medidata may update or modify the stated security controls from time to time provided that such updates and modifications meet or exceed the level of security as of the effective date of this Exhibit.

4.2 **Security Certifications**. During the term of the Agreement, Medidata will maintain Federal Information Systems Management Act (FISMA), Service Organization Controls 2 (SOC 2) and ISO/IEC 27001:2013 certifications.

4.3 **External Security Audit**. During the term of the Agreement, Medidata will maintain its SOC 2 Type 2 Attestation Standard of the AICPA Codification Standards (AT Section 101). Medidata publishes a SOC 2 report that is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) professional standards. This dual-standard report can meet a broad range of auditing requirements for U.S. and international auditing bodies. The SOC 2 report audit attests that Medidata data center control objectives are appropriately designed to ensure the data protection safeguards set forth in this Exhibit and that the individual controls defined to safeguard customer data are operating effectively. Medidata will update its SOC 2 audit report, at least every twelve (12) months.

5 SUBPROCESSORS

5.1 **Appointment of Subprocessors**. Customer acknowledges and agrees that (a) Medidata's Affiliates may be used as Subprocessors; and (b) Medidata and Medidata's Affiliates may use Subprocessors in connection with the provision of the Services.

5.2 **List of Current Subprocessors; Notification of New Subprocessors**. A list of current Subprocessors as may be used for Processing Personal Data, including a description of their processing services and countries of location, is available to Customer without charge and is maintained on Medidata's Knowledge Hub (https://learn.medidata.com) (the "**Subprocessor List**"). Customer hereby consents to Medidata's use of these Subprocessors and provides its general authorization for Medidata's use of new Subprocessors, subject to all requirements of this Section 5. To receive Subprocessor notifications, Customer is providing the following contact information for purposes of this Section 5: _____. Customer may also provide or update such contact information at any time by contacting Medidata at dataprivacy@mdsol.com. Where Customer has not provided such contact information to Medidata, Customer thereby provides its approval for new Subprocessors under this Section 5.

5.3 **Right to Object to New Subprocessors**. Medidata will not use any new Subprocessor until at least thirty (30) days after providing notice to Customer as set forth in Section 5.2 above. If Customer does not approve Medidata's use of a new Subprocessor on any grounds that relate to degradation in the protection of Personal Data, Customer may object by notifying Medidata in writing, specifying the grounds, within thirty (30) days of receipt of Medidata's notice to Customer. Where Customer objects to a new Subprocessor in accordance with the previous sentence, Medidata will make reasonable efforts to change its Services, or recommend a commercially reasonable change to Customer's configuration or use of the Services, to avoid Processing of Personal Data by the new Subprocessor. If the foregoing changes are not possible in a reasonable period of time (not to exceed thirty (30) days), Customer may terminate the applicable Sales Order(s) with respect to the Services requiring use of the new Subprocessor. No further fees will be owed under such terminated Sales Order(s) and Medidata will refund any prepaid fees covering the remainder of the term of such Sales Order(s) following the effective date of termination with respect to such terminated Services. This termination right is Customer's sole and exclusive remedy for the foregoing terminated Sales Order(s).

5.4 **Processing Restrictions; Liability.** Medidata will ensure that its Affiliates or any Subprocessors only Process Personal Data in accordance with the terms of the Agreement (including this Exhibit) and that they are bound by written obligations that require them to, at all times relevant to the Processing of Personal Data, have in place data protection measures designed to be no less protective than those in the Agreement with respect to the protection of Personal Data as applicable to the nature of the services provided by such Subprocessor. Medidata shall be liable for the acts and omissions of its or its Affiliate's Subprocessors to the same extent Medidata would be liable if performing the Services of the Affiliate or Subprocessor directly under the terms of this Exhibit.

6 RIGHTS OF DATA SUBJECTS AND COOPERATION WITH REGULATORS

6.1 **Correction, Deletion and Blocking**. To the extent Customer, in its use of the Services, does not have the ability to correct, amend, block or delete Personal Data as required by Privacy Laws, Medidata shall provide Customer with assistance to comply with any reasonable request by Customer to facilitate such actions to the extent Medidata is legally permitted to do so. Customer shall be responsible for any actual costs on a time and materials basis arising from Medidata's provision of such assistance, where such assistance is not included in the scope of the Services.

6.2 **Data Subject Requests**. Medidata shall, to the extent legally permitted, promptly notify Customer if it receives a Data Subject Request. Medidata shall not respond to any such Data Subject Request without Customer's prior written consent. Medidata shall provide Customer with assistance in relation to handling of a Data Subject Request, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use of the Services. Customer shall be responsible for any actual costs on a time and materials basis arising from Medidata's provision of such assistance, where such assistance is not included in the scope of the Services.

6.3 Medidata shall promptly notify Customer of all enquiries from a Regulator that Medidata receives which relate to the Processing of Personal Data or the provision to or receipt of the Services by Customer, unless prohibited from doing so by law or by the Regulator.

6.4 Unless a Regulator requests in writing to engage directly with Medidata, or the parties (acting reasonably and taking into account the subject matter of the request) agree that Medidata shall handle a Regulator request itself, Customer shall: (a) be responsible for all communications or correspondence with the Regulator in relation to the Processing of Personal Data with respect to the provision or receipt of the Services; and (b) keep Medidata informed of such communications or correspondence to the extent permitted by law.

7 ASSISTANCE AND INFORMATION FOR DATA PROTECTION IMPACT ASSESSMENT, NOTIFICATIONS

7.1 The information made available as Privacy Assistance Materials is intended to assist Customer in complying both with its obligations under Privacy Laws (including the GDPR), such as data protection impact assessment(s), data transfer impact assessment(s), prior consultation with the Regulator and other Regulator inquiries, and with any requests by Customer with respect to Medidata's privacy practices, including any audit request ("**Privacy Inquiries**"). Customer agrees to use Medidata's Privacy Assistance Materials in the first instance to fulfill Customer's Privacy Inquiries. In the event that Customer requires information in addition to the Privacy Assistance Materials, such information shall be made available under a separately executed audit support agreement. Such agreement may, in Medidata's sole reasonable discretion, require Customer to compensate Medidata for its actual costs on a time and materials basis, where such support requires more than sixteen (16) FTE (full-time employee) hours.

7.2 If Medidata becomes aware of a Personal Data Breach, Medidata will notify Customer of such Personal Data Breach without undue delay. Medidata will take appropriate actions to contain, investigate and mitigate the Personal Data Breach and work with Customer to provide information to Customer concerning the Personal Data Breach, and will assist Customer with any required notifications to affected individuals, subject to any related limitations set forth in the Agreement. Customer agrees that notification of or response to a Personal Data Breach will not be construed as an acknowledgement by Medidata of any fault or liability with respect to the Personal Data Breach.

7.3 To the extent that the Personal Data Breach is the result of Medidata's failure to comply with the terms of the Agreement, and in addition to the agreed liability terms in the Agreement, Medidata shall bear the actual, reasonable costs of notifying affected individuals and providing one year of credit monitoring (or up to the amount of time legally required under Privacy laws, if longer) to individuals in jurisdictions where monitoring is available. Medidata and Customer shall mutually agree on the content and timing of any such notifications, in good faith and as needed to meet applicable legal requirements. Notwithstanding the preceding sentence, the parties agree that Medidata shall have no obligation to send notification letters or provide credit monitoring for Customer unless such letters are legally required or otherwise reasonably required to alert individuals of potential harm.

8 DELETION OR RETURN OF PERSONAL DATA

8.1 Medidata shall return Personal Data to Customer or delete Personal Data in accordance with the terms of the Agreement and the policies and schedules set forth in Medidata's Record Retention Policy and Schedule, which Policy and Schedule adhere to limitations required by law and regulation, including Good Clinical Practices (ICH GCP), except as required by law or as required in order to defend any actual or possible legal claim.

8.2 Customer acknowledges and agrees that Medidata shall have no liability for any losses incurred by Customer arising from or in connection with Medidata's inability to perform the Services as a result of Medidata complying with a request to delete or return Personal Data made by Customer under this Section 8.

9 MAKING AVAILABLE INFORMATION TO DEMONSTRATE COMPLIANCE

9.1 **Distribution of Privacy Assistance Materials**. Medidata makes available to Customer the Privacy Assistance Materials (along with such additional information that Customer may have requested, as described in Section 7.1) to demonstrate compliance with this Exhibit and Privacy Laws.

10 EXPORT OF DATA AND APPLICATION OF THE STANDARD CONTRACTUAL CLAUSES

10.1 The parties hereby execute the Standard Contractual Clauses, which are hereby incorporated into this Exhibit. The Standard Contractual Clauses will not apply to Personal Data that is transferred (either directly or indirectly) from the European Economic Area (EEA) to outside the EEA, or the United Kingdom (UK) to outside the UK, or Switzerland to outside Switzerland, as applicable, where: (a) the recipient or country has been recognized by the European Commission, or UK Secretary of State, or Swiss Federal Data Protection and Information Commissioner (FDPIC), respectively, as providing an adequate level of protection for Personal Data as described in applicable Privacy Laws; (b) Medidata adopts an alternative recognized compliance standard for the lawful transfer of Personal Data outside the EEA, or UK, or Switzerland, respectively; or (c) such transfer is covered by a suitable framework or derogation recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including but not limited to Binding Corporate Rules for Processors or consent by the Data Subject.

10.2 Customer agrees that Sections 4.2, 4.3, 7.1 and 9.1 will be deemed to fully satisfy the audit rights granted under Clauses 9 (c) and 13 (b) of the Standard Contractual Clauses. The security certification and audit obligations in the preceding sentence are entered at the request of Customer.

10.3 For the purposes of Clause 9 of the Standard Contractual Clauses, Customer consents to Medidata appointing Subprocessors in accordance with the Agreement and Section 5 of this Exhibit.

10.4 For the purposes of Clause 16 (d) of the Standard Contractual Clauses, Medidata shall return and delete Data Exporter's data in accordance with the relevant provisions of the Agreement and Section 8 of this Exhibit.

10.5 For the purposes of Clause 14 of the Standard Contractual Clauses and the parties' obligation to conduct a Transfer Impact Assessment, Medidata provides the supporting documentation attached as **Attachment D** (Transfer Impact Assessment) in addition to the Privacy Assistance Materials made available under this Exhibit. Customer confirms to have reviewed the documentation provided with **Attachment D** (Transfer Impact Assessment) and that such documentation is sufficient for Customer to conduct the Transfer Impact Assessment. Customer shall conduct its Transfer Impact Assessment and provide a copy to Medidata upon request. In the event that Customer requires further information or Medidata's cooperation for such Transfer Impact Assessment (as the Customer may request under Clause 14 (c) of the Standard Contractual Clauses), such information and cooperation shall be made available in accordance with the relevant provisions of the Agreement and Section 7.1 of this Exhibit. Medidata may update **Attachment D** (Transfer Impact Assessment) and the Privacy Assistance Materials from time to time to provide Customer new or updated information for Customer's Transfer Impact Assessment.

10.6 By entering into this DPE, the parties agree that they are also entering into the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses under S119A(1) of the Data Protection Act 2018, as set out at https://www.medidata.com/wp-content/uploads/2022/09/Medidata_UK-Addendum-for-International-Transfer_2022.pdf, which shall only apply where required by Privacy Laws.

10.7 For the purposes of Clause 18 (c) of the Standard Contractual Clauses, Swiss courts are an alternative place of jurisdiction for Data Subjects habitually resident in Switzerland.

10.8 For data transfers subject to the Swiss Federal Act on Data Protection (FADP), the Standard Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under the Swiss Federal Act on Data Protection (FADP) until such laws are amended to no longer apply to a legal entity.

11 MISCELLANEOUS

11.1 **Governing Law**. To the extent required by applicable Privacy Laws (e.g., in relation to the governing law of the Standard Contractual Clauses), this Exhibit shall be governed by the law of the applicable jurisdiction. In all other cases, this Exhibit shall be governed by the laws of the jurisdiction specified in the Agreement.

11.2 **Nondisclosure**. The terms of this Exhibit (including its Attachments) are not publicly known and constitute Medidata's Confidential Information under the Agreement. Customer may only disclose the terms of this Exhibit to a Regulator or any other entity to the extent required by Privacy Law or regulatory authority. Customer shall take all reasonable steps to ensure that Regulators do not make the terms of this Exhibit public, including by marking any copies as "Confidential and Commercially Sensitive," requesting return of any copies, and requesting prior notice and consultation before any public disclosure.

11.3 **Conflict**. In the event of and to the extent of any conflict between the terms of the Agreement and this Exhibit, the terms of this Exhibit will prevail, except and to the extent the terms of Agreement are more protective of Personal Data, in which case the more protective terms of the Agreement will prevail. In the event of and to the extent of any conflict between the terms of this Exhibit and the SCCs, the terms of the SCCs shall prevail to the extent required by Privacy Laws. Except as expressly amended herein, the terms of the Agreement remain in full force and effect.

11.4 **Additional Products**. Customer acknowledges that if it installs, uses, or enables Additional Products that interoperate with the Services but are not part of the Services themselves, then by such actions Customer is instructing Medidata to cause the Services to allow such Additional Products to access Personal Data as required for the interoperation of those Additional Products with the Services. Such separate Additional Products are not required to use the Services and may be restricted for use as determined by Customer's system administrator. This Exhibit does not apply to the Processing of Personal Data by Additional Products which are not part of the Services.

11.5 **Limitation of Liability**. Except with respect to the notifications and credit monitoring set forth in Section 7.3 above, the parties agree that all liabilities between them under this Exhibit and the Standard Contractual Clauses will be subject to the limitations and exclusions of liability and other terms of the Agreement.

11.6 **Exclusion of Third Party Rights**. Data Subjects are granted third party rights under the Standard Contractual Clauses. All third party rights not required under Privacy Laws are excluded.

11.7 **Termination**. This Exhibit and the Standard Contractual Clauses will terminate when Medidata ceases to Process Personal Data. For the purpose of Customer's right to terminate the Agreement under Clause 14 (f) of the Standard Contractual Clauses, such termination shall not constitute termination for breach of the Agreement.

Attachment A
to the Data Processing Exhibit to Medidata Services Agreement

Details of Data Processing
(at the same time Annex I to the Standard Contractual Clauses)

A. LIST OF PARTIES

Data exporter(s):

Name: [Customer, as defined in the Agreement]

Address: [Customer address as defined in the Agreement]

Contact person's name, position and contact details: [If available, as defined in the Agreement]

Activities relevant to the data transferred under these Clauses: Data is transferred to allow data importer to provide the Services under the Agreement.

Signature and date: [As set out in the main body of Exhibit, or Agreement]

Role (controller/processor): Controller

Data importer(s):

Name: Medidata Solutions, Inc.

Address: 350 Hudson Street, 9th Floor, New York, NY 10014, USA

Contact person's name, position and contact details: dataprivacy@mdsol.com; Tel.: 212-918-1800; Fax: 1-212-918-1818

Activities relevant to the data transferred under these Clauses: The Personal Data is contained in the Data which Customer and its Authorized Users make available to Medidata as part of Medidata's Services under the Agreement. Medidata has access to such Data for Processing, including administration, solely pursuant to the Agreement and relevant Sales Order(s).

Signature and date: [As set out in the main body of Exhibit, or Agreement]

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER AND DETAILS OF DATA PROCESSING

Categories of data subjects whose personal data is transferred	Clinical trial participants.
Categories of personal data transferred	Key coded clinical trial data.
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 (i.e. pseudonymized) clinical trial data.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	On continuous basis for as long as Customer makes use of the Services under the Agreement.
Nature of the processing	Data importer Processes Personal Data to provide the Services as specified under the Agreement. The nature of the Processing is mainly to electronically collect, Process and store clinical trial data.
Purpose(s) of the data transfer and further processing	Medidata Processes only pseudonymized health data, including vital health measurements, demographics, medical history, treatments and details associated with clinical trial participants. Personal Data is contained in the data which data exporter and its Authorized Users enter into Medidata Applications as part of Medidata's Services under the Agreement. Medidata has access to such Data solely for purposes pursuant to the Agreement and relevant Sales Order(s).
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	25 years after end of clinical trial, in accordance with regulatory requirements that apply to the Services, such as Good Clinical Practice (GCP).
For transfers to (sub-) processors, also specify location, subject matter, nature and duration of the processing	The data importer mainly uses Amazon Web Services, Snowflake and Cognizant as hosting and service management subprocessors. Further subprocessors are set out in the Subprocessor List as described in the main body of this Exhibit. The subprocessors' services may be used as long as Medidata's Services are provided with their help. The location of the subprocessing includes the United States and locations as set out in the Subprocessor List.

C. COMPETENT SUPERVISORY AUTHORITY

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

1. Supervisory authority with responsibility for ensuring compliance by the data exporter, as provided in Clause 13 of the Standard Contractual Clauses set forth in Attachment C hereto.

2. For data transfers subject to the Swiss Federal Act on Data Protection (FADP), the Swiss Federal Data Protection and Information Commissioner (FDPIC) shall act as competent supervisory authority.

Attachment B
to the Data Processing Exhibit to Medidata Services Agreement

Details of Technical and Organisational Measures
(at the same time Annex II to the Standard Contractual Clauses)

This Attachment B forms part of the Agreement. Where specific systems and processes are identified herein, Medidata reserves the right to modify such systems and processes without notice as necessary to improve the security requirements of the Services. Any such modifications will not degrade the security of Customer's data. As of the effective date of this Exhibit, Medidata abides by the Security Measures set out in this Attachment. All references to "data" or "systems" in this Schedule refer to the Personal Data that Medidata Processes in the course of providing the Services to Customer as set forth in the Agreement.

1 **Access control to premises** (to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used).

Medidata maintains a hybrid data center architecture consisting of traditional data centers as well as cloud-based data centers operated by Amazon Web Services (AWS). All data centers are physically secure data centers with controls that include uniformed guards, multiple mantraps with smartcards, biometric access and monitored 24x7 CCTV. Systems are housed in non-descript buildings that provide no indication that Medidata computers are within.

The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) systems, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 3 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Medidata employs a monthly analysis process to increase the security of the data center servers used to provide the services and products in production environments.

Medidata maintains formal access procedures for allowing physical access to the Medidata managed data centers. The data centers are housed in facilities that require electronic card key access, as well as a biometric handprint access. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

Medidata has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Medidata's infrastructure security personnel are responsible for the ongoing monitoring of Medidata's security infrastructure, the review of the Services, and for responding to security incidents. Medidata has implemented and maintains an incident response program designed to optimize the prompt identification, containment, and remediation of threats to the confidentiality, integrity and availability of systems and data.

2 **Access control to systems** (to prevent data processing systems from being used without authorization).

Medidata systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks, or other necessary devices help provide this redundancy. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Medidata servers use a virtualized approach with VMWare on top of a Linux base. Windows server operating systems are then installed on top of the virtual machines. In AWS this same approach is taken with Unix and Windows servers running atop virtual machines provided by AWS.

Medidata has designed and regularly tests a disaster recovery program to help to protect against accidental destruction or loss. The disaster recovery program backs up data at least every 15 minutes locally and daily to disk and replicated off-site. Encryption is maintained at rest and in transit (using FIPS 140-2 compliant cryptographic methods).

Medidata employs multiple layers of network devices, Security Information and Event Management (SIEM) and Intrusion Detection and Prevention to protect our external attack surface. Medidata considers potential attack vectors and incorporates appropriate purpose-built technologies and procedures into external facing systems.

Medidata's systems are protected by a stateful firewall solution. Traffic inbound and outbound through the firewall is denied by default. The firewall threat prevention database is updated automatically in accordance with vendor best practices. Firewalls are configured to provide OSI model layer 3 (Network) through layer 7 (Application) security.

Medidata Intrusion Detection and Prevention (IDP) offers protection from both external and internal attackers-severing the traffic when necessary. These threat prevention systems use signature analysis mechanisms to analyze traffic for both hostile attacks originating from outside the organization as well as for system misuse or attacks originating from within the organization. Application and network traffic signature pattern matching is used to identify potential security threats. Traffic anomaly detection is employed to analyze network traffic for known attacks and variations of those attacks. Threat prevention signatures are automatically updated in accordance with vendor best practices.

SIEM is intended to provide insight into ongoing attack activities by generating insights through the review of (including the use of statistical techniques and/or artificial intelligence on) log files correlated from sources such as servers, intrusion detection devices, routers and load balancers. The SIEM can provide adequate information to respond to incidents. Medidata SIEM analysis involves:

- Tightly controlling the complexity of Medidata's attack surface through preventative measures;
- Employing intelligent detection controls at data ingress and egress points; and
- Employing automatic and manual procedures remedy certain dangerous situations.

Medidata monitors a variety of intelligence feeds for security threats, and Medidata's security personnel will react promptly to known incidents. Medidata also makes HTTPS encryption a required standard for all customers.

Medidata conducts security assessments to identify vulnerabilities, and to determine the effectiveness of Medidata's patch management program. In addition, authorized third parties on Medidata's behalf conduct penetration tests to assess current threats and vulnerabilities. Each security concern is reviewed to determine if it is applicable, ranked based on risk, and assigned to the appropriate team for remediation. Medidata does not permit its customers or any third parties on their behalf to conduct vulnerability or penetration testing.

Customer's administrators and end users must authenticate themselves via a central authentication system with two-factor authentication or via a federated (SAML) sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.

Medidata will take appropriate steps to ensure compliance with the Security Measures by its staff to the extent applicable to their scope of performance. All personnel are subject to a background check prior to hire, a security briefing upon hire, and annual refresher training opportunities in accordance with POL-InfoSec-001 Information Security Policy. Medidata personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

3 **Access control to data** (to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage).

Medidata's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process customer data. Medidata aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. Medidata employs a two-factor authentication system designed to provide Medidata with secure and flexible access mechanisms. Medidata requires the use of unique user IDs, strong passwords; two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Medidata's internal data access policies and training. Workflow tools that maintain audit records of all changes manage approvals. Access to systems is logged to create an audit trail for accountability. Password policies follow industry standard practices. These standards include password expiry, restrictions on password reuse and appropriate password strength.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Medidata's confidentiality and privacy policies. Personnel are provided with security training.

4 **Transmission control** (to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged).

All transmissions encrypt the data in flight using the FIPS 140-2 compliant primary protocol. This is designed to prevent data from being read, copied, altered or removed by unauthorized parties. Medidata employs a code analysis process to increase the security of the application code used to provide the services and enhance the security of products in production environments. During the code development developers can check and the code against the OWASP Top 10 and ISO 27000 requirements and make necessary corrections.

Prior to being placed into production, finished code is subjected to a comprehensive dynamic vulnerability scan in a sandbox environment by the Information Security department. Deficiencies are prioritized and noted in the SDLC ticketing system for remediation.

5 **Input control** (to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed).

Prior to onboarding Subprocessors, Medidata conducts due diligence efforts such as audits and vendor qualifications of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Medidata has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 5 of the Exhibit (the Data Processing Exhibit to Medidata Services Agreement), the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

6 **Job control** (to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal).

Medidata personnel only access raw unreadable data to perform routine maintenance tasks. The data in this raw state is encrypted at rest to FIPS 140-2 compliant cryptographic methods to ensure data integrity and confidentiality are maintained.. Out of an abundance of caution all data is backed up prior to any maintenance activities. All other processing actions are a result of premeditated and direct instruction from the principle.

7 **Availability control** (to ensure that personal data are protected from accidental destruction or loss).

Medidata stores data in a multi-tenant environment on Medidata-owned servers in our traditional data centers, and on Medidata owned virtual servers in our AWS centers. All data is backed up on a regular basis. Full backups are performed at least weekly, with incremental backups performed daily. Critical clinical study data is backed up at least every 15 minutes. The backed-up data is transferred to disk in an encrypted format (at-rest encryption to FIPS 140-2 compliant cryptographic methods) and stored at an off-site location. Rave clinical data is also fully duplicated electronically each day to our disaster recovery backup facility.

When a hard drive in our conventional data center reaches the end of its useful life, Medidata procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. Medidata

uses the industry standard techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. Until a device can be decommissioned using these procedures, the device is physically stored in a locked secure environment in the server room.

8 Data separation (to ensure that data collected for different purposes can be processed separately).

Medidata segregates all processing using virtual servers for each customer. Medidata establishes an identification and authentication system to assure only the principle can create, delete, modify or access data. Valid users are further assigned privileges based on roles assigned by the principle. Those privileges allow or disallow access under the direction of the principle at all times.

Attachment C
to the Data Processing Exhibit to Medidata Services Agreement

Standard Contractual Clauses (controller to processors – module two)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Attachment A, section A (hereinafter each "**data exporter**"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Attachment A, section A. (hereinafter each "**data importer**")

have agreed to these standard contractual clauses (hereinafter: "**Clauses**").

(c) These Clauses apply with respect to the transfer of personal data as specified in Attachment A, section B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Attachment A, section B.

Clause 7

Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Attachment A, section A.

(b) Once it has completed the Appendix and signed Attachment A section A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Attachment A, section A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Attachment A, section B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Attachment B and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Attachment A, section B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Attachment B. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can

be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Attachment B and C.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) 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 subprocessors at least the number of days in advance as set out in Sections 5.1(a) and 5.1(b) of the main body of this Exhibit, 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.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Attachment B the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: 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 Attachment A, section C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Attachment A section C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Attachment A, section C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer

agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Attachment D
to the Data Processing Exhibit to Medidata Services Agreement

Transfer Impact Assessment for Medidata Services

The purpose of a Transfer Impact Assessment is to determine whether the data subjects whose personal data is transferred outside of the EEA to a country not deemed adequate are afforded data protection rights that are *essentially equivalent* to that protection guaranteed within the EU, taking into account the safeguards in place and the enforceable rights and effective legal remedies available to the relevant data subjects. Below is Medidata's Transfer Impact Assessment, provided for the purpose of Clause 14 of the Standard Contractual Clauses and the parties' obligation to conduct a Transfer Impact Assessment, and to which Medidata's Customer can refer for conducting its own transfer assessment. This assessment outlines relevant details of Medidata's Services and corresponding processing of personal data, potentially applicable national security laws in the United States and the safeguards that Medidata has implemented.

Medidata makes available additional materials on its Trust & Transparency Center (www.medidata.com/trust), including its third-party certifications and attestations for data protection, and its Transfer Impact Whitepaper with further analysis of relevant laws. Medidata may update this Assessment from time to time, based upon changes to the law and Medidata's Services. Please refer to the Transfer Impact Whitepaper for the most recent version of this Assessment.

A. Specifics about the transfer of personal data in connection with a processing activity	
1.	**Description of the export (plus details of any onward transfers)** For clinical trial participants, the data exporter transfers only pseudonymized data, including vital health measurements, demographics, medical history, and treatments. Data exporter also transfers details associated with Authorized Users (e.g. physicians, other health care providers, study site personnel and similar data subjects) which relate solely to their professional duties related to the data exporter's use of Medidata's Services, not details referring to data subjects' private lives or sensitive details. Personal data is contained in the data which data exporter and its Authorized Users enter into Medidata Applications as part of Medidata's Services under the Agreement. Medidata has access to such Data solely for purposes pursuant to the Agreement and relevant Sales Order(s).
2.	**What (if any) Article 46 safeguard is being relied upon in relation to the export (onward transfer)?** Customer enters into Standard Contractual Clauses with Medidata in order to export personal data outside the EEA, as attached as Attachment C above.
3.	**Current safeguards** ● Medidata can only access key coded data about clinical trial participants, where the Customer (or the trial site) exclusively holds the re-identification key. ● Medidata uses end-to-end Transport Layer Security ("TLS") encryption during data transmission (as well as AES-256 encryption for data at rest). Therefore, any information transferred to the U.S. as part of Medidata's services cannot be intercepted in a human-readable form as it enters the United States, nor can this data be searched using "selectors" leveraged under surveillance collection programs. ● Medidata confirms that it has not received, or ever implemented, any request to undermine its secure Processing of personal data to grant law enforcement bodies or public authorities any form of "back door" access to personal data. ● Medidata confirms that it has not received any requests from law enforcement bodies or public authorities to access personal data which Medidata holds (for itself or on behalf of others) in recent years.
B. Applicable local law	
1.	● Foreign Intelligence Surveillance Act (FISA) Section 702 applies to communications of non-U.S. persons located outside of the United States. Medidata's activities would not fall under FISA Section 702 since ● Medidata is not an 'electronic communication service provider' or 'remote computing service' subject to compelled disclosure under FISA Section 702; ● Imported data is not communications nor directed to a specific recipient who would be the identified target of collection; and ● Medidata's use of end-to-end encryption protects clinical trial records from being incidentally collected in a human-readable or machine-searchable format. ● Executive Order (EO) 12333, as limited by Presidential Policy Directive (PPD)-28 can be applied to all transmission of data into the US by authorizing surveillance of Internet 'backbone' infrastructure. Provided that data is encrypted in

	transit, surveillance under EO 12333 can be avoided. It is unlikely that Medidata's activities would fall under EO 12333 since ● Imported data is not communications nor directed to a specific recipient who would be the identified target of collection; and ● Medidata's use of end-to-end encryption protects clinical trial records from being incidentally collected in a human-readable or machine-searchable format. ● Stored Communications Act (SCA) applies to electronic communications and records stored within the United States where a court has found reasonable grounds for surveillance of a specific person. It is unlikely that Medidata's activities would be subject to court-ordered disclosure under the SCA since ● Medidata is not an 'electronic communication service provider' or 'remote computing service' subject to compelled disclosure; ● Imported data is not communications nor directed to a specific recipient who would be the identified target of collection. ● The CLOUD Act amends the SCA to require compliance with a court order or warrant by US respondents who have stored responsive data outside of the United States. Medidata's activities would not fall under the CLOUD Act because Medidata hosts information within the United States and is not likely subject to the SCA for the reasons outlined above. ● USA PATRIOT Act, Section 215 applies to records of telephone calls where one party is within the United States. Medidata's activities would not fall under Section 215 since Medidata does not process telephone records. **(together, also referred to as the "Impacting Laws")**
2.	● **Are the Impacting Laws publicly accessible so that it is possible to anticipate the circumstances in which law enforcement and government bodies can surveil individuals?** Yes, although provisions or case law dealing with limits on what can be accessed are sparse with respect to FISA as the FISA court operates primarily in secret. ● **Can the Impacting Laws be used to access personal data / undertake surveillance / otherwise undermine protections for limited necessary and proportionate purposes only?** Not entirely. While surveillance is limited with respect to targeted individuals through the use of either individualized court orders or pre-chosen "selectors" for collection, once triggered the Impacting Laws appear to permit fairly broad access to personal data. ● **Can the Impacting Laws only be relied upon by law enforcement bodies / public authorities following some form of judicial or governmental oversight / review process?** Yes, to an extent. In order for surveillance operations to be conducted under FISA Section 702, the Attorney General ("AG") and the Director of National Intelligence ("DNI") must first jointly submit a written certification to the Foreign Intelligence Surveillance Court ("FISC"). The FISC will then review and consider the certification and decide whether to issue a written order authorizing the surveillance. However, the Schrems II judgment found that the authorisation process was at a programme level rather than at an individual level and therefore did not provide the necessary level of oversight. Collections under the SCA, as well as those under the provisions of FISA other than Section 702, are subject to judicial review on an individualized basis with a finding that the identified target meets the appropriate legal grounds. ● **Do data subjects have rights of redress / effective legal remedies under the Impacting Laws or other laws (e.g. national privacy laws) in the event that their personal data is accessed in contravention of the Impacting Laws and the protections within them or within other national laws?** Not entirely. While the law enforcement agencies and public authorities of the United States are subject to judicial review where individuals can assert and defend their civil rights, there is generally no opportunity for targets of surveillance to know whether their communications or information have been acquired by the government under Section 702 or EO 12333. As a result, fewer opportunities may exist to seek judicial review of that acquisition. In any event, the Schrems II judgment also found that EU individuals did not have actionable rights against US authorities for overreach of these provisions. This is a result of the jurisdiction and standing requirements placed upon U.S. Federal Courts.
C. Impact of rules on relevant export	
1.	**Is the personal data being exported likely to be of interest to the public authorities in the third country?**

	No. The data which will be stored by Medidata largely consists of key coded clinical trial data and their Processing by Authorized Users, e.g. structured records of vital health measurements, demographics, medical history, treatments for clinical trials. Medidata does not process any communications that are exported from the EEA to the United States in the context of its Services to its Customers as their data processor. It is highly unlikely that any legal process approving U.S. government data collection would ever apply to the information involved in Medidata's Services.
2.	**Is the data importer(s) likely to be a target of the public authorities in the third country for data requests?** No. Medidata is highly unlikely to fall within the description of an "electronic communications service provider" or "remote computing service", and by extension it is highly unlikely to be compelled to provide Customer's data to US intelligence agencies under FISA Section 702. Medidata's subcontractors or telecoms service providers that might be subject to Section 702 FISA do not have access to the data in the clear at all. In addition, the US Department of Commerce paper Information on US Privacy Safeguards Relevant to SCCs https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF at page 2 makes it clear that the US intelligence agencies should not be interested in or collecting the structured records and pseudonymized information involved in Medidata's Services.
3.	**Confirm the data importer(s) has NOT received requests in the past from public authorities in the relevant third country for personal data? If it has, provide details.** Confirmed.

D. Assessment conclusion

The following factors support concluding that Medidata's access to personal data is in line with the European Essential Guarantees:

- Practices of the third country of destination demonstrate that clinical trial data is not in focus by public authorities. As confirmed above, Medidata has never received requests in the past from public authorities in the relevant third country for personal data. This documents Medidata's practical experience.

- The data which will be shared is (a) key-coded (pseudonymized) patient data and (b) non-sensitive business contact information of health care professionals and other Authorized Users. The risk of harm to these individuals caused by non-compliant export of this data is likely to be very low given its non-sensitive nature (for (b)) or that US authorities have no means to identify data subjects (for (a)).

- Medidata is unlikely to fall within the description of an "electronic communications service provider" or "remote computing services", and by extension it is unlikely to be compelled to provide Customer's data to US intelligence agencies under FISA Section 702 or related laws, like the Stored Communications Act. Clinical Trial Data is out of scope as U.S. surveillance authorities apply to communications between specific parties, or to communications concerning topics associated with foreign intelligence information. The data involved in Medidata's services is in form of structured records for clinical trials and is not communications at all. As such, it is highly unlikely that any legal process approving U.S. government data collection would ever apply to the information involved in Medidata's Services.

- Medidata's use of end-to-end encryption for data in transit (as well as encryption for data at rest) mitigates against incidental collection of data in a human-readable or machine-searchable format.