DATA ADDENDUM
(including the European Standard Contractual Clauses)

This Data Addendum ("**DA**") is an addendum to and forms part of the TriNetX Membership Agreement between Medway NHS Foundation Trust, Inc. (the "**Agreement**") dated 25th January 2018 and reflects the Parties' agreement with regard to the Controlling and Processing of Personal Data in accordance with the requirements of the European Union General Data Protection Regulation ("GDPR"). This DA, along with the exhibits and appendices attached hereto, supersedes, amends, and shall be in lieu of any and all Data Protection Addendum and Amendments regarding data processing and controlling that was executed between the parties. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. This DA consists of two parts: the main body of the DA and Exhibit 1 (including Appendices 1 and 2).

PURPOSE OF THIS DA

The purpose of this DA is to provide for additional details in order to differentiate the parties' responsibilities regarding personal data in order to comply with the GDPR.

DATA TERMS

In the course of providing the TriNetX Product and any professional services to Member pursuant to the terms of the Agreement (collectively, the "**Services**"), TriNetX is considered a Joint Data Controller with the Member. TriNetX is a Joint Controller with Member of the Personal Data in which Member provides for the TriNetX Product. Member shall pseudonymize the data prior to providing it to TriNetX. The basis under GDPR in which the Member provides the Pseudonymized Data to TriNetX is in furtherance of the Member's legitimate interest of conducting research.

TriNetX is also a Processor of only the *Member's users' personal information* which contains their names and e-mail addresses. Obtaining the aforementioned data is a necessity to perform under the Agreement. Therefore, consent is not required from the Member's Users under GDPR.

The following are definitions to be incorporated hereto:

1. DEFINITIONS

"**GDPR**" is the **General Data Protection Regulation** (Regulation (EU) 2016/679) which is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. When the GDPR takes effect, it will replace the data protection directive (officially Directive 95/46/EC) of 1995. The regulation was adopted on 27 April 2016. It becomes enforceable from 25 May 2018.

"Affiliate" has the definition provided in the Agreement and if not so defined, a person or entity that directly or indirectly controls, is controlled by, or is under common control with, another person or entity.

"Data Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data; where the purposes and means of processing are determined by EU or Member State laws, the Controller (or the criteria for nominating the Controller) may be designated by those laws.

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller.

"Sub-processor" means any Data Processor engaged by TriNetX.

"Personal Data" means any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

"Sensitive Personal Data" means personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

"Process" means any operation or set of operations which is performed upon Personal Data, whether by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Pseudonymization" is the procedure by which the most identifying fields within a data set are replaced by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field. The resulting data set is known as Pseudonymous or Pseudonymized Data.

"Pseudonymous / Pseudonymized Data" means data that has been processed in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

"Standard Contractual Clauses" means the agreement executed by and between Member and TriNetX and attached hereto as Exhibit 1 pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors and the Standard Contractual Clauses for the transfer of data between Controller to Controller, in which both were established in third countries which do not ensure an adequate level of data protection.

"Legitimate Interest" is the processing of personal data , which is necessary for compliance with a legal obligation to which the controller is subject. Under Recital 47, Article 6 (1)(f) of the GDPR, legitimate interests include those of a controller to which the personal data may be disclosed, or the legal basis provided by a third party.

"Research" under GDPR Article 6(1)(f) suggests that Controllers may process personal data, without consent, when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject". The research exemptions apply to processing Personal Data for scientific and historical research, statistical research, and archiving in the public interest. Statistical research is any operation of collection and the processing of Personal Data necessary for statistical surveys or for the production of statistical results in aggregate form.

"Contract Performance" under GDPR, Article 6, is the processing of Personal Data shall be lawful only if said processing is necessary for the performance of the agreement.

2. PROCESSING OF PERSONAL DATA AND SENSITIVE PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to Personal Data, Member and TriNetX are Joint Data Controllers, and TriNetX -may engage -sub-processors pursuant to the requirements set forth in section 4 "Sub-processors" below. Member is solely responsible to pseudonymize their Personal Data prior to providing it to TriNetX. In addition, Member warrants that only Member maintains the key to the Pseudonymized Data and TriNetX shall not gain any access to said key; therefore, TriNetX is unable to re-identify any of the Personal Data provided by Member.

2.2 Member's Processing of Personal Data and Sensitive Personal Data. Member shall, in its use of the TriNetX Product, Process Personal Data and Sensitive Personal Data in accordance with the requirements of GDPR. Member maintains the sole responsibility for the accuracy, quality, and legality of Personal Data and Sensitive Personal Data and the means by which Member acquires it. Member shall only transfer said data to TriNetX in full compliance with GDPR and represents and warrants to TriNetX that all transfers are in compliance.

2.3 TriNetX's Processing of Personal Data. TriNetX shall only Process **Personal Data of the Member's Users of the TriNetX Products for the purpose of providing the Services under the Agreement and permitting Member's Users to access the TriNetX Products.** TriNetX shall not process Sensitive Personal Data for either the Member's Users of the TriNetX Products or any of the Member's patients/data subjects. TriNetX will only process Pseudonymized patient data/data subjects from the Member prior to the data being transferred and used within the TriNetX product.

2.4 Data Subjects Correction, Blocking, Deletion, & The Right To Be Forgotten. Because the Personal Data TriNetX obtains from Member is Pseudonymized and does **not** contain any keys and other information which enables TriNetX to re-identify the personalized data, Member is **solely** responsible for patient's request to delete, amend, opt out, or be forgotten with the use of their personal data.

PERSONNEL

3.1 Confidentiality. TriNetX 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 executed written confidentiality agreements which survive the termination of their personnel engagement.

3.2 Limitation of Access. TriNetX shall ensure that TriNetX's access to Personal Data is limited to those personnel who require such access to perform under the Agreement.

3.3 Data Protection Officer. TriNetX has appointed a data protection officer where such appointment is required by Data Protection Laws and Regulations. The appointed person may be reached at:

Kshitij Kathaura
TriNetX, Inc.
125 Cambridgepark Drive, Cambridge, Massachusetts, USA.
Phone number: 857.285.6051
Kshitij.Kathuria@trinetx.com

4.SUB-PROCESSORS

4.1 *Appointment of Sub-processors.* *Member acknowledges and agrees that (a) TriNetX's Affiliates* may be retained as Sub-processors; and (b) TriNetX and TriNetX's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Member consents to (a) the appointment of TriNetX Affiliates as Sub-processors of Personal Data under this Agreement, and (b) the appointment by TriNetX of other third-party Sub-processors provided that (i) TriNetX gives Member at least 30 days' notice of the proposed appointment, (ii) TriNetX promptly provides any information concerning the proposed appointment and processing that is reasonably requested by Member within 30 days' of the notice described in subclause (i), and (iii) Member has not objected in writing to the appointment of such third-party processor within 30 days of the *later of* the date of notice of the proposed appointment pursuant to subclause (i) or the date upon which Company has received complete responses to any request for further information made pursuant to subclause (ii).

In the event that TriNetX appoints a third-party Sub-processor pursuant to this Section, TriNetX confirms that it has entered or (as the case may be) will, prior to concluding such appointment, enter with the third-party Sub-processor into a written agreement incorporating terms which are substantially similar to those set out in this Section and in all events, in compliance with the Data Protection Laws. As between Member and TriNetX, TriNetX shall remain fully liable for all acts or omissions of any third-party Sub-processor appointed by it pursuant to Section 4.1.

4.2 Liability. TriNetX shall be liable for the acts and omissions of its Sub-processors to the same extent TriNetX would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as may otherwise be set forth in the Agreement.

5. SECURITY

Controls for the Protection of Personal Data. TriNetX is ISO/IEC 27001:2013 certified and shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Medway NHS Foundation Trust User's Personal Data, as set forth in the Agreement. TriNetX regularly monitors compliance with these safeguards. TriNetX will not materially decrease the overall security of the TriNetX Product during the term of the Agreement in order to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of the Personal Data to be protected

6. SECURITY BREACH MANAGEMENT AND NOTIFICATION

TriNetX maintains security incident management policies and procedures specified in the Agreement and shall, to the extent permitted by law, without undue delay notify Member of any actual or reasonably suspected unauthorized disclosure of Personal Data by TriNetX or its Sub-processors of which TriNetX becomes aware (a "**Security Breach**"). To the extent such Security Breach is caused by a violation of the requirements of this DA by TriNetX, TriNetX shall make reasonable efforts to identify and remediate the cause of such Security Breach as promptly as practicable.

7. LIABILITY

7.1 Limitation on Liability. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DA, except as otherwise provided within the DA, , whether in contract, tort or under any other theory of liability, is subject to the "Exclusions of Damages; Limitation of Liability" clause of the Agreement, and any reference in such clause to the liability of a party, besides stated in this section, means the aggregate liability of that party and of its Affiliates under the Agreement and all the DA together.

7.2 Data Liability Exclusion. TriNetX shall not be responsible for Member's patients' personal data including but not limited to Member's improper consent of their patient's use of their personal data on the TriNetX Network, failure to change, delete, or amend personal data per the request of the patient, or breaches of Member's patient data which was under the Member's auspices.

8. RETURN AND DELETION OF PERSONAL DATA OF MEMBER'S USERS

TriNetX shall make available Personal Data of only the Member's *users* of the TriNetX products to Member and will return, amend, and/or delete the personal data at the direction from the Member.

9. ADDITIONAL TERMS FOR EU PERSONAL DATA

9.1 Application of Standard Contractual Clauses. The unamended controller to processor EC Standard Contractual Clauses in Exhibit 1 (the "**Standard Contractual Clauses**") as signed by the parties will apply to the Processing of Personal Data by TriNetX in the course of providing the Services as follows:

9.1.1 The Standard Contractual Clauses apply only to Personal Data that is transferred from the European Economic Area (EEA) to outside the EEA, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive), and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data.

9.1.2 The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all Affiliates (as defined in the Agreement) of Member established within the European Economic Area (EEA) and Switzerland that have a right to access and use the TriNetX Product under the Agreement and that have signed the Standard Contractual Clauses. For the Standard Contractual Clauses and this Section 9, the entities shall be deemed "Data Exporters"

9.1.3 **Audits and Certifications.** The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications (without limitation to Data Exporter's rights under Applicable Law): Upon Data Exporter's request, and subject to the confidentiality obligations set forth in the Agreement, Data Importer shall make available to Data Exporter (or Data Exporter's independent, third-party auditor that is not a competitor of TriNetX) information regarding TriNetX's compliance with the obligations set forth in this DA in the form of the third- party certifications and audits set forth in the Agreement.

9.1.4 **Conflict.** In the event of any conflict or inconsistency between this DA and the Standard Contractual Clauses in Exhibit 1, the Standard Contractual Clauses shall prevail.

10. LEGAL EFFECT

This DA shall only become legally binding between Member and TriNetX after complete execution by all relevant parties of the DA.

Medway NHS Foundation Trust
Signature: ______________
Print Name: Lesley Dwyer ______________
Title: Chief Executive ______________
Date: 22/6/18

TriNetX, Inc.
DocuSigned by:
Signature: ______________
Print Name: Christopher Fraser
Title: SVP, Finance & Administration
Date: 2018-06-28

EXHIBIT 1

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 organization: **Medway NHS Foundation Trust**

Address: Windmill Road, Gillingham, Kent, ME7 5NY

Tel.: 01634 830000 x3129 ………; fax: ……………………….. ; e-mail: edyta.mccallum@nhs.net

Member State in which the data exporter is established: United Kingdom

Other information needed to identify the organisation:

….ICO registration number: Z5002033..
(the data **exporter**)

And

Name of the data importing organisation: TriNetX, Inc.

Address: 125 Cambridgepark Drive Suite 500, Cambridge, MA, 02140

Tel.: [857-285-6037] fax: [617-945-2091] e-mail: [chris.fraser@trinetx.com]

Other information needed to identify the organisation: Not applicable

DocuSigned by:

………………………………………………………………………
19AA1E2D82344E8...

(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 subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 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 subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 subprocessor 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, if the data importer has retained or has in its possession any personal data the data importer and the subprocessor 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 subprocessor 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: Medway NHS Foundation Trust

Name (written out in full): Lesley Dwyer

Position: Chief Executive

Address: Windmill Road, Gillingham, ME7 5NY

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

Signature...

(stamp of organisation)

On behalf of the data importer: TRINETX, INC.

Name (written out in full): Christopher Fraser

Position: VP Finance & Privacy Officer

Address: 125 Cambridgepark Drive, Suite 500, Cambridge, MA 02140 USA

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

DocuSigned by:

Signature .... 19AA1E2D82344E8...

(stamp of organisation)

Processing operations

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

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

DATA EXPORTER: Medway NHS Foundation Trust

Name: Lesley Dwyer, Chief Executive.............

Authorized Signature ....

DATA IMPORTER: TRINETX, INC.

Name: ... Christopher Fraser....................

Authorized Signature ....

DocuSigned by:

19AA1E2D82344E8...

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:

Data Exporter is (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) each Affiliate of Member established within the European Economic Area (EEA) and Switzerland that has purchased or is receiving Services under the Agreement.

Data importer

The data importer is:

TriNetX, Inc. is a provider of a software-as-a-service informatics platform which processes personal data upon the instruction of the Data Exporter in accordance with the terms of the Agreement.

Data subjects

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

Data Exporter may submit Personal Data to the Services, or cause Personal Data to be submitted to the Services, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, patients, website visitors, business partners and vendors of Data Exporter (who are natural persons)
- Employees or contact persons of Data Exporters' prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Data Exporter (who are natural persons)
- Data exporter's Authorized Users authorized by Data Exporter to use the Services

Categories of data

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

Data exporter may submit Personal Data to the Services, or cause Personal Data to be submitted to the Services, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Contact information (email, phone, personal address, business address)
- Company, title, position
- ID data

Special categories of data (if appropriate)

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

None

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated: ....

FOR DATA IMPORTER

DocuSigned by:

....

19AA1E2D82344E8...

Christopher Fraser

....

FOR DATA EXPORTER

....

Lesley Dwyer, Chief Executive ....

as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

i. the data protection laws of the country in which the data exporter is established, or

ii. the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

Name of the data exporting organization: **Medway NHS Foundation Trust**

Address: Windmill Road, Gillingham, Kent, ME7 5NY

Tel.: 01634 830000 x3129........ ; fax: .... ; e-mail: edyta.mccallum@nhs.net
Member State in which the data exporter is established: United Kingdom

Other information needed to identify the organisation:

..........ICO registration number: Z5002033.......
(the data **exporter**)

And

Name of the data importing organisation: TriNetX, Inc.

Address: 125 Cambridgepark Drive Suite 500, Cambridge, MA, 02140

Tel.: [857-285-6037] fax: [617-945-2091] e-mail: [chris.fraser@trinetx.com]

Other information needed to identify the organisation: Not applicable

hereinafter "data importer"

each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

b) "the data exporter" shall mean the controller who transfers the personal data;

c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

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

Data Importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data related to the Services, as described in the Membership/Healthcare Newtwork Agreement.

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and
ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

Data subjects
The personal data transferred concern the following categories of data subjects:

The first category of Data being transferred by the HCO to TriNetX is Electronic Healthcare Data (EHR) however the data is Pseudonymised. Pseudonymisation is the procedure by which the most identifying fields within a data set are replaced by one or more artificial identifiers, or pseudonyms. The final data received by TriNetX is not attributed to an identified or identifiable natural person.

A secondary category of data is Personal Data of the employees of the HCO to get access to TriNetX Live.

Purposes of the transfer(s)
The transfer is made for the following purposes:

The purpose of transferring is the processing of the aggregation of pseudonymised EHR data in a manner that facilitates the possibility of researching treatments, drug administration and clinical outcomes through the use of TriNetX Live.

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

Category 1 – Pseudonymised Electronic Healthcare Data
Category 2 – Personal Data of Users of TriNetX Live (name, username, email address, and encrypted login credentials)

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

Only to Employees of TriNetX.

Sensitive data (if appropriate)
The personal data transferred concern the following categories of sensitive data:

The Data being transferred by the HCO to TriNetX is Electronic Healthcare Data (EHR) however the data is Pseudonymised. Pseudonymisation is the procedure by which the most identifying fields within a data set are replaced by one or more artificial identifiers, or pseudonyms. The final data received by TriNetX is not attributed to an identified or identifiable natural person and therefore not considered Sensitive Personal Data.

Data protection registration information of data exporter (where applicable)

ICO registration number: Z5002033

Additional useful information (storage limits and other relevant information)
……
……
……
………

Contact points for data protection enquiries

Data importer
………………………………………………
………………………………………………
………………………………………………

Data exporter
Lee Lauren…………………………
lauren.lee@nhs.net……………………
………………………………………………