chaucer...

LIFE SCIENCES

White Paper on TriNetX GDPR Readiness

Written By: Stephanie Roberts and Paul Gillingwater

Version 1.0

Last Updated: May 18, 2018

Chaucer is recognised by the Financial Times as a leading digital consulting company. For over 30 years we've been helping the world's largest companies transform. We specialise in advising and delivering complex business and digital change and transformation in highly regulated industries, predominantly for global clients.

Our Data Privacy specialists each bring a minimum of 20 years' cross-industry experience in organisational leadership positions (CIO/CTO/CDO) in data privacy, Cyber Security, IT Risk, data protection. Coupled with their consulting expertise, they bring comprehensive understanding of the GDPR that is grounded in real life understanding of the problems faced when implementing major regulatory changes.

We combine our digital transformation expertise with deep industry knowledge in Energy, Life Sciences, Financial Services, Telecommunications & Media, and Government.

https://chaucer.com/

Table of Contents

1. Introduction

Data-driven approaches are being used increasingly for the discovery and development of new healthcare therapies. An increase in innovative health data-driven strategies requires consideration around the ethical and legislative responsibilities of managing such sensitive (special category) data.

On May 25th 2018, a new EU Data Protection law named the General Data Protection Regulation (GDPR) will come into force and will require organisations that process personal data, including that pertaining to subjects' health, to comply with the provisions set out in the law.

This white paper describes the impact of the new EU legislation on organisations that process health data and the challenges and opportunities it provides. It also covers detail around the preparations **TriNetX, Inc.** have undertaken to ensure strict compliance with GDPR regarding their cloud-based health research platform *TriNetX Live.*

The intended audience of this white paper are persons who are representatives of Healthcare Organisations (HCOs) who are already TriNetX members, those wishing to collaborate and become a member of the global health research network or Contract Research Organisations (CROs) and pharmaceutical companies wishing to license *TriNetX Live* to augment their clinical trial research strategies.

The primary scope of legislation under consideration within this paper includes the General Data Protection Regulation, which goes into effect across all 28 Member States of the European Union on May 25th, 2018. We also consider the U.K. Data Protection Act 2018, which implements a number of derogations and other modifications to GDPR which apply specifically to the U.K. Note also that TriNetX conforms to the provisions of the U.S. HIPAA legislation, which regulates health data privacy.

2. Background on TriNetX

TriNetX connects HCOs, CROs and pharmaceutical companies, as well as a variety of other data sources such as registries and other data sets within organisations. These are linked through a global research network to facilitate the sharing and utilisation of Electronic Health Record (EHR) data. Institutions that join the network are provided with access to a cloud-based software platform to enable real-time research to be conducted across aggregate health record data and associated clinical document-derived data.

The platform enables researchers to be able to conduct real-time research on patient populations to help identify eligible trial participants, new clinical trial sites or test protocol development and undertake robust evidence-based feasibility. HCOs that join the network either conduct research on their own patient populations or collaborate with peer organisations to enable the identification of clinical research opportunities across a wider network of sites. Pharmaceutical companies and CROs can license *TriNetX Live* to supplement [protocol design and feasibility studies] clinical trial recruitment strategies and identify HCOs that could provide future sites for clinical trials. Patient recruitment is often a costly bottleneck in clinical trial delivery, therefore TriNetX provides opportunities to accelerate the process or anticipate risks; thus, making the process of bringing new medicines to market more efficient.

TriNetX has designed its research platform to be intuitive for its end-users. The application is aimed at Healthcare Professionals who have a role to play in academic research, trial design, feasibility and recruitment. Users of the system can build queries across aggregate data sets that contain information such as demographics, diagnoses, procedures and labs etc., to enable the selection of patient cohorts for further analysis.

The platform is now established globally with numerous HCO, pharma and CRO clients utilizing the application.

3. Introduction to GDPR

3.1. Why is it needed?

Achieving the correct balance between the rights of individuals to privacy and the ability for organisations to use data for legitimate purposes is the ultimate ambition of data protection. The new legislation brings increased expectations of organisations processing personal data: lawful, fair and transparent when controlling the processing of personal data. However, the new legislation does not impede research; it reflects current good practice in research, through safeguards that apply to all research using personal data. If an organisation is already implementing good practice under current data protection legislation, they will need to make relatively few changes to policies and practices; but will need to ensure evidence of such. There are specific exemptions relating to research purposes included within both GDPR and its enabling legislation in selected countries.

Some recent high-profile cases in the media have drawn attention to instances where such data privacy principles have not been applied; resulting in serious data breaches affecting the rights and freedoms of the data subjects involved. The organisations in question have had their reputations put at risk and suffered serious financial fines. Stricter data protection regulations such as GDPR will ensure that organisations that experience such breaches in the future will encounter steeper financial penalties. More importantly, the regulation provides Europe-wide consistency of data protection principles, allowing multi-nationals to reduce their cost of compliance.

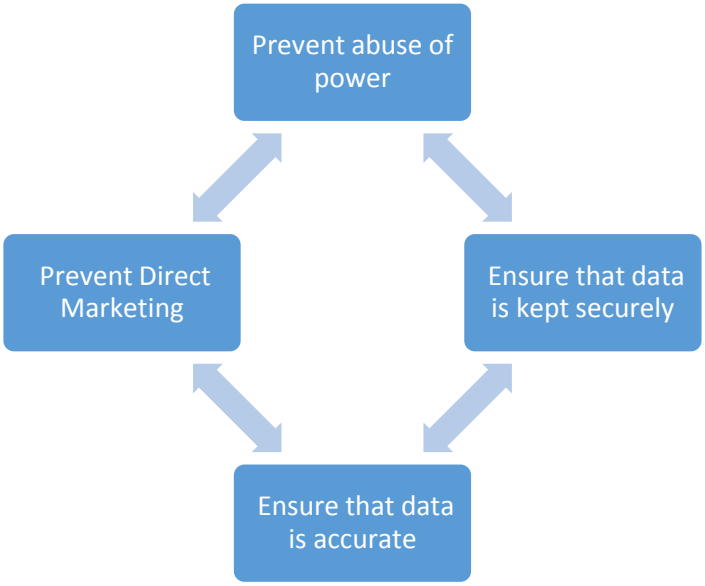

Figure 1: Ensuring that the human rights of data subjects are fully protected is enshrined in data protection law and is never more pertinent than now in the current big data era.

3.2. Introducing the Legalisation

European Data Protection and Privacy legalisation has been in existence for some time. The EU Data Protection Directive 1995 (Directive 95/46/EC) and UK Data Protection Act 1998 both sought to ensure human rights of subjects providing personal data were safeguarded and organisations holding, or processing data operated within clearly-defined ethical boundaries.

Due to some inconsistencies in the way that the existing EU regulation was applied and enforced, it became necessary to revise and update the existing legalisation and this new version of data protection law will apply from 25th May 2018, across the EU in the form of the General Data Protection Regulation (GDPR).

GDPR consists of 99 articles and 173 recitals and is built on the same fundamental principles of data protection that were familiar territory in the previous legalisation. Organisations are in scope for GDPR if they collect, control or process EU residents' personal data, irrespective of whether the organisation has a physical presence in the EU.

GDPR introduces more accountability for organisations controlling or processing data and a requirement for increased transparency of such processing activities. Subjects will not only have more visibility about what will be done with their personal data, but they will also have increased rights pertaining to their personal data. It is no longer adequate for organisations to just say they are compliant, instead they will need to show evidence of compliance through documentation strategies.

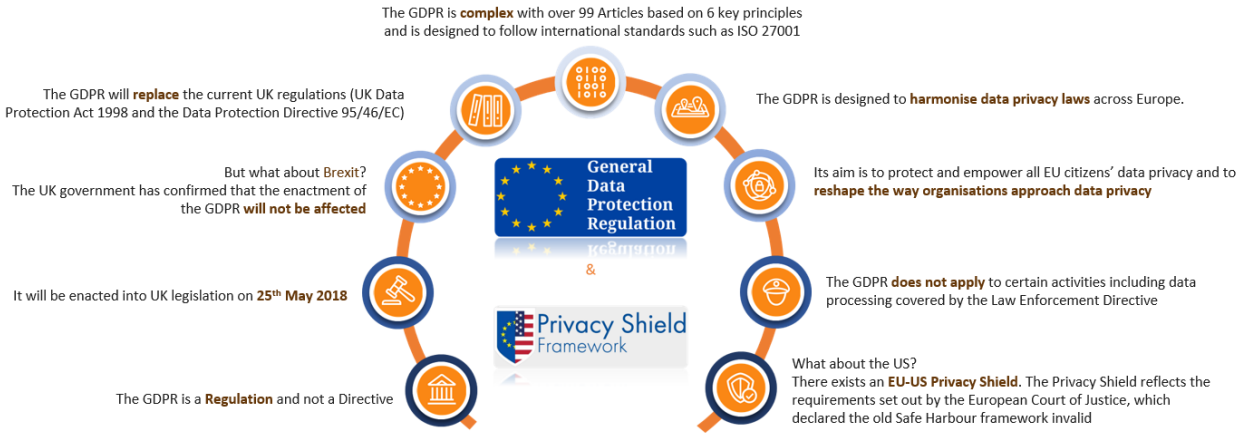

Figure 2: An overview of some of the key aspects of GDPR

3.3. GDPR: The basic principles

Personal data is a term that is used throughout the GDPR and applies to any information relating to an identifiable natural person ('data subject'). Examples of such information includes identifiers such as a name, an identification number, date of birth, post codes (including partials), place of birth, gender, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data. It includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

There are six main data protection principles that are outlined in Article 5 of the GDPR on which all processing activities regarding personal data should be based:

1. Processing must be lawful, fair and transparent to the data subject
2. Personal data must be collected for specified, explicit and legitimate purposes
3. Personal data must be adequate, relevant and limited to what is necessary ('data minimisation')
4. Personal data should be accurate and kept up to date
5. Personal data must be kept no longer than necessary
6. Personal data must be processed in a secure manner

3.4. Overview of main aspects

3.4.1. Controller and Processor Obligations

The GDPR separates out the responsibilities regarding data protection for 'data controllers' and 'data processors'. The data controller *'determines the purposes and means of processing personal data'*, and thus have the majority share of data protection responsibility. The processor *'is responsible for processing personal data on behalf of a controller'*. Thus, the processor is not relieved of responsibilities, but rather have their own legal obligations to fulfil, but must also work closely with the controller to ensure all duties are performed.

It is possible that there can be more than one controller involved in any data processing operation and these are referred to as 'Joint Controllers' in Article 26 of the GDPR. Where a processor or joint controller is used, and it's a separate entity to the primary controller, a special contract known as a Data Processing Agreement must be put in place, as outlined in GDPR Article 28.

3.4.2. Data Protection by Design and Default

Privacy by Design is a pivotal aspect of personal data protection. The GDPR is no different in this respect, and Articles 24, 25 and 28 outline some of the expected measures that should be implemented:

- Technical and organisational measures should be considered ahead of data processing and ensure they are implemented during data processing to meet the principles of GDPR such as data minimisation
- The controller needs to be able to demonstrate that processing is compliant
- The controller can use codes of conduct or approved certification mechanisms as a method to demonstrate compliance.

It is the controller's responsibility to ensure that the appropriate measures are employed, even in the situation where the controller is using a processor to perform the processing on their behalf.

3.4.3. Pseudonymisation

Pseudonymisation is a valuable tool to aid data protection by design and default in GDPR. It 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 Pseudonymised Data. It 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Pseudonymisation is referred to on multiple occasions throughout GDPR as an important procedure that can be used to safeguard personal data and is thus one of the primary security measures that organisations can implement along with other technology-focused measures such as data encryption.

It is worth pointing out that pseudonymisation is not the same as anonymisation, which completely removes all possibility of re-identification. When data is fully anonymised, it falls out of scope of GDPR, however this is not the case with pseudonymised personal data, which still needs to be treated under the regulation of GDPR. Unlike the U.S. Health Insurance Portability and Accountability Act (HIPAA), which sets forth a rule exempting data from regulation if 18 specific identifiers are removed, the GDPR applies a standard, considering data anonymous only when it cannot be identified by any means "reasonably likely to be used, either by the controller or by another person" (Recital 26). Thus, even if a researcher no longer has the ability to re-identify a data set, such data set may still be regulated under the GDPR if it could be re-identified with reasonable effort.

3.4.4. Contracts and Agreements

A written contract needs to be in place whenever a controller uses a processor or co-controller. The contract is vital to ensure that each party understands its responsibilities and liabilities. The GDPR specifies what should be included in the contract, as per Article 28.

Contracts must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.

Contracts must also include at a minimum a set of terms that outline the responsibilities of the processor to assist the controller in fulfilling the duties and measures necessary for GDPR, for example, using the appropriate technical and organisational measures to ensure the security of personal data.

3.4.5. Lawful basis for processing

One of the first decisions to be made ahead of any processing activity is to determine the lawful basis for processing. Identifying the most suitable lawful basis is mandatory for GDPR, along with a requirement to document it and inform data subjects upfront, typically through a privacy notice.

There are six lawful bases to select from and depending on which is chosen, data subjects' rights will differ as shown in this diagram (the x shows that the right does not apply):

	Right to erasure	Right to portability	Right to object
Consent			✖ but right to withdraw consent
Contract			✖
Legal obligation	✖	✖	✖
Vital interests		✖	✖
Public task	✖	✖	
Legitimate interests		✖	

Figure 3: Lawful bases and rights exceptions

3.4.6. Special category data

Special category data is personal data which the GDPR classifies as more sensitive. Data that falls into this classification includes health data, biometric data and genetic data, along with many others not applicable to health data processing. "Data concerning health" is defined by the GDPR as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."

The GDPR stipulates that special category data should not be processed at all unless it qualifies for one of the exemptions listed in Article 9. For example, processing is necessary to protect the vital interests of the data subject.

As with other types of personal data it is necessary to identify the lawful basis for processing, but in addition for special category data you must identify a processing condition too. There are ten conditions for processing special category data in the GDPR, with some additional conditions introduced by the U.K. Data Protection Act 2018.

As per Article 9(2), the ten conditions are as follows:

> (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
>
> (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3.4.7. Documentation

New documentation requirements are stipulated in the GDPR. Both Data Controllers and Data Processors must meet the obligations of maintaining up to date records on processing activities as laid out in Article 30. The type of information that needs to be documented includes the lawful basis and purpose of processing, information around data transfers, and the security measures that will be used to safeguard

personal data. The documentation records do not need to be filed with the ICO[1] but rather made available if requested.

In addition to Article 30, it will be expected that organisations also keep records of the following: consents, controller-processor contracts, records of personal data breaches and if applicable, Data Protection Impact Assessments and Legitimate Interest Assessments.

3.4.8. Rights of data subjects

GDPR provides increased rights to data subjects when it comes to decisions around processing of their personal data. The right to be informed ensures that organisations are transparent about their processing activities. The typical method for informing subjects is via a privacy notice. Once the subject is informed about how their data will be processed, they also have the right to restrict processing, the right to access their data, the right to rectify anything that is inaccurate and the right to have their data erased. Individuals also have the right to portability and the right to object to having decisions made on their data through automated methods alone. Some of these rights are not available, depending on the lawful basis used for processing, as per Figure 3 above.

3.4.9. Data Protection Officer and Data Protection Impact Assessments

When a new processing activity is planned, or a new data processing technology is introduced, GDPR encourages a risk assessment known as a Data Protection Impact Assessment (DPIA) to be performed in advance of the processing. This assists the controller of the processing operation to look in detail at each aspect of processing and identify any areas of risk so that the appropriate measures can be put in place.

The DPIA might be performed in consultation with the Data Protection Officer (DPO) if one is assigned. The DPO is required in instances where large scale processing of special category data is performed. The DPO should be an independent expert who has no conflict of interest with respect to processing.

TriNetX has appointed a full-time DPO, who is based at the headquarters in Cambridge, MA.

3.4.10. International Transfer of Personal Data

The transfer of personal data outside of the EU is authorised if the supervisory authorities are satisfied that the country has adequate data protection measures in place, or other appropriate transfer mechanisms are used. For international organisations that need to transfer personal data within their organisation across EU boundaries, it is possible to use binding corporate rules or model contractual clauses. Transfers to countries that do not have adequate measures of protection are more problematic.

[1] The Information Commissioner's Office is the data protection supervisory authority within the U.K.

3.4.11. Data Security

GDPR emphasises the importance of adequate security measures to protect personal data. Article 32 specifies that the controller and processor should use procedures to ensure the confidentiality, integrity, availability and resilience of personal data. Organisations need to plan for events such as a technical or security incident that might result in data loss, they must be able to give assurance that alternative options exist for accessing personal data should such an event arise.

4. GDPR Impact on Real-World Data Research

The Health Research Network platform hosted by TriNetX is a database containing a collection of Electronic Health Records (EHRs), a form of real-world data used increasingly by pharmaceutical organisations and CROs to aid clinical trial design and other research activities.

EHRs are longitudinal electronic records of patient health information generated by one or more encounters in a care delivery setting. A typical electronic health record will contain information on an individual patient including demographics, progress notes, medications, vital signs, medical history, immunisations, laboratory data and radiology reports.

The patient record is a tool that can be used by any clinician during a patient consultation or healthcare encounter. It is used to recall observations and exchange information with those involved in the patient's care to enable an accurate diagnosis, treatment plan or intervention. EHRs can also be used for observational studies across patient populations to benefit epidemiological research and public health.

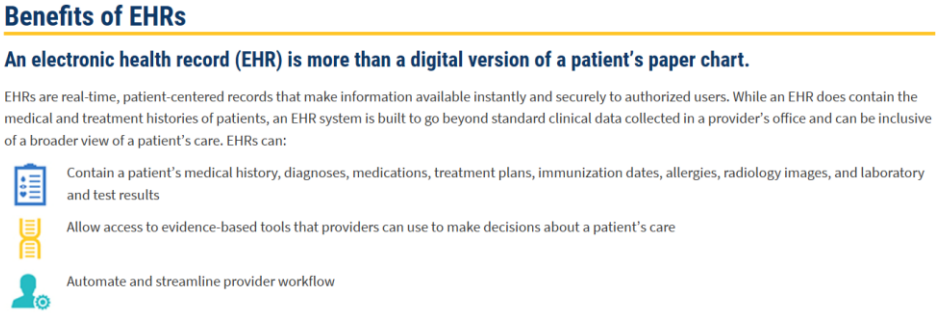

Figure 4: Benefits of EHRs

A diversity of EHR vendors are licensed by HCOs domestically and internationally.

4.1. Processing of EHR data

In terms of GDPR the HCO will assume responsibility as the controller and the vendor as a processor. It is the HCO's responsibility to ensure that the EHR vendor meets the requirements of GDPR. They are determining how the data will be processed and will need to take responsibility for ensuring that the appropriate security measures are in place to safeguard the data. They will additionally need to ensure that GDPR compliant contracts are in place between themselves and the EHR vendor. Both the HCO and EHR vendor must ensure that technical and organisational measures put in place to fulfil GDPR requirements, including adequate training for end users of the system and a comprehensive set of procedures and policies.

4.2. Consent

Electronic health records constitute special category data in GDPR, and therefore are prohibited from being processed unless exemptions exist such as an individual's explicit consent as is the case in Clinical Trials Research.

In contrast to a Clinical Trial where explicit patient consent is routinely obtained in advance of conducting the trial and prior to any data processing, a patient will not routinely participate in a consent process prior to electronic health record data collection. The ramifications of the lack of consent include the fact that the patient will not be informed about the processing as required by GDPR. In most cases in a primary care setting it is not practical to obtain consent at the time of data collection. Also, at the time the data is collected, it may not be completely understood what processing activities will be conducted using the data.

GDPR does provide some derogations to the consent process. One of these circumstances relates to medicine development and is referred to in Article 9 (i), this has relevance in the situation of Real World Data research as is the case here, i.e.

> *processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;*

4.3. Data Subject Rights

4.3.1. Right to be Informed

Increased transparency is one of the core aspects of the GDPR and this includes the obligation to inform data subjects that will have their personal data collected about all the details of the processing. Article 13 outlines the requirements in terms of the information that should be provided at the time of data collection. A privacy notice is one way that this information can be communicated with the patient ahead of data collection for their EHR. The HCO involved in their treatment should have a GDPR compliant privacy notice available for subjects to view to understand who is involved in processing, how long the data will be kept for, what the lawful basis for processing is and what the purposes of processing are.

4.3.2. Right to Access

Procedures have been in place for some time for patients to request access to their electronic health records and this also applies in GDPR. The patient will channel the request through the primary health organisation where their data resides. GDPR necessitates that subject access requests are responded to within one month.

4.3.3. Right to Erasure

Article 17 describes the 'right to erasure' as one of the rights data subjects are entitled to, however it does not automatically apply in every situation. The derogations that are listed in the GDPR include areas of public health and for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Maintaining an accurate and complete EHR for a patient is crucial for a high standard of care, as it ensures that clinicians are fully informed. Downstream secondary research such as epidemiological studies would also be inhibited if the right to erasure were to apply.

4.3.4. Right to Data Portability

A new right under GDPR concerns making available to the data subject a copy of their personal data in machine-readable form. This applies however only if the lawful basis used for processing is either consent or contract fulfilment.

4.3.5. Right to Object

Under certain conditions, individuals may object to the processing of their data. Individuals have the right to object to the following types of processing:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

4.3.6. Rights related to Automated Decision Making (including Profiling)

Where decisions are made with a significant legal or other ramification, data subjects may request to have their data processed manually or may challenge the results of a decision. You can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

4.4. Data Protection Officer (DPO)

Under Article 37, the controller and the processor should designate a Data Protection Officer (DPO) where the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9.

All HCOs as well as TriNetX should appoint a DPO to meet this requirement.

5. TriNetX GDPR Readiness

Key to TriNetX's success in delivering a valued clinical research application is its diligent approach to data security and personal data protection. TriNetX understands the critical importance of information protection to their customers and recognises the contribution information security can make to an organisation's strategic initiatives and overall risk management. TriNetX has therefore adopted security controls and practices that are designed to protect the confidentiality, integrity and availability of customer information that is hosted within the TriNetX platform. TriNetX continually works to strengthen and improve those security controls and practices.

TriNetX pulls in healthcare data from multiple territories including the US, Asia-Pacific, European Union and United Kingdom. TriNetX has ensured that it operates in a manner that is compliant with international data privacy rules and regulations. TriNetX compliance with GDPR will be covered in the following section.

5.1. TriNetX as a Joint Controller

TriNetX will act as a Joint Data Controller with existing and prospective HCOs that provide data to TriNetX, as they have a role in directing the purpose of processing. *TriNetX Live* is not an open-ended exploratory application used to mine the data, instead it has been designed with a specific purpose in mind. The application directs its users to a predefined set of workflows to allow them to address a specific objective for clinical trial design and recruitment. Extensive research and testing has enabled *TriNetX Live* to be built so that users are able to extract value from the data in the way it is intended, and chances of misinterpreting results is low.

As a Joint Controller, TriNetX will execute a Data Addendum with each of the participating HCOs.

5.2. Privacy by Design and Default (Technical and Organisational Measures)

5.2.1. Certification

To ensure the highest level of information protection TriNetX have established an Information Security Management System(ISMS) in accordance with ISO 27001:2013 that governs the processes required to protect assets and information supporting the *TriNetX Live* Platform. TriNetX uses the ISO 27001:2013 framework to identify and maintain assets, technologies and processes needed to protect customer information and to help ensure the confidentiality, integrity, and availability of customer data and supporting services.

5.2.2. Secure TriNetX Appliance

The TriNetX Appliance, a secured and locked down server, built and provided to the HCO by TriNetX, is installed at the HCO's facility, behind the HCO's firewall, and hosts the HCO Agent, the HCO's TriNetX Database and other services local to the HCO data and software for security and remote system management of the appliance.

All extraneous system processes on the appliance have been deactivated and no processes listen for inbound connections from the internet. The appliance only initiates outbound HTTPS communication to the TriNetX platform. The outbound communications from the TriNetX Appliance to the TriNetX Platform does not contain any Personal Data.

Other SSL outbound communications from the TriNetX Appliance to 3rd party providers are utilised for remote malware protection and system monitoring software used by TriNetX to remotely manage the TriNetX Appliance.

The TriNetX Appliance is viewed as an extension to their virtual datacentre. Since TriNetX is responsible for monitoring, upgrading and managing the appliance, they require remote administrative access. Remote access from TriNetX to the HCO Appliance is managed using Teleport from Gravitational. Teleport is purpose built to manage remote access to servers running within a datacentre and beyond. Teleport requires two-factor authentication, requires authorisation on a per server level, has advanced logging and session playback capabilities and supports session collaboration in troubleshooting scenarios. This access control uses outbound only communications using secure protocols and does not require VPNs, additional keys or certificates. All remote sessions are logged, and audit reports are available to comply with security audit regulations.

5.2.3. Flow of Data

The TriNetX Appliance accepts queries that are sent through *TriNetX Live* by its users, executes the queries against the pseudonymised dataset it holds within its internal databases and then returns the relevant query results back to the user.

Results from each query are in the form of discrete aggregate counts. No Personal Data/ Healthcare Data is ever transmitted, and patients cannot be identified from the aggregate counts. In the use case where a query spans a network of multiple HCOs, the count data from each HCO is added to the count data from all network members before being displayed to the user in response to their query.

The TriNetX appliance facilitates an easy integration model, enabling indirect data ingestion from any clinical system(s) and/or data warehouse(s), typically through the use of a data extract and file ingestion process that would be facilitated periodically by the HCO.

Details on the security and governance controls implemented in *TriNetX Live* and the TriNetX Appliance are available in detail in the TriNetX Security and Governance Document.

5.2.4. Pseudonymisation

TriNetX accepts data which has been pseudonymised by the HCO. Pseudonymisation 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 pseudonymised data. It 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

The HCO maintains the additional material that links the pseudonym back to the data subject, allowing re-identification if necessary for clinical reasons. TriNetX does not have access to this additional material, and therefore has no way to identify data subjects based on the data it collects.

Pseudonymisation substantially reduces the risk associated with processing of the EHRs, because re-identification is effectively impossible without the key.

5.2.5. User-Interface Privacy Design

The statistical probability of re-identifying a data subject through use of *TriNetX Live* has been reduced significantly due to design features in the application. To minimise the risk that patients could be re-identified, TriNetX obfuscates certain patient and HCO information. When conducting searches using specific criteria such as disease, choice of medications or age group, the application will not enable the retrieval of small cohorts of subjects. Where particular searches yield a small number of subjects, the subject number is rounded up to 10.

5.3. Contracts

All HCOs in the E.U. or E.E.A. will be invited to sign an amendment that includes the relevant provisions of a data processing agreement as per Article 28 of the GDPR.

5.4. Lawful Bases for Processing

Legitimate interest as set out in Article 6 has been identified as the primary lawful basis for processing of the pseudonymised EHRs. The use of pseudonymisation means that consent cannot be used as the lawful basis by TriNetX, as proper records of consent cannot be collected without identifying the data subject.

Instead, TriNetX has documented a legitimate interest in storing and processing the pseudonymised records, to facilitate the more efficient operation of clinical trials. This is the subject of a separate Legitimate Interests Assessment.

A secondary lawful basis for processing applies to the underlying TriNetX software administration layer, which identifies a limited number of persons for administration purposes. These persons are employees

of TriNetX or employees of the HCO or CRO and Pharma customers. The lawful basis for recording their name, username, email address, and encrypted login credentials is fulfilment of contract.

5.5. Data Security

The security principle of GDPR requires data controllers and processors to implement and document appropriate technical and organisational measures for data security. TriNetX is an ISO/IEC 27001:2013 certified organisation. ISO/IEC 27001:2013 is a globally recognised standard for the establishment and certification of an Information Security Management System (ISMS). The standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organisation's overall business risks. It sets forth a risk-based approach that focuses on adequate and proportionate security controls that protect information assets and give confidence to interested parties which includes TriNetX members and customers. The TriNetX ISMS supports the infrastructure and services used to manage the information assets, staff, processes and technology behind the TriNetX platform.

The details of the TriNetX ISO/IEC 27001:2013 Certification are available here.[2]

5.6. Data Transmission

The TriNetX platform is deployed in a secure Virtual Private Cloud (VPC) hosted on Amazon Web Services (AWS) which is the leading provider of cloud hosted services. Detailed information regarding AWS security is available here[3]. All access to *the* TriNetX platform is over HTTPS (TLS only) with a 2048-bit SHA256 certificate.

Different browsers make use of different SSL/TLS handshake and encryption algorithms. The TriNetX services which are hosted behind an AWS Elastic Load Balancer (ELB) are configured to use the latest AWS ELB Security Policy which at the time is 2016-08. Full details of the protocols, options and ciphers allowed by this policy are here[4]. The policy includes protection from all known SSL vulnerabilities. AWS updates their SSL policy from time-to-time and TriNetX reviews and updates their configuration as new policies are issued.

TriNetX currently supports Google Chrome (version 47.x and higher) and Microsoft Internet Explorer (version 11.x and higher).

5.7. Special Category Data Processing

EHR information is pseudonymised prior to being loaded in to the TriNetX Appliance. This pseudonymisation is the sole responsibility of the HCO, which will retain the key as well as any other material which is required to allow re-identification. At no time will it be possible for re-identification of

[2] TriNetX ISO 27001:2013 Certification: https://cert.schellmanco.com/?certhash=s6mGTy52Qteb
[3] AWS Security: https://aws.amazon.com/security/
[4] AWS ELB Policy: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-table.html

EHR data contained within the TriNetX system. This is also enforced in the contract between the HCO and TriNetX, which stipulates clearly that such Pseudonymisation is mandatory.

Because re-identification is still theoretically possible, for example if there is a data breach at the HCO, the data must still be treated as in scope of GDPR. Additionally, because it is largely special category data, we must apply Article 9, that affirms processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

The Keeling Schedule for GDPR, as amended on 5th March 2018, states the following:

> *(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the applied GDPR (as supplemented by section 19 of the 2018 Act) and is authorised by domestic law (see section 10 of that Act).*

TriNetX relies on the exemption to GDPR Article 9 outlined in Part 2 Section 10(1)(e), i.e. "archiving, research and statistics."

In any case, the HCO is obligated, both as a matter of law and of contract, to obtain consent from data subjects to permit processing of special category data. Such consent is not relied upon by TriNetX however, due to the fact that the health records are pseudonymised. Instead, TriNetX has a legitimate interest to facilitate the carrying out of medical research based on the data it holds, which has been balanced against the rights and freedoms of the data subjects.

Consent from those data subjects is recorded and maintained by the HCO; such records of consent are not available to TriNetX, as they would allow re-identification of individuals. Due to this reason, TriNetX cannot process SARs for individual users.

5.8. Data Protection Officer

TriNetX has appointed a Data Protection Officer (DPO) to act for the company as the independent advisor on data protection matters. The following are the contact details of the DPO

Kshitij Kathuria
VP, Security & Compliance
125 Cambridgepark Drive, Suite #500. Cambridge. MA. 02140. USA.
Email: Kshitij.kathuria@trinetx.com
Phone: +1-857-285-6051
Fax: +1-617-945-2091

5.9. Data Protection Impact Assessment

TriNetX conducted a detailed Data Protection Impact Assessment (DPIA). The DPIA is an analysis of expected data processing activities performed by TriNetX on the EHR data provided by the HCOs and any related activities. It is also an assessment of the risks associated with the processing activities including

any measures that need to be taken to mitigate those risks. It also identifies whether the necessity of processing personal data balances out the privacy rights of collecting and processing the data.

This DPIA is performed due to the requirement per Article 35 of the GDPR, where processing is likely to result in a high risk to the rights and freedoms of natural persons.

This section considers the risk to natural persons, in this case participants in the assessment process. Other risks which apply to the organisation, but which do not impact privacy, are out of scope. What is in scope are risks which could lead to physical, material or non-material harm to the data subject, including any discrimination, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage.

In this analysis, all risks are also associated with a "likelihood" based on the definitions below

Classification	Definition
Almost Certain	• Threat-source is guaranteed. • Controls are not able to prevent the vulnerability from being exercised. • The threat-source can be both internal and external. • There is residual risk.
Likely	• The threat-source is highly motivated and capable. • Controls are not able to prevent the vulnerability from being exercised. • The threat-source can be both internal and external. • There is residual risk.
Possible	• The threat-source is motivated and capable. • Controls are in place that may impede, but not prevent, successful exercise of the vulnerability. • The threat-source can be both internal and external. • There is residual risk.
Unlikely	• The threat-source lacks motivation and capability. • Controls are in place that prevent the vulnerability from being exercised. • The threat-source can only be external. • There is no residual risk.
Rare	• There is no identifiable threat-source. • There are no vulnerabilities requiring controls. • There is no residual risk.

The analysis also determined the "impact" levels based on the definitions below

Classification	Definition
Major	This impact rating represents a significant level of business risk to enterprise information systems and assets. The High Magnitude of Impact Classification deals with highest level of sensitive and confidential information that if modified or disclosed could cause severe consequences such as legal, regulatory, financial or negative public perception impact. • **Information Sensitivity** - Examples include: Credit Card Number/ Expiration Date, PHI, SSN • **Company Branded** – applies to sites carrying Company logo or disclosure that Company is endorsing the site. • **High Profile** – applies to sites with high reputational risk, due to public placement and media coverage. • **Connectivity** – applies to external connection to Internet or other public Networks. • **Architecture** – applies to non-standard and not approved architecture. • **Regulatory** – there is a specific legal compliance requirement.
Moderate	This impact rating represents a moderate level of business risk to enterprise information assets. The Medium Magnitude of Impact Classification deals with such levels of sensitivity and confidentiality that in case if modified or disclosed, it could cause legal, regulatory, financial, or negative public perception impact. • **Information Sensitivity -** Examples include: Consumer Name, Address, Account Information, and other Privacy Related data • **Company Affiliated –** applies to sites where Company Logo is not necessary but may include other companies such as a consortium. • **Connectivity –** applies to dedicated /leased lines, or connections to subs/affiliates. • **Architecture –** applies to varying types of architecture generally implemented using standard and accepted architecture, but with applied special circumstance.
Minor	This impact rating represents a low level of business risk to enterprise information assets. The Low Magnitude of Impact Classification deal with low if any level of sensitive and confidential information. Disclosure or modification of the data could cause company restricted impact or if designed to be public in nature will cause little if any consequences. • **Information Sensitivity** - Examples include: Employee Name and Status, Cost Centre • **Non-Company Branded –** applies to sites where Company Logo would not appear and no disclosure to Company affiliation is present on the site. • **Connectivity –** applies to the internal connection within Company WAN. • **Architecture** – applies to standard, approved, and existing architecture.

Using a qualitative approach, the likelihood times the impact (consequence) was used to determine the risk level. The table below shows the Risk Levels and how they are determined.

Risk Level	Description
High	This is the highest level of risk as it affects sensitive and confidential information that if modified or disclosed could cause severe consequences such as legal, regulatory, financial or negative public perception impact. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	This information, if modified or disclosed, could cause legal, regulatory or negative public perception impact. Corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period.
Low	Disclosure or modification of the data could cause company restricted impact or if designed to be public in nature will cause little if any consequences. The asset owner must determine whether corrective actions are still required or decide to accept the risk.

The table below shows the summary of the assessment.

Note: All healthcare data provided by the HCO is Pseudonymised prior to being provided to TriNetX and hosted on the TriNetX Appliance. A data subject / patient cannot be re-identified using the data from the TriNetX Appliance without access to additional material used to pseudonymise the data which in sole possession of the HCO. TriNetX has no access to this material nor is aware of where this additional material is stored. The assessment below has been conducted based on this fact.

ID	Threat description	Likelihood	Impact	Risk Level	Risk Mitigation / Controls in place
1	Interception of data during transmission between *TriNetX Live* and the TriNetX Appliance (man in the middle attacks or wire sniffing).	Unlikely	Moderate	Low	The TriNetX platform is deployed in a secure Virtual Private Cloud (VPC) hosted on Amazon Web Services (AWS) which is the leading provider of cloud hosted services. All access to the TriNetX platform is over HTTPS (TLS only) with a 2048-bit SHA256 certificate. The TriNetX Appliance is secured and locked down. All extraneous system processes have been deactivated and no processes listen for inbound connections from the internet. The appliance only initiates outbound HTTPS communication to the TriNetX platform in the AWS VPC over the public internet
2	Physical access to data stored on the TriNetX Appliance. Extraction of data using portable media.	Unlikely	Moderate	Low	Physical Access to the TriNetX Appliance is controlled by the HCO as it is hosted within their data centre. It is assumed that the HCO has all the Physical and Environmental controls in place to protect their infrastructure.

					TriNetX uses Full Disk Encryption (FDE) on the TriNetX Appliance. Any data extracted from the appliance using portable media would be rendered useless.
3	Software vulnerability, failure to patch or malware allows an attacker access and causes a data breach.	Possible	Moderate	Low	TriNetX maintains the TriNetX Appliance on a regular basis patching the various components of the application architecture as required by the TriNetX Risk Treatment methodology. TriNetX uses a malware protection suite on the TriNetX Appliance which is kept up to date with new definitions.
4	Insiders using their access to extract data.	Possible	Moderate	Low	All access in TriNetX is granted on a "Need to Know" basis and a Role Based Logical Access model is used to grant access. Limited individuals have access to the TriNetX Appliance once it is provisioned and hosted behind the HCO's firewall. Privileged and unprivileged access is reviewed on a quarterly basis. Access is removed promptly upon termination of employees. All access and activity on the TriNetX Appliance is monitored, logged and reviewed periodically.
5	Access to data by subcontractors and vendors	Unlikely	Minor	Low	TriNetX does not allow any individuals who are not direct employees of TriNetX access to the TriNetX Appliances hosted in the EU. TriNetX may however use Subcontractors and Vendors for other support services related to its products. TriNetX has a Vendor Risk Management Program and ensures that all Subcontractors and Vendors go through a rigorous vetting process before providing any services. Subcontractors and Vendors are subject to the same level of Security controls as TriNetX.
6	Risk of loss of data in a disaster	Unlikely	Minor	Low	The TriNetX Appliance ingests fresh data from the original source on a periodic basis. Every time an HCO provides new data, the existing data is purged, and new data is ingested. In the event of a disaster, the TriNetX Appliance would be rebuilt, shipped and re-provisioned at the HCO site and data will be re-ingested from the original source. Note that the TriNetX Appliance is not the original source of data and is also not a mission critical application.
7	Risk of failure of controls	Unlikely	Major	Low	TriNetX believes in Security by Design and therefore has multiple controls at various levels in the architecture of the TriNetX Appliance and *TriNetX Live* which makes it

					virtually impossible to extract healthcare data. In the event that a single control fails, there are other controls in place. At the highest level, all data provided to TriNetX has been Pseudonymised at source which significantly reduces the risk of reidentification of a data subject even if various controls fail for some unknown reason.

5.9.1. Identification of the Need for a DPIA

The implementation of the *TriNetX Live* service requires the introduction of an innovative technical approach to make life easier for HCOs in the communication of clinical trial data to researchers, whilst preserving the privacy of trial participants.

A DPIA is generally required for new projects where they may be a significant risk to the rights and freedoms of individuals. Specifically, due to the processing of special category health data, we have evaluated that unauthorised access to such data would constitute such a risk.

5.9.2. Nature, Scope, Context and Purpose of Processing

The nature of processing is the aggregation of pseudonymised EHR data in a manner that facilitates the possibility of researching treatments, drug administration and clinical outcomes.

The scope of processing is the collection and aggregation of a large scale of special category data, grouped at the highest level by the TriNetX appliance, which collects data from a single HCO, covering all trials submitted by the HCO to the system. Usually, this data consists of the EHR data of groups of trial participants, or other groupings selected by the HCO for submission to the study platform offered by *TriNetX Live*.

The context of the processing is to facilitate research by CROs and pharmaceutical companies, with the aim of improving clinical outcomes through modifications of drug protocols or other treatment methodologies. The purpose underlying the processing is to facilitate the communication of the EHR data between HCOs and CROs or pharmaceutical companies in a way that maintains both security and privacy.

5.9.3. Necessity, Proportionality and Compliance Measures

We believe that the necessity of the processing is clearly in the public interest, to improve treatment outcomes of various types of disease, as well as indirectly improving the profits of the CROs and pharmaceutical companies. Additionally, it could be argued that such processing is in the vital interests of the data subjects who are members of the clinical trial, as it can lead to improved treatments and better outcomes for their particular problems.

Proportionality may be judged based on the accrual of benefits to the members of trials, both individually or collectively. The processing of their medical data is essential to receive such benefits.

Compliance measures are fully documented elsewhere in this white paper.

5.10. Article 30 Records of Processing Activities

TriNetX has completed its obligations under Article 30 to document its processing activities, specifically those which are in scope for GDPR.

5.11. EU Representative

TriNetX has appointed an EU Representative according to Article 27. The EU Representative will liaise with the supervisory authority in EU countries where TriNetX has customers, as well as data subjects, on all issues related to processing, for the purposes of ensuring compliance with the regulation. The EU Representative is:

Chaucer Consulting Ltd.
Northern & Shell Building
10 Lower Thames St.
London
EC3R 6EN
Email: compliance@chaucer.com

5.12. International Transfer of Personal Data

The lawful transfer mechanism for countries outside the EU/EEA is based on the EU-US Privacy Shield. TriNetX is certified under EU-US Privacy Shield Framework and its status can be validated here[5].

5.13. Data Privacy Notice

TriNetX provides a Privacy Notice to all users of *TriNetX Live* before the user's access to the application for the first time. The Privacy Notice is also viewable to the users from the profile section of *TriNetX Live.*

5.14. Personal Data Breach Response Plan

TriNetX has a Breach Notification and Incidence Response Plan which identifies appropriate steps to follow if Sensitive Data or Personal Data is breached or exposed to unauthorised individuals. This response to any potential data breach situation fulfils TriNetX's legal and contractual obligations including GDPR

[5] TriNetX EU-US Privacy Shield Framework: https://www.privacyshield.gov/participant?id=a2zt00000004FDEAA2&status=Active

Article 33 and will minimise the risk to any data subjects who may be affected by the potential data exposure as well as minimum risk to TriNetX.

The plan includes notification of a data breach to its EU Representative through its DPO and further to controllers of Personal Data (HCOs) whose data may have been compromised during the potential breach within the 72 hours of becoming aware of the breach.

Note that as a joint Controller, TriNetX may in some circumstances also notify the relevant supervisory authorities in countries where individuals may be affected by a breach, and where there is an impact on the rights and freedoms of individuals, may also notify those persons affected. This notification will be carried out in conjunction with their EU Representative.

It should however be noted that TriNetX does not have any information about the identities of data subjects whose personal data is being processed, as they are pseudonymised, therefore such notification can only be carried out by the joint Controller with possession of the additional materials required to reidentify the data subjects.

5.15. Governance Framework

TriNetX is governed by a Board of Directors who meet on a regular basis (5x annually) to go over various initiatives within TriNetX. The profiles of the TriNetX Board of Directors are available here[6].

TriNetX is an ISO/IEC 27001:2013 certified organisation. ISO/IEC 27001:2013 is a globally recognised standard for the establishment and certification of an Information Security Management System (ISMS). The standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organisation's overall business risks. The TriNetX ISMS Committee comprises of its CEO, Security Officer, Privacy Officer, CTO and VP of Engineering. The ISMS Committee meets on a quarterly basis to specific Security & Compliance based initiatives.

All efforts related to compliance with GDPR were presented to the TriNetX ISMS Committee in its Quarterly Meeting which was conducted on November 29, 2017. The committee approved the budget presented to move forward with all compliance efforts.

In the last Quarterly TriNetX ISMS Committee meeting conducted on March 5, 2018, it was agreed that a Data Protection Officer (DPO) would be nominated and approved by the Board of Directors before May 25, 2018. It was also agreed that TriNetX would hire the services of a 3rd party to complete a GDPR gap assessment.

The Board of Directors approved the appointment of Mr. Kshitij Kathuria as the DPO and Chaucer as the TriNetX EU Representative on April 25, 2018.

[6] TriNetX Board of Directors: https://www.trinetx.com/board-of-directors/

6. Ongoing Compliance

In addition to the provisions of GDPR, TriNetX has exercised all necessary due diligence to make itself compliant with the provisions of HIPAA (for the USA).

Furthermore, TriNetX has taken steps to comply with the potential variations in privacy laws in various European countries, where such laws differ from GDPR.

7. Summary and Conclusions

We have examined TriNetX's assertion that they have undertaken all required steps to establish an on-going program of compliance with the General Data Protection Regulation (GDPR) and related laws. TriNetX management is responsible for the assertion. Our responsibility is to express, an opinion based on our examination. We believe that our examination provides a reasonable basis for our opinion.

Furthermore, specific analysis of the *TriNetX Live* platform shows that, as described in the related Data Protection Impact Assessment and Legitimate Interests Assessment, all applicable principles, guidelines and regulations have been adopted to ensure that the product and related services are fully compliant with the relevant privacy laws in the European Union.

DocuSigned by:
Stephanie Roberts
21BA85AA2C2B4F5...

Stephanie Roberts
Management Consultant
Chaucer Life Sciences

DocuSigned by:
Paul Gillingwater
C6663F5CB1B24D7...

Paul Gillingwater
Associate Partner
Chaucer Group

