ANNEX 1 STANDARD CONTRACTUAL CLAUSES

Data Transfer Agreement (Controller to Processor)

For the Transfer of Personal Data to Processors in Third Countries

This Data Transfer Agreement ("**DTA")** based on the unmodified standard contractual clauses for the transfer of personal data to processors established in third countries as per Commission Decision 2010/87/EU as of February 5, 2010, including Appendices 1 ("Details of the Transfer"), and 2 ("Technical and Organizational Measures") (collectively: "**Model Clauses**") is entered into

by and between:

The User as "data exporter", receiving the services rendered by the data importer,

and

Siemens Healthcare Diagnostics Inc., 511 Benedict Avenue, Tarrytown, NY 10591, USA located outside EU/EEA as "data importer".

This DTA consists of two parts:

Part 1 contains general provisions and provisions implementing mandatory requirements regarding commissioned data processing as defined under the GDPR.

Part 2 contains the unmodified Model Clauses, which apply, subject to the amendments provided for in Part 1, to the processing operations (the "service(s)") described in Appendix 1 of the Model Clauses.

WHEREAS, applicable data protection laws require data exporters in EEA countries and Switzerland to provide adequate protection for transfers of personal data to non-EEA countries and such protection can be adduced by requiring data importers to enter into the Model Clauses;

WHEREAS, The User and data importer have entered into the agreement Terms of Service and Conditions of Use for the Atellica® COVID-19 Severity Algorithm (the "main agreement") covering the provision of services entailing the processing of personal data on behalf of the User by the data importer as a processor;

Definitions

Terms used in Part 1 in this DTA shall have the meaning as defined in Part 2, Clause 1 (a) – (f).

Part 1

§ 1 GDPR Requirements

1. **Compliance with data privacy laws.** In order to comply with the GDPR regarding the commissioning of the data importer as a data processor, the parties agree on the following supplementations regarding Part 2. For the avoidance of doubt, the parties agree that the terms of this Part 1 are not intended to amend or modify the terms of Part 2. The data exporter and the data importer are aware

of the importance of protecting the right to privacy and shall comply with all applicable existing privacy laws and regulations in particular the GDPR with regard to the processing of personal data by the data importer on behalf of the data exporter.

2. **Confidentiality.** Notwithstanding the other provisions of this DTA the data importer ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3. **Assistance.**
   (a) Taking into account the nature of the processing as described in the main agreement and this DTA, the data importer shall assist the data exporter by appropriate technical and organizational measures, for the fulfilment of data exporter’s obligation to respond to requests for exercising the data subject's rights laid down in Articles 12 to 23 GDPR.
   (b) Taking into account the nature of the processing, data importer shall assist the data exporter in ensuring the data exporter’s own compliance with the obligations pursuant to Articles 32 (security of processing), 33 (notification of personal data breach to the supervisory authority), 34 (communication of a personal data breach to the data subject), 35 (data protection impact assessment) and 36 (prior consultation) GDPR.

4. **Information for demonstrating compliance with Article 28 GDPR.** With regard to the processing under the main agreement, the data importer shall upon request of the data exporter make available to the data exporter all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR.

§ 2 Other

1. In the event of inconsistencies between Part 1 and Part 2 the provisions of Part 2 shall prevail. Provisions of Part 1 shall however remain valid to the extent that they do not contradict but merely amend the provisions of Part 2.

2. Should any provision or condition of this DTA be held or declared invalid, unlawful or unenforceable by a competent authority or court, then the remainder of this DTA shall remain valid. Such an invalidity, unlawfulness or unenforceability shall have no effect on the other provisions and conditions of this DTA. The provision or condition affected shall be either (i) amended to an extent that ensures its validity, lawfulness and enforceability, while preserving the parties’ intentions, or (ii) construed in a manner as if the invalid, unlawful or unenforceable part had never been contained therein.

Part 2

Standard Contractual Clauses for 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

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 organizational security measures” means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 organizational 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, unauthorized 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 subprocessing 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 subprocessing, 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:

1. 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,
2. any accidental or unauthorized access, and
3. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 subprocessing, 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 subprocessing, 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

Subprocessing

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 fulfil 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 subprocessing 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 subprocessing 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.

APPENDIX 1

Details of the Transfer

This Appendix forms part of the Model Clauses and needs to 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: User as defined in the Terms of Service and Conditions of Use

Data importer

The data importer is: Siemens Healthcare Diagnostics Inc., 511 Benedict Avenue, Tarrytown, NY 10591

Data subjects

The personal data to be transferred may concern any one or more of the following categories of data subjects:

- Test Subjects

Categories of data

The personal data transferred concern the following possible categories of data:

- Special categories of data

- Other: Age

Special categories of data

The personal data transferred concern the following special categories of data:

- Health (i.e., diagnostics data from specific blood tests of patient samples)

Processing operations

The personal data transferred will be subject to the following basic processing activities:

See: main agreement

APPENDIX 2

Technical and Organizational Measures

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

Description of the technical and organizational security measures implemented by the data importer

in accordance with Clauses 4(d) and 5(c):

1. Pseudonymization and Encryption of Personal Data

Data importer separates personal data from the processed data so that it is not possible to link the processed data to an identified or identifiable person without additional information that is stored separately and securely. Data importer encrypts personal data with symmetric and asymmetric keys.

2. Confidentiality, Integrity, Availability and Resilience of Systems and Services

a) Data importer ensures confidentiality and integrity by taking the following measures:

Access control:

Data importer protects its buildings with appropriate access control systems based on a security classification of the buildings and an appropriately defined access authorization concept. All buildings are secured by access control measures using a card reader system. Depending on the security category, property, buildings or individual areas are secured by additional measures. These include special access profiles, biometrics, pin pads, DES dongles, separation locks, video surveillance and security personnel. Access rights for authorized persons are granted individually according to defined criteria. This also applies to external persons.

System access control:

Access to data processing systems is only granted to authenticated users based on a role-based authorization concept using the following measures: Data encryption, individualized password assignment (at least 8 characters, regularly automatic expiration), employee ID cards with PKI encryption, password-protected screen savers in case of inactivity, intrusion detection systems and intrusion-prevention systems, regularly updated antivirus and spyware filters in the network and on the individual PCs and mobile devices.

Data access control:

Access to personal data is granted on the basis of a role-based authorization concept. A user management system has been set up, which maps the user database with their respective authorizations and is available centrally in the network for retrieval by requesting data processing systems. Furthermore, data encryption prevents unauthorized access to personal data.

Data transmission control:

Data importer secures electronic communication channels by setting up closed networks and data encryption procedures. If a physical data carrier transport takes place, verifiable transport processes are implemented that prevent unauthorized data access or logical loss. Data carriers are disposed of in accordance with data protection regulations.

b) Data importer ensures systems and services constant availability and reliability by taking the following measures:

Data importer ensures availability and resilience of systems and services by isolating critical IT and network components, by providing adequate backup and redundancy systems, using power redundancy systems, and regularly testing of systems and services. Test and live systems are kept completely separated.

3. Availability and Access to Personal Data in the Event of an Incident

Data importer shall restore the availability of and access to personal data in the event of a physical or technical incident by taking the following measures:

Data importer stores personal data in RAID systems and integrates redundant systems according to security marking. Data importer uses systems for uninterruptible power supplies (e. g. UPS, batteries, generators) to secure the power supply in the data centers.

Databases or data centers are mirrored in different physical locations.

A comprehensive written emergency plan is available. Emergency processes and systems are regularly reviewed.

4. Control Procedures to ensure the Safety of Processing

Data importer maintains a control procedure based on a risk-management-based approach, taking into account the basic IT protection catalogues of the Federal Office for Information Security (BSI) and ISO/IEC 27001 requirements for the regular review, assessment and evaluation of the effectiveness of technical and organizational measures to ensure security of processing. This ensures the protection of relevant information, applications (including quality and safety test methods), operating environments (e. g. by network monitoring against harmful effects) and the technical implementation of protection concepts (e. g. by means of vulnerability analyses). By systematically detecting and eliminating weak- points, the protective measures are continuously questioned and improved.

5. Personnel Measures

Data importer issues written work instructions and regularly trains personnel who have access to personal data to ensure that personal data is only processed in accordance with the law, this DTA and associated instructions of the data exporter, including the technical and organizational measures described herein.