



## **Purchase Order Terms and Conditions**

Vendor named on the face of the Purchase Order agrees to be bound by these terms and conditions ("Terms") upon: i) receipt and acceptance of the Purchase Order; or ii) commencing performance of the services or provision of the goods described on the face of the Purchase Order or attached thereto.

### **1. Relationship of the Parties**

The relationship of Vendor to Research Triangle Institute d/b/a RTI Health Solutions ("RTI" or "RTI-HS") is that of an independent contractor and nothing in these Terms shall be construed as creating any other relationship. Vendor shall comply with all laws and assume all risks and obligations arising from its status as an independent contractor. This includes, but is not limited to, responsibility for all applicable federal and state income taxes, payroll and business taxes, licenses, permits, and fees.

### **2. Provision of Deliverables, Standard of Performance**

Vendor shall perform the services or deliver the goods which are set forth on the face of the Purchase Order (collectively the services and goods constitute the "Deliverables") to which these Terms are attached and shall furnish the necessary qualified personnel, materials, services, equipment and facilities to provide the Deliverables.

Vendor shall furnish the Deliverables: (i) in accordance with these Terms and with reasonable care, skill and diligence, and in a workmanlike and scientific manner; (ii) in compliance with all applicable laws and regulations including but not limited to the regulatory requirements listed in Section 6d, and shall obtain all required licenses, approvals and permits necessary to furnish the Deliverables; (iii) according to the standards and industry guidelines for quality and performance adopted by comparable organizations performing similar work; and (iv) in a manner substantially consistent with the RTI Code of Conduct, which can be accessed on the RTI website at: [https://www.rti.org/sites/default/files/rti\\_code\\_of\\_conduct.pdf](https://www.rti.org/sites/default/files/rti_code_of_conduct.pdf).

### **3. Record Retention, Inspection**

Vendor shall retain all financial books and records relating to this Purchase Order at its sole expense, for a period of three (3) years following termination of this Purchase Order. Vendor shall return or destroy RTI's project records, materials, data and Results in accordance with Paragraph 8d unless otherwise instructed by RTI.

RTI may, in its sole discretion, require that Vendor undergo a qualification by RTI's Office of Quality, either prior to commencing the services or during the term of this Purchase Order, to evaluate Vendor's policies and procedures, quality control and quality assurance practices, regulatory compliance, and compliance with these Terms.

Vendor shall permit RTI or its client, upon reasonable notice and during regular business hours, to audit any Services performed and all books and records relating to such Services, the facilities where the Services are or will be performed, the data processing systems used in the performance of the Services, if applicable, and the supporting documentation for invoices submitted to RTI by Vendor, to confirm that the Services are conducted in accordance with these Terms. If Vendor fails to demonstrate quality or compliance practices as required by these Terms, RTI may in its sole discretion require prompt corrective action, withhold payment or terminate the Purchase Order.

Vendor shall maintain and make available for inspection all work product and Deliverables in accordance with these Terms.

### **4. Invoicing and Payment Terms**

RTI will reimburse Vendor for Services actually performed and goods furnished in accordance with this Purchase Order.

- a. All invoices shall specify the invoice number, Purchase Order number, Deliverables completed, total amount due and cumulative amount billed.
- b. Vendor shall send invoices via electronic mail to [HSAccountsPayableUS@rti.org](mailto:HSAccountsPayableUS@rti.org). Questions regarding submitted invoices should be directed to RTI Accounts Payable at +1-919-541-6903.
- c. All equipment purchased by Vendor and reimbursed by RTI shall become the sole property of RTI.
- d. RTI will pay invoices within thirty (30) days of receipt. RTI shall promptly notify Vendor if it intends to withhold payment of any portion of a submitted invoice due to defect or other discrepancy with a Deliverable. Vendor shall submit its final invoice to RTI within sixty (60) days following completion of the Deliverables.
- e. RTI shall issue payments by Electronic Funds Transfer (EFT). Within ten (10) days of the execution of this Purchase Order, Vendor shall submit a completed EFT form provided by RTI. All EFT information and any changes to EFT

information shall be sent to the email address provided on the form.

## 5. Term and Termination

This Purchase Order shall be effective during the period set forth on the face of the Purchase Order (the "Term"), unless sooner terminated as set forth herein. RTI may terminate this Purchase Order at any time and for any reason upon prior written notice to Vendor. Upon receipt of such notification, Vendor shall cease work and refrain from incurring further charges, and RTI shall have no further obligation to Vendor except to pay for Services performed and Deliverables provided prior to notice of termination. If requested, Vendor shall perform any Services specified in the notice and these Terms shall continue to govern.

If Vendor is in default of these Terms and such default continues for more than five (5) days after written notice thereof is given to the Vendor, then RTI shall be entitled to immediately terminate this Purchase Order and seek any other remedy available at law or in equity.

## 6. Additional Obligations and Warranties of Vendor

- a. **Research Involving Human Subjects.** If the Services involve research with human subjects, or if otherwise applicable to the Services to be performed, Vendor shall obtain approval or exemption by an Institutional Review Board or Ethics Committee prior to Vendor engaging with human subjects, unless RTI notifies Vendor that it will obtain such approval or exemption.
- b. **Personally Identifiable Data.** Vendor agrees that it shall not provide to RTI any personally identifiable data for any person who is a study subject. All data and Results, defined in Section 11, submitted to RTI by Vendor shall be in non-identifiable or aggregate form as set forth in the Purchase Order.
- c. **Debarment.** Vendor warrants that:
  - i. Neither the Vendor nor any person employed or subcontracted or otherwise engaged by Vendor to perform any of the Services or furnish the Deliverables:
    - a. is or has been debarred, excluded or convicted of any offense by the U.S. Food and Drug Administration or the U.S. Department of Health and Human Services or similar counterpart agency in any country (e.g. EMA in the EU, MHRA in the UK, Pmda in Japan, TGA in Australia, etc.); or
    - b. is or has been prohibited by law or regulation from performing services on behalf of a pharmaceutical or biotechnology entity by a regulatory agency or any government entity having jurisdiction over the Vendor and its business operations
  - ii. It shall immediately notify RTI if it becomes aware of the actual or potential debarment, suspension, exclusion, sanction, or ineligibility of any Vendor employees or any third-party persons or subcontractors engaged by Vendor who are supporting the provision of Deliverables under this Purchase Order.
- d. **Regulatory:** Vendor shall comply with all applicable statutes, regulations, administrative requirements and industry guidelines, as amended, governing the Services, including but not limited to:
  - i. anti-corruption and anti-bribery legislation such as the U.S. Foreign Corrupt Practices Act ("FCPA"), the UK Anti Bribery Act or other similar laws;
  - ii. data privacy and security regulations concerning the handling of personal data, including the U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996, the EU General Data Protection Regulation (Regulation (EU) 2016/679) and any other local privacy or data protection regulations, as applicable;
  - iii. legislation and industry guidelines regarding research protection of human subjects; and
  - iv. applicable export control regulations, anti-trafficking laws, and employment laws.
- e. **No Conflicts of Interest.** Vendor warrants that Vendor and its personnel do not have and shall remain free from any commitments or conflicts of interest that could diminish Vendor's ability to comply with these Terms or provide the Deliverables in an independent and unbiased manner.
- f. **Data Security.** If Vendor utilizes data processing systems in the performance of the Services pursuant to this Agreement:
  - i. Vendor shall develop, implement, maintain and monitor a comprehensive, written privacy and information security program applicable to all employees, facilities, systems, devices and media that process or contain data collected or processed in the performance of the Services. The information security program will provide for administrative, technical, organizational and physical safeguards that are: (a) designed to protect against reasonably anticipated threats to the security, confidentiality, availability or integrity of the data; and (b) consistent with the requirements of applicable data protection laws and prevailing industry practices. Such safeguards will include access controls, password protections, firewalls and anti-virus and malware protections to protect data, and periodic risk assessments to identify reasonably foreseeable threats to the data. The information security program will include both disaster recovery and data breach response plans.

- ii. Vendor warrants that it shall not implement a material change to its data processing systems that are used in the performance of the Services without prior notice to RTI; nor will it implement a change to its information security program that materially lowers or lessens the safeguards in place at the time of execution of this Agreement.
- iii. Vendor shall encrypt any Personal Data using industry standard encryption tools, whether in transit or at rest. "Personal Data" means any information that identifies an individual, or taken with other information in the possession of Subcontractor or its vendors or agents can be used to identify an individual.
  - a. If Vendor creates web interfaces as part of the Services, those shall be HTTPS TLS 1.2 or higher, and data in transit other than via TLS shall be encrypted with Secure FTP or an add-on tool using at least AES-256 encryption.
  - b. If Vendor is processing Personal Data originating in the EU or UK or concerning EU or UK residents, then the Data Processing Addendum, which is attached hereto as Appendix B and incorporated by reference, shall apply.
- iv. Vendor shall ensure the proper disposal of project data, particularly Personal Data at completion of the project and in accordance with RTI's direction. If Vendor disposes of any paper or electronic record or any media containing Personal Data, Vendor shall take all reasonable steps to destroy the information by (a) shredding; (b) permanently erasing and deleting; (c) degaussing; or (d) otherwise making it unreadable and indecipherable. Destruction of electronic data shall be done in compliance with industry standards for destruction of sensitive data, e.g. NIST 800-88. Documentation of destruction must be provided to RTI within three (3) business days of destruction of the data. Questions or additional guidance on this requirement may be directed to [dataprotection@rtihs.org](mailto:dataprotection@rtihs.org).
- v. Vendor shall notify RTI in writing at [dataprotection@rtihs.org](mailto:dataprotection@rtihs.org) if Vendor reasonably believes that there has been a data security breach involving any data that is subject of the Services, whether involving Vendor's facilities, systems or equipment or those of a third-party Vendor, and shall provide detailed information regarding the nature and scope of the breach, its actual or potential cause, and the measures being taken by Vendor to investigate, correct or mitigate the breach and prevent future breaches. Such notification shall be given no later than twenty-four (24) hours after Vendor's discovery of the breach.
- vi. Vendor shall provide, at its sole cost, reasonable assistance and cooperation requested by RTI to correct, remediate, or investigate any data security breach and mitigate any damage, including any notification that RTI may determine appropriate to send to regulators or to individuals actually or potentially affected by the Data Security Breach.
- vii. Vendor shall ensure that all employees, agents, suppliers, and subcontractors, including cloud service vendors, of Subcontractor who process or otherwise access project data comply with the data security requirements of this Section 6f and Appendix A, if applicable.
- g. The obligations and warranties of this Section 6 are continuing in nature, and Vendor shall advise RTI immediately should any facts or circumstances change affecting their accuracy or completeness.

## 7. Insurance

- a. Vendor shall maintain professional liability insurance coverage throughout the Term of this Purchase Order and thereafter as needed to cover its performance under this PO in an amount sufficient to cover the obligations or liabilities that could arise pursuant to these Terms with insurance companies having an A.M. Best or S&P ratings of at least A VII, and in addition the coverages listed below:
  - i. Worker's compensation and employer's liability insurance as required by local law;
  - ii. Commercial general liability insurance covering claims for damages arising out of any negligent act or omission of the Vendor or of any of its employees, agents, or third-party Vendors, with \$1,000,000 combined single limits;
  - iii. Where applicable due to the nature of the Services, professional Errors & Omissions (E&O) insurance
  - iv. Where applicable due to the nature of the Services, Cyber Insurance to cover costs associated with data breaches or violations of data protection laws when the Vendor will obtain or hold data subject to legal protections.
- b. Vendor shall provide to RTI, upon request, a copy of its certificate of insurance.

## 8. Confidentiality

- a. During the Term of this Purchase Order, one Party ("Recipient") may receive or have access to Confidential Information of the other Party ("Discloser"). "Confidential Information" means all non-public scientific, technical, financial or business information disclosed by or on behalf of Discloser to the Recipient including but not limited to: (a) information

about Discloser's products, customers, partners, and business operations and strategies; (b) materials, developments, records, scientific data and information including but not limited to any Personal Data collected from or about an individual; and (c) financial information including pricing information, forecasts, and personnel information; (d) the existence of this Purchase Order or nature of the Deliverables. For the avoidance of doubt, all work product arising from the performance of Services are the Confidential Information of RTI or its client.

- b. Confidential Information shall remain the sole property of Discloser and may only be used by the Recipient to perform its obligations hereunder. Recipient may disseminate Discloser's Confidential Information within its own organization only on a "need-to-know" basis and solely for the purpose of carrying out its obligations hereunder. Recipient shall not disclose Confidential Information of Discloser to a third party for any reason without the prior written consent of Discloser. These obligations shall not apply to Confidential Information which:
  - i. is generally available to the public other than because of an improper disclosure by the Recipient;
  - ii. becomes available to the Recipient from a third-party which is not legally prohibited from disclosing such information;
  - iii. the Recipient develops independently without use of the Discloser's Confidential Information, as demonstrated by pre-existing written records or other evidence;
  - iv. was in the Recipient's possession or known to it prior to receipt from Discloser; or
  - v. is required by a competent authority to be disclosed, provided that Recipient promptly notifies Discloser of the request, gives Discloser an opportunity to seek a protective order, and limits any such disclosure to the minimum required by law.
- c. Recipient shall maintain the Confidential Information using no less than a reasonable standard of care.
- d. All RTI Confidential Information and all copies thereof shall be returned by Vendor to RTI upon the earlier of i) RTI's request; or ii) immediately upon the termination or expiration of this Purchase Order. If RTI Confidential Information cannot be returned, Vendor shall destroy and shall certify such destruction in writing to RTI within ten (10) days of the termination or expiration of the Purchase Order; provided, however, that subject to all confidentiality and data security obligations in this Purchase Order, Vendor shall be permitted to keep one (1) copy of the Confidential Information, except for Personal Data, for purposes of internal audit and to demonstrate compliance with this Purchase Order.
- e. Vendor shall ensure it has adequate measures in place to protect Confidential Information in accordance with all applicable laws and standards.
- f. The obligations of confidentiality, non-use and non-disclosure shall remain in effect indefinitely after the termination or expiration of this Purchase Order.
- g. This Section 8 shall apply in addition to the terms of any Confidential Disclosure Agreement ("CDA") previously executed between the Parties. In the event of a conflict between this Section and the CDA, the terms of this Purchase Order control.

## **9. Publicity**

Vendor shall not, without RTI's prior written approval, use or disclose the names or marks of "RTI", "RTI Health Solutions" or "RTI International", or RTI's client's name or marks, or any variation thereof, in any advertising, sales promotion, press release, or any other form of publicity.

## **10. Publication**

Vendor shall refrain from publishing or otherwise disseminating any information resulting from any Services except with prior written consent of RTI.

## **11. Ownership of Results and Background Rights.**

All Deliverables specified in this Purchase Order will be the sole and exclusive property of RTI or its designee; provided however, Vendor Methods, defined below, shall remain the property of the Vendor. Vendor and all individuals performing hereunder hereby assign and transfer to RTI all right, title and interest to the Deliverables without additional consideration. All Services performed and all Deliverables arising therefrom shall be deemed a "work made for hire" under the copyright laws of the United States and any items not subject to such designation shall be the property of RTI without restriction of any kind.

Vendor shall retain ownership of any data, materials, tools, methodologies, technologies, intellectual property, and Confidential Information which: i) existed prior to this Purchase Order; or ii) was created other than through provision of the Deliverables and without use of any Confidential Information of RTI or its client (collectively, "Vendor Methods"). To the extent that any Vendor Methods are included in the Deliverables, Vendor grants to RTI a world-wide, fully paid, royalty-free, non-exclusive license to freely use such Vendor Methods and RTI shall be entitled to sub-license such Vendor Methods to its client or client's affiliates. Vendor shall promptly notify RTI if any Vendor Methods are included in the Deliverables.

## 12. Materials

All materials ("RTI Materials") supplied by RTI to Vendor, shall remain the property and Confidential Information of RTI or its client. Such RTI Materials may only be used by Vendor for the express purpose of providing the Services and/or Deliverables and no other use or disclosure of RTI Materials is authorized or permitted by these Terms. All RTI Materials and all copies thereof shall be returned to RTI upon the earlier of (a) RTI's request or (b) immediately upon the termination or expiration of this Purchase Order. If the RTI Materials cannot be returned, Vendor shall destroy and shall certify such destruction in writing to RTI within ten (10) days of the termination or expiration of this Purchase Order.

## 13. Indemnification

Vendor shall indemnify and hold harmless RTI and its directors, officers and employees ("Indemnities") against any third-party claims for loss, damage or expense, including reasonable attorney's fees and costs ("Claims"), arising out of the Vendor's negligence, willful misconduct, or violation of its statutory, contractual or other obligations.

In addition, Vendor specifically agrees to indemnify RTI against any Claim which alleges infringement of intellectual property rights of any item furnished by Vendor to RTI. Vendor, at no expense to RTI, shall obtain for RTI the unrestricted right to use such item or shall substitute an equivalent item reasonably acceptable to RTI.

RTI will promptly notify Vendor of any Claim for which it believes indemnification is due. Vendor shall not enter into any settlement agreement or other voluntary resolution of any Claim without the written consent of RTI, which shall not be unreasonably withheld or delayed.

## 14. Non-Assignment

- a. Any assignment of rights or delegation of duties or obligations set forth in these Terms made by Vendor without RTI's prior written consent is void. No assignment or delegation made with RTI's consent shall relieve Vendor of its obligations hereunder.
- b. RTI shall be entitled to assign this Purchase Order to any successor to RTI's business without prior notice to or consent from Vendor. Any other assignment by RTI shall require consent of the Vendor.

## 15. Electronic Contracting

This Purchase Order may be executed in multiple counterparts. An electronic signature shall be deemed valid in the same manner as an original signature.

## 16. Dispute Resolution

- a. In the event of a dispute arising out of the provision of the Deliverables or these Terms, the Parties shall use best efforts to mutually agree upon a resolution. Pending resolution, Vendor shall proceed diligently with the performance of its obligations in this Purchase Order.
- b. If the Parties are unable to agree upon a resolution of a dispute, then at the election of either Party, they may settle such dispute by mediation, or by arbitration in accordance with the Rules of the American Arbitration Association in the city of Raleigh, North Carolina, USA.

## 17. Governing Law

These Terms shall be governed by and construed in accordance with the laws of the State of North Carolina. All claims, controversies and causes of action arising out of or relating to these Terms whether sounding in contract, tort or statute, shall be governed by the laws of the State of North Carolina, including its statutes of limitations, without giving effect to any conflict of laws rules that would result in the application of the laws of a different jurisdiction.

## 18. Miscellaneous

- a. **No Waiver.** The failure of either Party to enforce a provision of these Terms will not be deemed a waiver of the right to enforce that or any other Term. A valid waiver shall be evidenced in writing and signed by an authorized representative of the waiving Party.
- b. **Modification.** Any modification of this Purchase Order will be authorized by RTI using a signed Purchase Order modification to be acknowledged or signed by Vendor.
- c. **Survival.** The following Sections shall survive the termination of these Terms: 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 16, 17 and 18.
- d. **Force Majeure.** The delay or failure of a Party to carry out its duties hereunder will be excused if the delay or failure is from unforeseen causes beyond the reasonable control of the Party, so long as the Party claiming relief notifies the

other of the circumstances, provides an estimate of the impact on its performance, and takes all reasonable steps to promptly resume performance. Either Party may terminate this Purchase Order if it or the other Party experiences a Force Majeure event that exceeds sixty (60) days.

**19. If Vendor is located in Spain, then the following paragraph shall apply.**

In accordance with current regulations on the protection of personal information, RTI hereby informs Vendor that the personal information that may be obtained concerning the individuals working on this Study or who are subcontracted by Vendor to work on this Purchase Order ("Vendor Representatives") is included in files owned by Research Triangle Institute and used to properly manage this contractual relationship, as well as the communication related to this Purchase Order.

The legal basis for the use of Vendor Representatives information is the maintenance of the commercial and administrative relationship with RTI, in addition to consent in cases when legally required.

Vendor Representative information will be retained in our files during our relationship and for up to three years thereafter (in view of future collaborations) and will not be transferred to third parties (in the absence of a legal obligation) without Vendor Representatives' prior consent. RTI shall maintain confidentiality with respect to the processing of Vendor Representatives' personal information and adherence with the security measures which are stipulated by current regulations. Automated decisions based on Vendors Representatives' personal data will not be made.

Vendor shall ensure that the owner of the personal information specifically authorizes that their personal information may be communicated to the RTI headquarters in the USA for internal administrative purposes (Research Triangle Park, North Carolina 27709, US Employer Tax ID No. 56-0686338) or to other locations of RTI and to RTI's third-party service providers as necessary to fulfill their contractual obligations to RTI.

To exercise the rights of access, rectification, deletion, and portability of your information, and the limitation or opposition to its processing as provided for by law, the owner of the information can, in writing, contact RTI, Ref. Protección de datos [Ref. Data protection], Av. Diagonal 605, 9-1, 08028 Barcelona, or send an email to [dataprotection@rtihs.org](mailto:dataprotection@rtihs.org).

**20. If Vendor is located in an EU or EEA country other than Spain, or Switzerland, then the following paragraph shall apply.**

In accordance with current regulations on the protection of personal information, RTI hereby informs Vendor that the personal information that may be obtained concerning the individuals working on this Study or who are subcontracted by Vendor to work on this Purchase Order ("Vendor Representatives") is included in files owned by Research Triangle Institute and used to properly manage this contractual relationship, as well as the communication related to this Purchase Order.

The legal basis for the use of Vendor Representatives' information is the maintenance of the commercial and administrative relationship with RTI, in addition to consent in cases when legally required.

Vendor Representative information will be retained in our files during our relationship and for up to three years thereafter (in view of future collaborations) and will not be transferred to third parties (in the absence of a legal obligation) without Vendor Representatives' prior consent. RTI shall maintain confidentiality with respect to the processing of Vendor Representatives' personal information and adherence with the security measures which are stipulated by current regulations. Automated decisions based on Subcontractor Representatives' personal data will not be made.

Vendor shall ensure that the owner of the personal information specifically authorizes that their personal information may be communicated to the RTI headquarters in the USA for internal administrative purposes (Research Triangle Park, North Carolina 27709, US Employer Tax ID No. 56-0686338) or to other locations of RTI and to RTI's third-party service providers as necessary to fulfill their contractual obligations to RTI.

## Appendix A DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "**Addendum**") shall be applicable when Subcontractor processes Personal Data as defined in GDPR Article 4(1) ("**Personal Data**") or as defined in the UK Data Protection Act, as applicable, in the course of performing Services pursuant to the Subcontract. "**GDPR**" means EU Regulation 2016/679 of 27 April 2016 (the General Data Protection Regulation).

RTI-HS has or may conducted a qualification of the Subcontractor as set out in Article 28(1) of the GDPR.

1. The Personal Data to be processed by the Subcontractor includes the categories of data, the categories of data subjects, and the nature and purpose of the processing as set forth in the Subcontract.
2. The Subcontractor shall only process Personal Data:
  - a. in accordance with this Data Processing Addendum;
  - b. on written instructions from the RTI-HS; and
  - c. for the purpose of providing the data processing services described in the Subcontract.
3. The Subcontractor shall ensure compliance with this Addendum by its employees and all other authorized persons, including any pre-approved third-party subcontractors or subprocessors.
4. The Subcontractor shall immediately notify the RTI-HS in writing if it considers an instruction from the RTI-HS to be in violation of the GDPR, or other European Union or Member State data protection provisions (collectively, the "**Data Protection Legislation**").
5. The country(ies) in which the Subcontractor will process the Personal Data is set forth in the Subcontract. The Subcontractor shall not transfer Personal Data to third countries, nor make any onward transfer of the Personal Data to a location outside the EU/EEA, nor permit access to the data remotely from a location outside the EU/EEA, without the prior written approval of the RTI-HS.
6. The Subcontractor shall implement appropriate technical and organizational security measures ("**Security Safeguards**") to prevent accidental, unauthorized or unlawful destruction, loss, modification, access, loss of access or control, or disclosure of the Personal Data.
  - a. Appropriate technical and organizational security measures shall be identified with due regard to the nature of the Personal Data and risks to Data Subjects which may arise as a result of Subcontractor's possession, processing or transfer of the Personal Data.
  - b. Appropriate technical and organizational security measures may include, but not be limited to:
    - i. Use of current anti-virus or other software and an updated firewall to protect IT systems and Personal Data from unauthorized network access and malicious code.
    - ii. Encryption of wireless networks including a comprehensive access code.
    - iii. Mitigation of security vulnerabilities with current software and patches.
    - iv. Use of logon restrictions, passwords, locks, and role-based access to computers, mobile devices, data storage media and printed copies containing Personal Data.
    - v. Use of password change procedures, including requiring strong passwords and periodic updates.
    - vi. Use of safe disposal procedures for computers, mobile devices, data storage media (including printed copies) containing Personal Data.
    - vii. Use of pseudonymization and encryption of Personal Data when in transit or at rest.
    - viii. Use of encryption for transmission of Personal Data over public networks.
    - ix. Storage of backups of Personal Data either in a secure off-site facility or in a fire and water-proof container.
    - x. Ensuring the ability to restore the availability and access to Personal Data and access audit logs in a timely manner.
    - xi. Regular testing and assessment of the effectiveness of the technical and organizational security measures, including network penetration testing, documented for review as requested by RTI-HS or its clients.
    - xii. Employee training on the security measures, including on how to recognize a Personal Data Breach or other security incident, and how to respond appropriately.

- xiii. Maintenance of current documentation of appropriate technical and organizational security measures and staff training.
  - xiv. System logging of failed login attempts and blocking access after a certain number of failed login attempts.
  - xv. Maintain a system log of user activities, including log of time, user, search, search criteria, access, modification, close, print, export, erasure/delete, etc. and automated erasure of log after a certain time interval.
  - xvi. Perform background checks, if permitted by applicable law, on new employees or any approved subcontractors serving in key positions processing Personal Data.
7. The Subcontractor shall immediately notify RTI-HS at [dataprotection@rtihs.org](mailto:dataprotection@rtihs.org) of (i) any Personal Data Breach (defined below); or (ii) any vulnerability in the Security Safeguards which present a material risk of compromising the confidentiality, integrity or security of the Personal Data; or (iii) any violation of applicable law related to the processing of Personal Data (collectively, a "**Security Incident**").
    - a. In the event that RTI-HS deems it necessary to provide notification of the Security Incident to government authorities, Subcontractor shall reimburse RTI-HS for all reasonable costs associated with such notification, including any mitigation efforts that are required, unless Subcontractor can demonstrate that the Security Incident was caused by RTI-HS's negligence or willful misconduct.
  8. The Subcontractor shall maintain a written record of all categories of processing activities carried out on behalf of the RTI-HS, which shall contain all information necessary to demonstrate compliance with Article 30 of the GDPR and this Addendum.
  9. The Subcontractor shall cooperate with RTI-HS in cases of inquiries and inspections conducted by the responsible supervisory authority, or by clients of RTI-HS.
  10. The Subcontractor shall permit audits and inspections by either RTI-HS or its designee, if reasonable notice is provided by the RTI-HS.
    - a. The Subcontractor shall provide RTI-HS or its designee with sufficient information to enable RTI-HS to verify the Subcontractor's compliance with the obligations in Article 28 of the GDPR and this Data Processing Addendum.
  11. The Subcontractor shall immediately notify RTI-HS in writing about:
    - a. any request for disclosure of Personal Data processed under this Addendum by data protection authorities or any other public or government authority, unless such notice is expressly prohibited by law; and
    - b. any request it receives from a data subject regarding exercising of the data subject's rights under applicable Data Protection Legislation, including requests to amend, correct, access, transfer, block or delete Personal Data.
      - i. The Subcontractor shall promptly assist RTI-HS and comply with RTI-HS's reasonable instructions in the handling of any such requests from data subjects.
  12. The Subcontractor shall assist RTI-HS in ensuring compliance with the obligations of Articles 32 to 36 of the GDPR with regard to Security Safeguards, notification of supervisory authorities, notification of individuals, preparation of data protection impact assessments and prior consultation with supervisory authorities.
  13. The Subcontractor shall not engage another subcontractor for the processing of Personal Data without prior written approval of the RTI-HS.
    - a. The Subcontractor warrants that all subcontractors that will be used in the performance of the Services have been identified in the Subcontract.
    - b. The Subcontractor agrees that RTI-HS is entitled to withdraw its approval of the use of a subcontractor in its sole discretion.
    - c. The Subcontractor must inform RTI-HS in writing of any discontinued use of a subcontractor unless such discontinuance is planned as part of the activities described in the Subcontract.
    - d. Prior to engaging a subcontractor to carry out activities covered by this Addendum, the Subcontractor shall ensure that a pre-audit as set out in GDPR Article 28(1) is completed and enter into a written data processing agreement with the subcontractor (hereinafter the "**Lower Tier Subcontractor Agreement**"), having at least the same obligations on the subcontractor as those set out in this Addendum.
    - e. RTI-HS has the right to receive documentation relating to pre-audit of any subcontractor and a copy of the Lower Tier Subcontractor Agreement upon request.



- f. The use of any subcontractor by the Subcontractor shall not relieve or release the Subcontractor from any of its obligations under this Addendum and the Subcontractor shall remain fully liable for the performance of any subcontractor's obligations.

14. **CONFIDENTIALITY.** With respect to Confidential Information that is Personal Data, the Subcontractor, including its personnel and any subcontractors or other authorized persons, shall, in addition to all other confidentiality obligations in the Subcontract, comply with the following:

- a. The Subcontractor shall inform RTI-HS at [dataprotection@rtihs.org](mailto:dataprotection@rtihs.org) within 24 hours after learning of any security breach which results in the accidental, unauthorized or unlawful destruction, loss, modification, access, loss of access or control, or disclosure of Personal Data transmitted, stored or otherwise processed under this Addendum ("**Personal Data Breach**").
- b. The Subcontractor shall provide RTI-HS with all information necessary for RTI-HS to comply with its obligations pursuant to the Data Protection Legislation, including:
  - i. a description of the nature of the Personal Data Breach,
  - ii. the categories and approximate number of data subjects concerned,
  - iii. the categories and approximate number of personal data records concerned, and
  - iv. information about any initiatives to safeguard against future Personal Data Breaches.
- c. The Subcontractor shall indemnify and hold harmless RTI-HS against all claims and proceedings and all liability, loss, fines, costs and expenses incurred by RTI-HS as a result of violation of this Addendum (or the Data Protection Legislation) by the Subcontractor, its employees, subcontractors or other authorized persons in the course of the Subcontractor's processing of Personal Data under this Addendum.

- 15. Should any provision of this Addendum be held to be unenforceable, illegal or invalid by a competent authority, such provision may, through negotiation of the parties, be replaced by provisions that to the widest extent possible gives effect to the intent of the original provisions. If that is not possible, such term or provision shall be deemed not to form part of this Addendum. All other terms and conditions of this Addendum shall remain in full force and effect. The obligations of this Data Protection Addendum shall survive termination of the Subcontract indefinitely.
- 16. Upon completion of the Services relating to processing of Personal Data, the Subcontractor shall promptly obtain direction from RTI-HS and then immediately, per such instruction, (i) delete all the Personal Data; or (ii) return all Personal Data to RTI-HS (or another Subcontractor if so requested by RTI-HS); provided, however, that the Subcontractor shall be entitled to retain a copy of the Personal Data only to the extent required by law. If the Subcontractor is obligated to retain Personal Data to comply with applicable legislation in third countries, the Subcontractor must notify RTI-HS thereof, including the legal basis for continued storage.
- 17. If any provisions of this Addendum conflict with the provisions of the Subcontract or any other agreement between the Parties, then the provisions of this Addendum shall supersede such conflicting provisions as to the matters addressed in this Addendum.