# 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 underlying agreement, by which Medidata Solutions, Inc. or its Affiliate, as applicable ("**Medidata**") provides the Services to Customer (the "**Agreement**") 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. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to Customer pursuant to the Agreement, Medidata only Processes Personal Data on behalf of Customer pursuant to the Instructions. The parties agree to comply with the following provisions with respect to any Personal Data submitted by or for Customer to the Services or collected and Processed by or for Customer using the Services. Nothing in this Exhibit shall alter the parties' agreement, as set forth in the Agreement, with respect to representations, warranties, liability, indemnification, or any other commercial terms with respect to data protection or data security; in the event of any such conflict between this Exhibit and the Agreement, the Agreement shall prevail.

## 1 DEFINITIONS

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

1.2 **"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.

1.3 **"Customer Data"** has the same meaning as in the Agreement (whether referred to as Customer Data or Partner Data).

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

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

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

1.7 **"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.

1.8 **"GDPR 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) and/or prior consultations with Regulators. GDPR Assistance Materials will include, at a minimum, Medidata's current security certifications and reports, such as its SOC 1 and SOC 2 audit reports (or comparable industry-standard successor reports), ISO/IEC 27001:2013 Certification and Privacy Shield Certification.

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 the Services.

1.11 "**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") as of its effective date.

1.12 **"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.

1.13 "**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.

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

1.15 **"Standard Contractual Clauses"** means the Standard Contractual Clauses for Data Processors established in third countries pursuant to Commission decision (2010/87/EU) of the Data Protection Directive, as set out in Attachment B to 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.

1.16 **"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.

## 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 (Security Program).

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 Appendix 1 to Attachment B (the Standard Contractual Clauses).

## 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 regard to the Processing of Personal Data 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 Site Users**. Medidata, Customer and other Medidata customers are each independent controllers with regard to the registration data provided by investigators and other site-based Authorized Users to Medidata's hosted portal application, including without limitation, name, email, address, and training records ("Investigator 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 **Instructions**. Other than as set forth in Section 3.2 above, Medidata shall only Process Personal Data on behalf of and in accordance with the Instructions and shall protect Personal Data as Confidential Information. Customer shall ensure that its Instructions to Medidata shall comply with Privacy Laws. 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 5(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.

3.4 **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 Attachment A (Security Program) and ensures that access to Personal Data is limited to those personnel who require such access to perform the Agreement.

3.5 **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. Without prejudice to the foregoing, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data, and the means by which Customer acquired Personal Data and shall establish the legal basis for Processing under Privacy Laws, including by providing all notices and obtaining all consents as may be required under Privacy Laws in order for Medidata to Process Personal Data on behalf of the Customer in order to provide the Services pursuant to the Instructions.

## 4 SECURITY OF PERSONAL DATA

4.1 **Security Controls**. Medidata will take and implement the appropriate administrative, organizational and technical controls as set out in Attachment A (Security Program). Medidata may update or modify the stated security controls from time to time provided that such updates and modifications meet or exceed the stated security controls. Customer agrees that Medidata has no obligation to protect Customer Data that Customer elects to store outside of Medidata and its backup systems. Customer has assessed the level of security appropriate to the Processing in the context of its obligations under Privacy Laws and agrees that the security measures set out in Attachment A (Security Program) are consistent with such assessment.

4.2 **Security Certifications**. During the term of the Agreement, Medidata will maintain its Privacy Shield, 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 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 and Customer Consent**. Customer acknowledges and specifically authorizes Medidata's use of its Subprocessors existing as of the Effective Date, including Amazon Web Services, C3i, Cognizant and Medidata Affiliates. Customer hereby gives a general authorization to further Subprocessors, provided Medidata follows the following procedure:

(a) Medidata agrees to provide notice to Customer of any new or replacement Subprocessor that Processes Personal Data under the Agreement thereby giving the Customer the opportunity to object to such changes within ten (10) days from the date of receipt of notice (**Subprocessor Notice**). Customer agrees that it will not object to any Subprocessor (a) with which Medidata has executed a written agreement that obligates it to (i) protect such Personal Data to the same extent as is required of Medidata by the Agreement and (ii) be in compliance with applicable Privacy Laws and (b) which is subject to industry-standard external security auditing (collectively, the **Conditions**).

(b) If Customer has reasonable grounds to object to Medidata's use of a new or replacement Subprocessor, Customer shall notify Medidata promptly in writing within ten (10) days after receipt of the Subprocessor Notice and specify those grounds. Such reasonable grounds (provided that such reason does not conflict with the Conditions above) may be that the new or replacement Subprocessor is unlikely to be able to comply with the terms of the Agreement so far as they relate to the protection of Personal Data, or other reasons that are at least as important. Customer acknowledges that Medidata provides a standardized service to all customers which does not allow using different Subprocessors for different customers and, therefore, that the inability to use a particular new or replacement Subprocessor for the Services to the Customer may result in delay in performing the Services, inability to perform the Services or increased fees. Medidata will notify Customer in writing of any change to Services or fees that would result from Medidata's inability to use a new or replacement Subprocessor to which Customer has objected. Customer may either execute a written amendment to the Agreement implementing such change or exercise its right to terminate the Agreement in accordance with the termination provisions thereof. Such termination shall not constitute termination for breach of the Agreement. This termination right shall be Customer's sole and exclusive remedy for such termination of the Agreement.

5.2 **Processing Restrictions**. Medidata will ensure that Subprocessors only access and use Personal Data in accordance with the terms of the Agreement (including this Exhibit) and that they are bound by written obligations: (i) that require them to

provide at least the level of data protection required by Privacy Laws and by the Agreement; and (ii) where applicable, that impose the level of data protection required by the Standard Contractual Clauses.

5.3 **Liability**. 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 each Subprocessor directly under the terms of this Exhibit.

5.4 **List of Current Subprocessors and Notification of New Subprocessors**. A current list of Subprocessors as may be used for Processing Data is available to Customer without charge. The parties agree that any copies of the Subprocessor agreements that Medidata must make available to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Processing of Customer's Personal Data, removed by Medidata beforehand; and, that such copies will be provided by Medidata only upon request by Customer. Medidata will keep the Subprocessor list current and inclusive of any new Subprocessors and will make available to Customer the updated Subprocessor list upon request by Customer. Medidata shall notify Customer prior to using any Subprocessor not included in such list, in accordance with clause 5.1 above.

## 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, reasonable costs 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 except to confirm that the request relates to Customer, unless the Data Subject request relates only to that Data Subject's registration data for accessing the Services. 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. If legally permitted, Customer shall be responsible for any actual, reasonable costs arising from Medidata's provision of such assistance, where such assistance is not included in the scope of the Services.

6.3 The parties acknowledge and agree that, other than for Data Subject Requests that relate only to that person's registration data for accessing the Services, Medidata and/or Customer are generally not legally permitted to provide access to, correction, amendment or deletion of a Data Subject's Personal Data pursuant to but not limited to Good Clinical Practices (ICH GCP).

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

6.5 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 and 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 GDPR Assistance Materials is intended to assist Customer in complying both with its obligations under the GDPR, such as data protection 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 that Medidata's GDPR Assistance Materials will be used to fulfill Customer's Privacy Inquiries. Except as otherwise agreed to in the Agreement, in the event that Customer requires information in addition to the GDPR Assistance Materials, including to demonstrate compliance with this Exhibit, such information shall be made available under a separately-executed audit support agreement. Customer shall be responsible for the actual, reasonable costs on a time and materials basis for Medidata's provision of such assistance at Medidata's then-current Professional Services rates.

7.2 If Medidata becomes aware of a security incident which leads or is likely to lead to a material infringement of Privacy Laws, or of this Exhibit, that compromises the security, confidentiality or integrity of Customer's Personal Data and that would

require reporting to a regulatory authority (as defined under applicable Privacy Laws) (a "**Security Incident**"), Medidata will notify Customer of such Security Incident without undue delay. Medidata will take appropriate actions to contain, investigate and mitigate the Security Incident and work with Customer to provide information to Customer concerning the Security Incident, and will assist Customer with any required notifications to affected individuals, subject to any related limitations set forth in the Agreement. Notification of or response to a Security Incident under this Section will not be construed as an acknowledgement by Medidata of any fault or liability with respect to the Security Incident.

7.3 Except as otherwise agreed to in the Agreement, to the extent that the Security Incident is the result of Medidata's failure to comply with the terms of the Agreement, Medidata shall bear the actual, reasonable costs of notifying affected individuals and providing one year of credit monitoring 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.

8.3 Customer agrees that during and after the term of the Agreement, and solely to the extent provided in the Agreement, Medidata may use information it collects and uses in connection with the Services, together with information from its other clients, for data analytics purposes, including to create insights, reports and other analytics to improve the quality of and market Medidata's advice, products and services, or to make Improvements.

## 9 MAKING AVAILABLE INFORMATION TO DEMONSTRATE COMPLIANCE

9.1 **Distribution of GDPR Assistance Materials**. Medidata will make available upon Customer request its GDPR Assistance Materials (along with such additional information as the parties may agree to as part of an audit support agreement, described in Section 7.1) to demonstrate compliance with this Exhibit and Privacy Laws.

## 10 APPLICATION OF THE STANDARD CONTRACTUAL CLAUSES

10.1 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 where: (a) the recipient or country has been recognized by the European Commission 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 such as EU-US and Swiss-US Privacy Shield; 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 5(f) and 12(2) 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 11 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 purposes of Clause 12 (1) 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 Where the Standard Contractual Clauses apply, in the event of any conflict or inconsistency between this Exhibit and the Standard Contractual Clauses in Attachment B, the Standard Contractual Clauses shall prevail.

## 11 MISCELLANEOUS

11.1 **Governing Law**. To the extent required by applicable Data Protection 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 Attachment A) are not publicly known and constitute Confidential Information under the Agreement. Customer may only disclose the terms of this Exhibit to a data protection Regulator to the extent required by law or regulatory authority. Customer shall take reasonable steps to ensure that data protection 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 **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.

11.4 **Limitation of Liability**. 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, except that such limitations and exclusions of liability will not apply to any party's liability to Data Subjects, such as under the third party beneficiary provisions of the Standard Contractual Clauses, to the extent limitation of such rights are prohibited by Privacy Laws.

11.5 **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.

11.6 **Termination**. This Exhibit and the Standard Contractual Clauses will terminate when Medidata ceases to Process Personal Data, except as otherwise agreed in writing between the parties.

**Attachment A**

**to the Data Processing Exhibit to Medidata Services Agreement**

**Security Program**

This Schedule forms part of the Agreement. Where specific systems and processes are identified herein, Medidata reserves the right to modify such systems and processes as necessary to improve the security requirements of the Services. Notwithstanding the forgoing, Medidata improvements will not be less onerous security measures and shall notify Customer in advance of such change during the term of the Agreement.

As of the Effective Date, Medidata abides by the Security Measures set out in this Appendix. During the term of the Agreement, the Security Measures may change without notice but Medidata agrees that any such change shall not materially reduce or weaken the protection provided for Personal Data that Medidata Processes in the course of providing the Services to Customer.

**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) flywheel energy 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. A redacted quarterly summary of the findings is available upon request.

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.

**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 Windows servers running atop virtual machines provided by AWS.

Medidata backs up data to help to protect against accidental destruction or loss. Data is backed up every 15 minutes locally and daily to tapes. Medidata designed and regularly tests its disaster recovery program.

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

Medidata provides a comprehensive firewall solution. The inbound firewall is configured in a default deny-all mode except for ports 80 (HTTP) and/or port 443 (HTTPS). The outbound firewall is in a default deny-all mode. The firewalls are updated with the most current definitions available on scheduled basis consistent with our change management procedures. Firewalls are configured to provide OSI model layer 2 (Data Link) through layer 7 (Application) security.

Medidata's Intrusion Detection System (IDS) offers protection from both external and internal attackers—where traffic doesn't go past the firewall at all. Our systems use signature analysis mechanisms to analyze all traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization. Application and network traffic signature pattern matching is used to identify potential security weaknesses. Protocol anomaly traffic detection analyzes network traffic for known attacks and variations of those attacks. Updated network traffic signature files are automatically implemented upon release by the vendor.

SIEM is intended to provide insight into ongoing attack activities by correlating log files through artificial intelligence from 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.

Customer's administrators and end users must authenticate themselves via a central authentication system 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-ISP-007 Information Security & Privacy Policy.

**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 sufficient password strength.

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. Medidata conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

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 approved AES 256 algorithm over TLS as the 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 products in production environments. During the code development developers can check and the code against the OWASP top 10, HIPAA, and ISO 27000 requirements and make necessary corrections.

Prior to going live the finished code is subjected to a comprehensive dynamic vulnerability scan in a sandbox environment by the Information Security & Privacy 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 provides all control of personal data processing to the principle. Medidata personnel only access raw unreadable data to perform routine maintenance tasks. The data in this raw state are meaningless ones and zeros. 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 every 15 minutes. The backed-up data is transferred to tape in an encrypted format 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 B**

**to the Data Processing Exhibit to Medidata Services Agreement**

**Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

**Name of the data exporting organisation**: [Customer as defined in the Agreement]

Address: [Customer address as defined in the Agreement]

Tel.: [If available, as defined in the Agreement]; Fax: [If available, as defined in the Agreement]

Email: [If available, as defined in the Agreement]

Other information needed to identify the organization:

[If available, as defined in the Agreement] (the data **exporter**)

And

Name of the data importing organisation: **Medidata Solutions, Inc.**

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

Telephone: 212-918-1800 Fax: 1-212-918-1818

E-mail: dataprivacy@mdsol.com

Other information needed to identify the organisation:

A corporation organized under the laws of the State of Delaware (the **data importer**),

EACH A "PARTY", TOGETHER "THE PARTIES", HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

*Clause 1*

***Definitions***

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the sub-processor'* means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2*

***Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

*Clause 3*

***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4*

***Obligations of the data exporter***

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

*Clause 5*

***Obligations of the data importer***

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

*Clause 6*

***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

*Clause 7*

***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a)to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

*Clause 8*

***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

*Clause 9*

***Governing Law***

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

*Clause 10*

***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

*Clause 11*

***Sub-processing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

*Clause 12*

***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**On behalf of the data exporter (Customer):**

Name (written out in full): [As provided for execution of the Agreement]

Position: [As provided for execution of the Agreement]

Address: [As provided for execution of the Agreement]

Other information necessary in order for the contract to be binding (if any):

Signature: [Executed by incorporation into the Agreement]
(stamp of organisation)

**On behalf of the data importer (Medidata Solutions, Inc.):**

Name (written out in full): [As provided for execution of the Agreement]

Position: [As provided for execution of the Agreement]

Address: [As provided for execution of the Agreement]

Other information necessary in order for the contract to be binding (if any):

Signature: [Executed by incorporation into the Agreement]
(stamp of organisation)

## APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

**Data exporter**

The data exporter is (please specify briefly your activities relevant to the transfer):

The data exporter is a company making use of the Services, and to this end accessing and using the Medidata Applications and Documentation for clinical trial study(ies) set forth in the Sales Order(s) (f/k/a Statement of Work). Such use granted shall be applicable only for the clinical trial study set forth on the Sales Order(s).

The parties agree that Medidata shall collect, process and use Personal Data as described in the Agreement, as amended in the Exhibit (the Data Processing Exhibit to Medidata Services Agreement).

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

The data importer is Medidata Solutions, Inc., a computer technology corporation, headquartered in New York, United States of America, that specializes in developing and marketing cloud computing-based solutions to address functions throughout the clinical development process. To this end, the data importer provides Services for collecting, processing and using data provided by health care providers and which is used by Data Exporter.

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

Physicians; other health care providers, study nurses, Authorized Users, clinical trial subjects.

**Categories of data**

The personal data transferred concern the following categories of data (please specify):

name, address, Email, phone, position, role/responsibility, specialty, clinical trial data

**Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

Pseudonymized health data, including vital health measurements, demographics, medical history, treatments.

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

The Personal Data is contained in the Data which Customer and its Authorized Users enter into Medidata Applications as part of Medidata's Services under the Agreement. Medidata has access to such Data for administration and data aggregation purposes pursuant to the Agreement and relevant Sales Order(s).

**DATA EXPORTER**

Printed Name: [As provided for execution of the Agreement]

Authorised Signature: [Executed by incorporation into the Agreement]

**DATA IMPORTER (Medidata Solutions, Inc.)**

Printed Name: [As provided for execution of the Agreement]

Authorised Signature: [Executed by incorporation into the Agreement]

## APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

*See Attachment A (Security Program) to this Exhibit*.

**DATA EXPORTER**

Printed Name: [As provided for execution of the Agreement]

Authorised Signature: [Executed by incorporation into the Agreement]

**DATA IMPORTER (Medidata Solutions, Inc.)**

Printed Name: [As provided for execution of the Agreement]

Authorised Signature: [Executed by incorporation into the Agreement]