Nuventra PHARMA SCIENCES	**Overall Data Privacy Policy**
	Privacy Policy 001 Effective Date: 12 March 2021

TABLE OF CONTENTS

1. INTRODUCTION

Nuventra, Inc. (and its subsidiaries and affiliates, collectively referred to as "Nuventra," Company," "we" or "our") has been providing drug development services in the US and Globally for over 10 years. Nuventra US operations are based in Durham, NC with additional offices in Exton, PA, and Broomfield, CO.

Nuventra respects the relationships we have with our clients and respects the privacy of all data subjects whose personal data may be processed by Nuventra in the performance of our services and our normal business operations. To demonstrate our commitment to the protection of data transferred out of the European Union (EU) and the European Economic Area (EEA) for the performance of our services and business operations, we adhere to the General Data Protection Regulation (GDPR) [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016] as described herein, which is directly applicable as law in all 28 EU countries. GDPR is the EU legal framework focusing on harmonizing the protection of personal data, which means any information relating to an identified or identifiable natural person or what it calls a "data subject". The GDPR affects all organizations and public entities, wherever located, that handle data of persons residing in the EU. Nuventra will adhere to this regulation when collecting any data concerning an EU citizen.

In addition to GDPR, Nuventra will also adhere to the United Kingdom General Data Protection Regulation (UK-GDPR) which was made effective on 31 January 2020, as well as any applicable US State Privacy laws.

2. POLICY SCOPE

The scope of this policy includes appropriate administrative, technical and physical safeguards and other security measures that are designed to: (i) ensure the confidentiality, integrity, and availability of Personal Data; (ii) protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Personal Data; and (iii) protect against unauthorized access, use, or disclosure of Personal Data.

Note: In general, data received by Nuventra is Key-Coded Data/pseudonymised so that personal data can no longer be attributed to a specific data subject.

3. DEFINITIONS

Administrative, Technical, Organizational and Physical Security Measures	Administrative, technical, organizational and physical measures designed to protect the confidentiality, security, integrity and confidentiality of Personal Data, including measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.
Affiliate	An entity related to Nuventra through common ownership or control.
Applicable Law	Any Applicable Law or regulation including, but not limited to, the laws and regulations of the European Economic Area, European Union member states United Kingdom and Switzerland, that relate to the Processing of Personal Data, including, but not limited to, from 25 May 2018, the General Data Protection Regulation (EU 016//679) ("GDPR the Electronic Communications") Regulations 2003 ("EC Directive"), and any legislation which amends, re-enacts or replaces any such instrument.
Biometric Data	Personal data resulting from specific technical processing related to physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Consent	Consent of the data natural person means any freely given, specific, informed and unambiguous indication of the data natural person's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Controller	Refers to the natural or legal person, public authority, agency or 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 such processing are determined by the Union (EU) or Member State (EEA) law, the controller or the specific criteria for its nomination may be provided for the Union or Member State law.
Data Controller	The entity which alone or jointly with others determines the purposes and means of the Processing of Personal Data.
Data Privacy Program	Nuventra's comprehensive written privacy and information security program.
Data Processor	An entity which Processes Personal Data on behalf of the Data Controller

Data Protection Officer	The person designated for ensuring compliance with Applicable Law and involved in all issues which relate to the protection of Personal Data and performing the tasks described in Articles 38 and 39 of the GDPR.
Data Subject (Consumer under US State Privacy Laws)	An identified or identifiable natural person in accordance with Article 4(1) of GDPR; an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person but as related to only natural persons residing within the European Union (EU) or Member State (EEA). A consumer is any natural person who is a resident of a state.
Encryption	The transformation of data through the use of an algorithmic Process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential Process or key in accord with industry best practices for data Encryption. "Unencrypted" means data that is not encrypted or is encrypted using an Encryption method of insufficient strength.
European Economic Area EEA	Refer to www.efta.int for the current list of the EEA member states.
Genetic Data	Personal data related to the inherited or acquired genetic characteristics of a natural person which give unique information about physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
Personal Data	Any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural 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, an online identifier (IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person as related to only natural persons residing within the European Union (EU) or Member State (EEA).
Personal Data Breach	A Breach of security leading to the unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

Process or Processing	Any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, restriction, erasure or destruction.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data natural person without the use of additional information, provided that such additional information is kept separately.
Recipient	A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
Records	All Personal Information, documentation, data, records, materials, and information obtained or generated by Nuventra in the course of providing services to a client.
Security Incident	Security Incident shall mean any of the following: a) a Personal Data Breach; b) a security vulnerability that carries a material risk of compromising the confidentiality, integrity, or security of Personal Data; but shall exclude: a) any unintentional acquisition, access, or use of Personal Data by an employee or agent of Nuventra if such acquisition, access, or use was made in good faith and does not result in further unauthorized or inappropriate Processing of Personal Data; b) any inadvertent disclosure by a person who is authorized to access Personal Data on behalf of Nuventra to another person authorized to access Personal Data on behalf of Nuventra, provided the information received as a result of such disclosure is not further used or disclosed in an unauthorized or inappropriate manner; or c) any loss or unauthorized acquisition of or access to Encrypted Personal Data, provided the confidential Process or key that is capable of compromising the security, confidentiality, or integrity of the Encrypted Personal Data is not also subject to loss or unauthorized acquisition or access.

Sensitive Personal Data	Personal Data, the unauthorized access, use, or disclosure of which could threaten serious harm to the rights or interests of Data Subjects, including: (a) Personal Data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life; (b) Personal Data Subject to obligations of professional secrecy; (c) Personal Data referring to criminal or administrative offences or to suspected criminal or administrative offences; (d) Personal Data concerning bank or credit card accounts; or (e) identification numbers specially protected by local laws (e.g., Social Security Numbers). Any other data which, if involved in a Security Incident, would result in a breach notification obligation to Data Subjects or government authorities under Data Protection Laws, including but not limited to usernames and passwords.
Sub-Processor	Any third party engaged by Nuventra to Process Personal Data on behalf of Company but excludes any Affiliate of Nuventra.
Supervisory Authority	A "Supervisory Authority" as defined in Article 4(21) of the GDPR as well as any other legislative, executive, administrative, or regulatory entity, judicial body, or other public agency or authority of any country, state, territory, or political subdivision of a country, state, or territory, or a person or entity acting under a grant of authority from or under contract with such public agency or authority, that is authorized by law to enforce individual rights with respect to Personal Data, or to oversee or monitor compliance with privacy, data protection, or data security laws, rules, regulations, or other Applicable Law.
Third Party	A natural or legal person, public authority, agency, or body other than the data natural person, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

4. ASSOCIATED RESOURCES

- Privacy Policy 003 Incidence Response Policy
- Privacy Form 003f_Sub-processor Data Processing Agreement Template
- Privacy Form 004f Request for Personal Data Deletion Form
- General Data Protection Regulations (GDPR; EU law)
- United Kingdom General Data Protection Regulations (UK-GDPR)
- US State Privacy Laws as applicable to Nuventra's business processes

5. DATA SECURITY AND PRIVACY MEASURES

Nuventra's data privacy security measures are summarized in this section.

Nuventra conducts the following procedures:

1. Monitors the effectiveness of its safeguards, controls, systems, and procedures, including conducting internal security assessments and security gap analyses and correcting discovered security gaps in a timely manner.
2. Has an enterprise-wide authentication management strategy with standard authentication process for remote access.
3. Has network traffic pass through firewall(s).
4. Maintains policies and procedures to protect against malware (e.g., viruses, worms, ransomware, spyware).
5. Provides continuous network security monitoring by qualified staff.
6. Conducts periodic security awareness exercises to train staff to recognize social engineering attacks (e.g., phishing) and reinforce the importance of cybersecurity.
7. Has role-based access controls in place that are reviewed and updated as needed, to constraining user-level access to those with a "need to know", with periodic reviews of access entitlements—particularly those granted to privileged users.
8. Uses encryption or secure technologies in connection with any transmission, transfer, communication, or remote access connectivity involving Personal Data. Nuventra encrypts Personal Data, whether in transit or at rest, including that which is stored on laptop computers, removable media, or other portable computer devices or media.
9. Ensures that security procedures applicable to Personal Data comply with the following electronic security specifications: (i) log-in validation; (ii) creation of accounts on a 'need to know' basis; (iii) secure encrypted connections to access servers; (iv) a level of virus protection in keeping with industry best practice; and (v) servers firewalled in accordance with current best practice.
10. Ensures that any premises at which the services (or any part thereof) are carried out have effective physical security controls.

11. Maintains a secure disposal procedure to provide sanitization of electronic media prior to reuse or disposal.
12. Maintains a commercially reasonable business continuity and disaster recovery plan that describes the procedures to be followed with respect to the continued provision of the services if any portion of the services are unavailable for the Company's use because they are damaged, destroyed, or otherwise unavailable for use for any reason whatsoever.
13. Periodically tests the business continuity and disaster recovery plan.
14. Maintains documented backup procedures, conduct periodic backup of data, and maintain backup media.
15. Has an incidence response plan (Refer to Privacy Policy 003; Section 4) and incidence form for actual or suspected Personal Data Breach.
16. Ensures that sub-processors of Personal Data enter a written agreement agreeing to abide by the terms of this policy.
17. Ensures that clients are designated as the 'Data Controller', as defined by the European Union General Data Protection Regulation ("GDPR"), and Nuventra shall be designated as the 'Data Processor' in regard to such European Economic Area Personal Information.
18. Has a Data Protection Officer and designated backup Data Protection Officer to oversee this policy.

6. NOTICE

Where Nuventra collects Personal Data directly from data subjects, it will provide clear and conspicuous notice of the purposes for which it collects and uses Personal Data about the data subject, the types of third parties to which Nuventra discloses that information, and the choices and means, if any, Nuventra offers data subjects for limiting the use and disclosure of Personal Data about them. This explanation will be provided as soon as practicable and, in any event, before Nuventra discloses the Personal Data or uses such information for a purpose materially different than that for which it was originally collected or processed. Where Nuventra receives Personal Data from its subsidiaries, affiliates or other entities, including when acting as a Contract Research Organization (CRO) processing Personal Data under the direction of a Client, it will use such information in accordance with the notices provided by such entities and the choices made by the data subjects to whom such Personal Data relates.

Nuventra staff has documented training on this Privacy Policy to ensure compliance.

Nuventra has a Privacy Notice which details the purposes of processing and legal basis for the processing of all personal data.

6.1. Nuventra as a Data Controller

Nuventra gathers contact information (e.g., email, phone number, physical address) from individuals (Data Subjects) that contact Nuventra through Nuventra's website, by email, through marketing or business development campaigns, at conferences/webinars, or by phone in order to contact individuals who are interested in Nuventra's services. Nuventra uses this information for internal business purposes only and does not sell any of this information.

Nuventra also gathers contact and personal information for individuals (Data Subjects) who apply to work at or for Nuventra. Nuventra's Human Resources department must gather basic information regarding work history, contact information, etc. to make informed decisions for hiring individuals. This information is used for internal hiring decisions only and Nuventra does not sell this information.

6.2. Nuventra as a Data Processor

For any individual who participates in a clinical trial, Nuventra's Clients are designated as the Data Controller and Nuventra is designated as the Data Processor. **As such, Nuventra will provide the rights of data subjects outlined in Section 7 based on the instructions of the Data Controller (Client) only.**

Nuventra provides services on behalf of our clients and as such receive clinical trial data. Nuventra processes clinical trial data as outlined in the scope of work and/or data processing agreement that has been approved by both the Client and Nuventra.

6.3. Pseudonymisation

Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data natural person without the use of additional information, provided that such additional information is kept separately

Pseudonymised data that could still be attributed to a trial participant using other information will be considered personal data. Only the anonymization of data will ensure that the data is no longer considered to be personal data.

Nuventra considers subject data from clinical trials processed for clients as personal data.

7. RIGHTS OF DATA SUBJECTS

Clients are designated as the Data Controller and Nuventra is designated as the Data Processor. **As such, Nuventra will provide the following rights based on the instructions of the Data Controller (Client) only**.

- The right to data portability (i.e., the data subject's right to obtain the personal data that he/she provided, in a structured, commonly used and machine-readable format, and to transmit, or have the data transmitted to a controller). This applies to data based either on a contract or a valid consent and is carried out by automated means such as a database or other IT systems.
- The "right to be forgotten" and the option to have personal data corrected, deleted, or restricted, including the right to data portability, as applicable under all other regulations (ICH GCP E6 R(2) and US FDA 21 CFR Part 11 regulations, at minimum) for which Nuventra is subject to.
- The right to lodge a complaint with a supervisory authority.
- The right to object to the processing of personal data.
- The right to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects the data subject.
- The right to withdraw consent and the right to understand the basis for legitimizing the export of personal data from the EU.

8. ACCOUNTABILITY FOR ONWARD TRANSFER

Nuventra may also share a data subject's Personal Data with a third-party who assists Nuventra in connection with providing services that these individuals or entities perform for, or with, Nuventra. Nuventra may, for example, provide a data subject's Personal Data to a third-party for hosting our databases, for data processing services, or to send to that data subject the information that he or she requested.

Nuventra may transfer Personal Data for specified, limited purposes to a third-party and will endeavor to obtain written agreement with such third-party providing for at least the same level of data privacy protection as is required by this Policy.

Where Nuventra knows that any third-party to whom it has provided Personal Data is using or disclosing Personal Data in a manner contrary to this Policy, Nuventra will take reasonable steps to prevent or stop the use or disclosure.

9. SECURITY

Nuventra will employ reasonable and appropriate technical, administrative and physical safeguards designed to protect Personal Data in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the Personal Data Nuventra is handling.

10. PERSONAL DATA BREACH

In the event Nuventra experiences a Personal Data Breach, Nuventra, as a Data Processor, will notify the Data Controller without undue delay after becoming aware of a personal data breach.

Nuventra as a Data Controller, will document any data breaches and will inform the affected data subjects if the breach is likely to result in a high risk to their rights and freedoms (i.e., concerns of sensitive data; when a large amount of personal data is involved and affects a large number of data subjects; when it may give rise to significant economic or social disadvantages such as discrimination, identity theft, or damage to reputation). Such notification will be communicated without undue delay and will be made in a clear and plain language.

11. DATA INTEGRITY AND SAFEGUARDS

Nuventra endeavors to take reasonable steps to use Personal Data only in ways that are compatible with and relevant to the purposes for which it was collected and for which notice was provided or for which consent was given or subsequently authorized by the Data subject. Nuventra will implement appropriate safeguards for protecting data including: pseudonymisation and/or encryption of personal data; ensuring ongoing confidentiality, integrity, availability, and resilience of systems; restoring the availability and access to data in a timely manner following a physical or technical incident; and instituting a process for regularly testing, assessing, and evaluating the effectiveness of these systems. Nuventra will take reasonable steps designed to ensure that only the Personal Data that is relevant to its intended use, accurate, complete, current, and otherwise reliable in relation to the purposes for which the information was obtained is used by Nuventra for as long as Nuventra retains possession of such information. Nuventra's Personnel have a responsibility to assist Nuventra in maintaining accurate, complete and current Personal Data. When acting as a CRO, Nuventra endeavors only to process Personal Data that is relevant to the services it provides,

and only for purposes compatible with those for which the Personal Data was collected; wherever possible, such Personal Data is de-identified.

12. ACCESS

Nuventra processes Personal Data under the direction of its clients (Data Controllers). Nuventra will, upon written request of the Data Controller, provide a data subject with confirmation regarding whether Nuventra is processing Personal Data about them. In addition, upon request of a data subject and Data Controller, Nuventra will take reasonable steps to correct, amend, or delete their Personal Data that is found to be inaccurate, incomplete or processed in a manner non-compliant with this Policy or the GDPR, except where the burden or expense of providing access would be disproportionate to the risks to that data subject's privacy, where the rights of persons other than the data subject would be violated, where clinical trial regulations dictate requirements for retaining data, or where doing so is otherwise consistent with GDPR policy.

13. RECOURSE, ENFORMENT, AND LIABILITY

Any questions or concerns regarding the use or disclosure of Personal Data should also be directed to Nuventra's Data Protection Officer through the contact information given below. Nuventra will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Data in accordance with the principles contained in this Policy, GDPR, and any applicable US state privacy laws.

Data Protection Officer contact: privacy@nuventra.com

Any personnel that Nuventra determines is in violation of this Policy will be subject to disciplinary action up to and including termination of employment, where applicable.

14. APPROVAL

Upon approval of this policy by Nuventra's CEO and Data Protection Officer the policy will become effective.

Approval signatures for this policy are maintained outside of this document.

15. VERSION HISTORY

Effective Date	Notes
31 March 2019	Original
12 March 2021	US State Privacy Laws references added. General updates to current business practices added. Information for how Nuventra controls and processes data in Section 6. Approval and Version History sections added.