

## RFP 6325 Z1 ATTACHMENT C

### DATA USE AGREEMENT (DUA) PROVISIONS

#### 1. PURPOSE; APPLICABILITY; ORDER OF PRECEDENCE

- 1.1. The purpose of this DUA is to facilitate access to, creation, receipt, maintenance, use, disclosure or transmission of Confidential Information with Contractor, and set forth Contractor's rights and obligations with respect to the Confidential Information and the limited purposes for which the Contractor may create, receive, maintain, use, disclose or have access to Confidential Information. This DUA includes, but is not limited to, taking any Confidential Information outside of any DHHS systems provided for data use, as well as the creation of any new data being used outside those systems. This DUA also describes DHHS's remedies in the event of Contractor's noncompliance with its obligations under this DUA. This DUA applies to both DHHS business associates, with "business associate" defined in the Health Insurance Portability and Accountability Act (HIPAA) (see Business Associate Provisions, Request for Proposal – Attachment A), as well as Contractors who are not business associates, who create, receive, maintain, use, disclose or have access to Confidential Information on behalf of DHHS, its programs or clients as described in the Contract. As a best practice, DHHS requires its contractors to comply with the terms of this DUA to safeguard all types of Confidential Information.
- 1.2. If any provision of the Contract conflicts with this DUA, this DUA controls.

#### 2. DEFINITIONS

For the purposes of this DUA, capitalized terms have the following meanings:

- 2.1. "Authorized Purpose" means the specific purpose or purposes described in the Contract for Contractor to fulfill its obligations under the Contract, or any other purpose expressly authorized by DHHS, in writing, in advance.
- 2.2. "Authorized User" means a person:
  - 2.2.1. Who is authorized to create, receive, maintain, access, process, view, handle, examine, interpret, or analyze Confidential Information pursuant to this DUA;
  - 2.2.2. Who has a demonstrable need to create, receive, maintain, use, disclose or have access to the Confidential Information; and
  - 2.2.3. Who has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information as required by this DUA.
- 2.3. "Breach" means an impermissible use or disclosure of electronic or non-electronic sensitive personal information by an unauthorized person or for an unauthorized purpose that compromises the security or privacy of Confidential Information such that the use or disclosure poses a risk of reputational harm, theft of financial information, identity theft, or medical identity theft. Any acquisition, access, use, disclosure or loss of Confidential Information other than as permitted by this DUA shall be presumed to be a Breach unless Contractor demonstrates, based on a risk assessment, that there is a low probability that the Confidential Information has been compromised.
- 2.4. "Confidential Information" means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to Contractor or that Contractor may create, receive, maintain, use, disclose or have access to on behalf of DHHS in connection with the Contract, which consists of or includes any or all of the following:
  - 2.4.1. Education records as defined in the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g; 34 C.F.R. Part 99
  - 2.4.2. Federal Tax Information as defined in Internal Revenue Code § 6103 and Internal Revenue Service Publication 1075;

- 2.4.3. Protected Health Information (PHI) in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information as defined in 45 C.F.R. §160.103;
- 2.4.4. Personally Identifiable Information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
- 2.4.5. Social Security Administration Data, including, without limitation, Medicaid information means disclosures of information made by the Social Security Administration or the Centers for Medicare and Medicaid Services from a federal system of records for administration of federally funded benefit programs under the Social Security Act, 42 U.S.C., Chapter 7;
- 2.4.6. Medicaid Client refers to:
- A Medicaid applicant;
  - A Medicaid member;
  - A person who is conditionally eligible for Medicaid; or
  - A person whose income or assets are considered in determining eligibility for an applicant or member
- 2.4.7. Personal Information as defined by Neb. Rev. Stat. § 87-802;
- 2.4.8. Information or records contained in Neb. Rev. Stat. § 84-712.05;
- 2.4.9. All privileged work product;
- 2.4.10. All other information designated as confidential under the constitution and laws of the State of Nebraska and of the United States
- 2.5. "Contract" includes, collectively, the Request for Proposal (or Request for Qualifications, as applicable), the Contractor's proposal, as well as any addenda, appendices, and attachments;
- 2.6. "Destroy" or "Destruction", for Confidential Information, means:
- 2.6.1. Paper, film, or other hard copy media have been shredded or destroyed such that the Confidential Information cannot be read or otherwise reconstructed. Redaction is specifically excluded as a means of data destruction.
- 2.6.2. Electronic media have been cleared, purged, or destroyed consistent with National Institute of Standards and Technology (NIST) Special Publication 800-88, "Guidelines for Media Sanitization," such that the Confidential Information cannot be retrieved.
- 2.7. "Discover" or "Discovery" means the first day on which a Breach becomes known to Contractor, or, by exercising reasonable diligence would have been known to Contractor.
- 2.8. "Legally Authorized Representative" of an individual means any individual as defined in 42 CFR 435.923 (authorized representative), or any individual legally authorized to act on behalf of another individual under Nebraska law;
- 2.9. "Required by Law" means a mandate contained in law that compels an entity to use or disclose Confidential Information that is enforceable in a court of law and is consistent with 42 CFR Part 431, Subpart F, including court orders, warrants, subpoenas or investigative demands.
- 2.10. "Subcontractor" means a person who contracts with a prime contractor to work, to supply commodities, or to contribute toward completing work for a governmental entity.
- 2.11. "Workforce" means employees, volunteers, trainees or other persons whose performance of work is under the direct control of a party, whether they are paid by that party.

### **3. CONTRACTOR'S DUTIES REGARDING CONFIDENTIAL INFORMATION**

- 3.1. *With respect to **PHI**, Contractor shall:*
- 3.1.1. Make PHI available if requested by DHHS, if Contractor maintains PHI, as defined in HIPAA.
- 3.1.2. Provide to DHHS data aggregation services related to the healthcare operations Contractor performs for DHHS pursuant to the Contract, if requested by DHHS, if Contractor provides data aggregation services as defined in HIPAA.

- 3.1.3. Provide access to PHI to an individual who is requesting his or her own PHI, or such individual's Legally Authorized Representative, in compliance with the requirements of HIPAA.
  - 3.1.4. Make PHI available to DHHS for amendment, and incorporate any amendments to PHI that DHHS directs, in compliance with HIPAA.
  - 3.1.5. Document and make available to DHHS, an accounting of use and disclosures in compliance with the requirements of HIPAA.
  - 3.1.6. If Contractor receives a request for access, amendment or accounting of PHI by any individual, promptly forward the request to DHHS or, if forwarding the request would violate HIPAA, promptly notify DHHS of the request and of Contractor's response. DHHS will respond to all such requests, unless Contractor is Required by Law to respond or DHHS has given prior written consent for Contractor to respond to and account for all such requests.
- 3.2. *With respect to **ALL Confidential Information**, Contractor shall:*
- 3.2.1. Exercise reasonable care and no less than the same degree of care Contractor uses to protect its own confidential, proprietary and trade secret information to prevent Confidential Information from being used in a manner that is not expressly an Authorized Purpose or as Required by Law. Contractor must access, create, maintain, receive, use, disclose, transmit or Destroy Confidential Information in a secure fashion that protects against any reasonably anticipated threats or hazards to the security or integrity of such information or unauthorized uses.
  - 3.2.2. Establish, implement and maintain appropriate procedural, administrative, physical and technical safeguards (for the purpose of this paragraph, "Safeguards") to preserve and maintain the confidentiality, integrity, and availability of the Confidential Information, in accordance with applicable laws or regulations relating to Confidential Information, to prevent any unauthorized use or disclosure of Confidential Information as long as Contractor has such Confidential Information in its actual or constructive possession. DHHS must review and approve said Safeguards before actual or constructive possession of any Confidential Information. Contractor must also allow DHHS, or a third party designated by DHHS, to review the Safeguards, in the sole discretion of DHHS.
  - 3.2.3. Implement, update as necessary, and document privacy, security and Breach notice policies and procedures and an incident response plan to address a Breach, to comply with the privacy, security and breach notice requirements of this DUA prior to conducting work under the Contract. Contractor shall produce, within three business days of a request by DHHS, copies of its policies and procedures and records relating to the use or disclosure of Confidential Information.
  - 3.2.4. Obtain DHHS's prior written consent to disclose or allow access to any portion of the Confidential Information to any person, other than Authorized Users, Workforce or Subcontractors of Contractor, provided said Authorized Users, Workforce or Subcontractors have completed DHHS-specified training in confidentiality, privacy, security, and on the importance of promptly reporting any Breach to Contractor's management and as permitted in Section 3.1.3, above. All Authorized Users, Workforce or Subcontractors must execute, individually, an acknowledgement noting their obligations as regards Confidential Information, and referencing this DUA. Additional requirements set forth below pertaining to Subcontractors dictate further requirements before disclosure.
  - 3.2.5. Establish, implement and maintain appropriate sanctions against any member of its Workforce or Subcontractor who fails to comply with this DUA, the Contract or applicable law. Contractor must maintain evidence of sanctions and produce it to DHHS upon request.
  - 3.2.6. Obtain prior written approval of DHHS, to disclose or provide access to any Confidential Information on the basis that such act is Required by Law, so that DHHS may have the opportunity to object to the disclosure or access and seek appropriate relief.

- 3.2.7. Certify that its Authorized Users each have a demonstrated need to know and have access to Confidential Information solely to the minimum extent necessary to accomplish the Authorized Purpose and that each has agreed in writing to be bound by the disclosure and use limitations pertaining to the Confidential Information contained in this DUA. Contractor and any previously authorized Subcontractors shall maintain at all times an updated, complete, accurate list of Authorized Users and supply it to DHHS upon request.
- 3.2.8. Provide, and require Subcontractors and agents to provide, to DHHS periodic written confirmation of compliance with controls and the terms of this DUA.
- 3.2.9. Return to DHHS or Destroy, at DHHS's election and at Contractor's expense, all Confidential Information received from DHHS or created or maintained by Contractor or any of Contractor's agents or Subcontractors on DHHS's behalf upon the termination or expiration of this DUA, if reasonably feasible and permitted by law. Contractor shall certify in writing to DHHS that all such Confidential Information has been Destroyed or returned to DHHS, and that Contractor and its agents and Subcontractors have retained no copies thereof. Notwithstanding the foregoing, Contractor acknowledges and agrees that it may not Destroy any Confidential Information if federal or state law, or DHHS record retention policy or a litigation hold notice prohibits such Destruction. If such return or Destruction is not reasonably feasible, or is impermissible by law, Contractor shall immediately notify DHHS of the reasons such return or Destruction is not feasible, and agree to extend the protections of this DUA to the Confidential Information for as long as Contractor maintains such Confidential Information.
- 3.2.10. Comply with the current DHHS Acceptable Use Policy (AUP), and require each Subcontractor and Workforce member who has direct access to DHHS Information Resources, as defined in the AUP, to execute a DHHS Acceptable Use Agreement. See Section 3.2.14 bullet point labeled "DHHS Information Security Policies."
- 3.2.11. Only conduct secure transmissions of Confidential Information whether in paper, oral or electronic form. DHHS must approve the method of secure transmission before any Confidential Information is transmitted by Contractor. A secure transmission of electronic Confidential Information in motion includes secure File Transfer Protocol (SFTP) or encryption at an appropriate level as required by rule, regulation or law. Confidential Information at rest requires encryption unless there is adequate administrative, technical, and physical security as required by rule, regulation or law. All electronic data transfer and communications of Confidential Information shall be through secure systems. Contractor shall provide proof of system, media or device security and/or encryption to DHHS no later than 48 hours after DHHS's written request in response to a compliance investigation, audit, or the Discovery of a Breach. DHHS may also request production of proof of security at other times as necessary to satisfy state and federal monitoring requirements. De-identification of Confidential Information in accordance with HIPAA de-identification standards is deemed secure.
- 3.2.12. Designate and identify a person or persons, as Privacy Official and Information Security Official, each of whom is authorized to act on behalf of Contractor and is responsible for the development and implementation of the privacy and security requirements in this DUA. Contractor shall provide name and current address, phone number and e-mail address for such designated officials to DHHS upon execution of this DUA and prior to any change. Upon written notice from DHHS, Contractor shall promptly remove and replace such official(s) if such official(s) is/are not performing the required functions.
- 3.2.13. Make available to DHHS any information DHHS requires to fulfill DHHS's obligations to provide access to, or copies of, Confidential Information in accordance with applicable laws, regulations or demands of a regulatory authority relating to Confidential Information. Contractor shall provide such information in a time and manner reasonably agreed upon or as designated by the applicable law or regulatory authority.

3.2.14. Comply with the following laws and standards if applicable to the type of Confidential Information and Contractor's Authorized Purpose:

- The Privacy Act of 1974 (USC 552a);
- OMB Memorandum 17-12;
- 42 CFR Part 431, Subpart F;
- The Federal Information Security Management Act of 2002 (FISMA);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Internal Revenue Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies;
- NIST Special Publication 800-66 Revision 1 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule;
- NIST Special Publications 800-53 and 800-53A – Recommended Security Controls for Federal Information Systems and Organizations, as currently revised;
- NIST Special Publication 800-47 – Security Guide for Interconnecting Information Technology Systems;
- NIST Special Publication 800-88, Guidelines for Media Sanitization;
- NIST Special Publication 800-111, Guide to Storage of Encryption Technologies for End User Devices containing PHI;
- Nebraska Information Technology Commission, Chapter 8 – Information Security Policy, available at: <https://nitc.nebraska.gov/standards/index.html>;
- DHHS IT Policies available at the following link:  
[http://dhhs.ne.gov/Documents/Information%20Technology%20\(IT\)%20Security%20Policies%20and%20Standards.pdf](http://dhhs.ne.gov/Documents/Information%20Technology%20(IT)%20Security%20Policies%20and%20Standards.pdf)
- Family Educational Rights and Privacy Act; and
- Any other state or federal law, regulation, or administrative rule relating to the specific DHHS program area that Contractor supports on behalf of DHHS.

3.2.15. Be permitted to use or disclose Confidential Information, except Confidential Information about Medicaid Clients, for the proper management and administration of Contractor roles and responsibilities or to carry out Contractor's legal responsibilities, except as otherwise limited by this DUA, the Contract, or law applicable to the Confidential Information, if: (1) Disclosure is Required by Law; or (2) Contractor obtains reasonable assurances from the person to whom the information is disclose that the person shall:

- Maintain the confidentiality of the Confidential Information in accordance with this DUA;
- Use or further disclose the information only as Required by Law or for the Authorized Purpose for which it was disclosed to the person; and
- Notify Contractor in accordance with Section 4 of a Breach of Confidential Information that the person Discovers or should have Discovered with the exercise of reasonable diligence.

3.2.16. For Confidential Information about Medicaid Clients, DHHS must provide prior written approval to the Contractor before Contractor is permitted to use such information for the uses described immediately above.

3.3. *With respect to **ALL Confidential Information**, Contractor shall **NOT**:*

3.3.1. Attempt to re-identify or further identify Confidential Information that has been de-identified, or attempt to contact any persons whose records are contained in the Confidential Information, except for an Authorized Purpose, without express written authorization from DHHS.

3.3.2. Engage in marketing or sale of Confidential Information.

3.3.3. Permit, or enter into any agreement with a Subcontractor to, create, receive, maintain, use, disclose, have access to or transmit Confidential Information, on behalf of DHHS without requiring that Subcontractor first gain approval from DHHS and execute the Form Subcontractor Agreement, Appendix 1. Contractor is directly responsible for its Subcontractors' compliance with, and enforcement of, this DUA. If Subcontractor requires Medicaid Client information access, the Contractor shall specifically identify as such in its request to DHHS.

#### 4. BREACH NOTICE, REPORTING AND CORRECTION REQUIREMENTS

##### 4.1. Cooperation and Financial Responsibility

4.1.1. Contractor shall, at Contractor's expense, cooperate fully with DHHS in investigating, mitigating to the extent practicable, and issuing notifications as directed by DHHS, for any Breach of Confidential Information.

4.1.2. Contractor shall make Confidential Information in Contractor's possession available pursuant to the requirements of HIPAA or other applicable law upon a determination of a Breach.

4.1.3. Contractor's obligation begins at the Discovery of a Breach and continues as long as related activity continues, until all effects of the Breach are mitigated to DHHS's satisfaction (the "incident response period").

##### 4.2. Initial Breach Notice

4.2.1. For federal information obtained from a federal system of records, including Federal Tax Information and Social Security Administration Data (which includes Medicaid and other governmental benefit program Confidential Information), Contractor shall notify DHHS of the Breach within the first hour of Discovery. The Contract shall specify whether Confidential Information is obtained from a federal system of records. For all other types of Confidential Information, Contractor shall also notify DHHS of the Breach within the first hour of Discovery, or in a timeframe otherwise approved by DHHS in writing. Contractor shall initially report to DHHS's Privacy and Security Officers via email at:

- [DHHS.InformationSecurityOffice@nebraska.gov](mailto:DHHS.InformationSecurityOffice@nebraska.gov); and
- [DHHS.PrivacyOfficer@nebraska.gov](mailto:DHHS.PrivacyOfficer@nebraska.gov).

Notification shall also be provided via email to the DHHS Contract Manager.

4.2.2. Contractor shall report all information reasonably available to Contractor about the Breach. This shall include, but not necessarily be limited to:

- Date and time of the incident;
- Date and time the incident was discovered;
- Description of the incident and the data involved, including specific data elements, if known;
- Potential number of records involved; if unknown, provide an estimated range;
- Address where the incident occurred;
- Information technology involved (e.g., laptop, server, mainframe etc.)

4.2.3. Contractor shall provide contact information to DHHS for Contractor's single point of contact who will communicate with DHHS both on and off business hours during the incident response period.

4.3. *Third Business Day.* No later than 5 p.m. on the third business day after Discovery, or a time within which Discovery reasonably should have been made by Contractor of a Breach of Confidential Information, Contractor shall provide written notification to DHHS of all reasonably available information about the Breach, and Contractor's investigation, including, to the extent known to Contractor:

4.3.1. The date the Breach occurred;

4.3.2. The date of Contractor's and, if applicable, Subcontractor's Discovery;

- 4.3.3. A brief description of the Breach, including how it occurred and who is responsible (or hypotheses, if not yet determined);
  - 4.3.4. A brief description of Contractor's investigation and the status of the investigation;
  - 4.3.5. A description of the types and amount of Confidential Information involved;
  - 4.3.6. Identification of and number of all individuals reasonably believed to be affected, including first and last name of the individual(s) and if applicable, the Legally Authorized Representative, last known address, age, telephone number, and email address if it is a preferred contact method;
  - 4.3.7. Contractor's initial risk assessment of the Breach, demonstrating whether individual or other notices are required by applicable law or this DUA for DHHS approval, including an analysis of whether there is a low probability of compromise of the Confidential Information or whether any legal exceptions to notification apply;
  - 4.3.8. Contractor's recommendation for DHHS's approval as to the steps individuals and/or Contractor on behalf of individuals, should take to protect the individuals from potential harm, including Contractor's provision of notifications, credit protection, claims monitoring, and any specific protections for a Legally Authorized Representative to take on behalf of an individual with special capacity or circumstances;
  - 4.3.9. The steps Contractor has taken to mitigate the harm or potential harm caused (including without limitation the provision of sufficient resources to mitigate);
  - 4.3.10. The steps Contractor has taken, or will take, to prevent or reduce the likelihood of recurrence of a similar Breach;
  - 4.3.11. Identify, describe or estimate of the persons, Workforce, Subcontractor, or individuals and any law enforcement that may be involved in the Breach;
  - 4.3.12. A reasonable schedule for Contractor to provide regular updates regarding response to the Breach, but no less than every three (3) business days, or as otherwise directed by DHHS in writing, including information about risk estimations, reporting, notification, if any, mitigation, corrective action, root cause analysis and when such activities are expected to be completed; and
  - 4.3.13. Any reasonably available, pertinent information, documents or reports related to a Breach that DHHS requests following Discovery.
- 4.4. *Breach Notification to Individuals and Reporting to Authorities.*
- 4.4.1. DHHS may direct Contractor to provide Breach notification to individuals, regulators or third-parties, as specified by DHHS following a Breach.
  - 4.4.2. Contractor must comply with all applicable legal and regulatory requirements, including but not limited to those contained in the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, Neb. Rev. Stat. §§ 87-801 et seq., in the time, manner and content of any notification to individuals, regulators or third-parties, or any notice required by other state or federal authorities. Notice letters will be in Contractor's name and on Contractor's letterhead, unless otherwise directed by DHHS, and will contain contact information, including the name and title of Contractor's representative, an email address and a toll-free telephone number, for the individual to obtain additional information.
  - 4.4.3. Contractor shall provide DHHS with draft notifications for DHHS approval prior to distribution and copies of distributed and approved communications.
  - 4.4.4. Contractor shall have the burden of demonstrating to the satisfaction of DHHS that any required notification was timely made. If there are delays outside of Contractor's control, Contractor shall provide written documentation to DHHS of the reasons for the delay.
  - 4.4.5. If DHHS directs Contractor to provide notifications, DHHS shall, in the time and manner reasonably requested by Contractor, cooperate and assist with Contractor's information requests in order to make such notifications.

## **5. GENERAL PROVISIONS**

### *5.1. Ownership of Confidential Information*

5.1.1. Notwithstanding any other provision in the Contract, all data collected as a result of this project (including but not limited to all Confidential Information) shall be the property of DHHS.

### *5.2. DHHS Commitment and Obligations*

5.2.1. DHHS will not request Contractor to create, maintain, transmit, use or disclose PII/PHI in any manner that would not be permissible under applicable law if done by DHHS.

### *5.3. DHHS Right to Inspection*

5.3.1. At any time, upon reasonable notice to Contractor, or if DHHS determines that Contractor has violated this DUA, DHHS, directly or through its agent, will have the right to inspect the facilities, systems, books and records of Contractor to monitor compliance with this DUA. For purposes of this subsection, DHHS's agent(s) include, without limitation, the Office of Public Counsel, the Nebraska Attorney General's Office, the Nebraska Auditor of Public Accounts, outside consultants, legal counsel, or other designee.

### *5.4. Term; Termination of DUA; Survival*

5.4.1. This DUA will be effective on the date on which it was signed, and will terminate upon termination of the Contract and as set forth herein. If the Contract is extended, this DUA is extended to run concurrent with the Contract.

5.4.2. If DHHS determines that Contractor has violated a material term of this DUA, DHHS may, in its sole discretion:

- Exercise any of its rights, including but not limited to reports, access and inspection under this DUA and/or the Contract; or
- Require Contractor to submit to a corrective action plan, including a plan for monitoring and plan for reporting as DHHS may determine necessary to maintain compliance with this DUA; or
- Provide Contractor with a reasonable period to cure the violation as determined by DHHS; or
- Terminate the DUA and Contract immediately, and, if DHHS further determines, seek relief in a court of competent jurisdiction.
- Before exercising any of these options, DHHS will provide written notice to Contractor describing the violation and the action it intends to take.

5.4.3. If neither termination nor cure is feasible, DHHS shall report the violation to the applicable regulatory authorities.

5.4.4. The duties of Contractor or its Subcontractor under this DUA survive the expiration or termination of this DUA until all the Confidential Information is Destroyed or returned to DHHS, as required by this DUA.

### *5.5. Injunctive Relief*

5.5.1. Contractor acknowledges and agrees that DHHS may suffer irreparable injury if Contractor or its Subcontractor fails to comply with any of the terms of this DUA with respect to the Confidential Information or a provision of HIPAA or other laws or regulations applicable to Confidential Information.

5.5.2. Contractor further agrees that monetary damages may be inadequate to compensate DHHS for Contractor's or its Subcontractor's failure to comply. Accordingly, Contractor agrees that DHHS will, in addition to any other remedies available to it at law or in equity, be entitled to seek injunctive relief without posting a bond and without the necessity of demonstrating actual damages, to enforce the terms of this DUA.

### *5.6. Indemnification*

5.6.1. All of Contractor's duties and obligations regarding indemnification otherwise contained herein apply to the provisions contained in this DUA.



5.7. *Automatic Amendment and Interpretation*

5.7.1. Upon the effective date of any amendment or issuance of additional regulations to any law applicable to Confidential Information, this DUA will automatically be amended so that the obligations imposed on DHHS and/or Contractor remain in compliance with such requirements. Any ambiguity in this DUA will be resolved in favor of a meaning that permits DHHS and Contractor to comply with laws applicable to Confidential Information.

5.8. *Notices; Requests for Approval*

5.8.1. All notices and requests for approval related to this DUA must be directed to the DHHS Contract Manager.

**APPENDIX 1. SUBCONTRACTOR AGREEMENT FORM**

**RFP 6325 Z1**

The DUA between DHHS and Contractor establishes the permitted and required uses and disclosures of Confidential Information by Contractor. Contractor has received permissions by DHHS for operations purposes for Authorized Use, and has subcontracted with \_\_\_\_\_ (Subcontractor name) for performance of duties on behalf of Contractor, which are subject to the DUA. Subcontractor acknowledges, understands and agrees to be bound by the same terms and conditions applicable to Contractor under the DUA, incorporated by reference in this Agreement, with respect to DHHS Confidential Information. Contractor and Subcontractor agree that DHHS is a third-party beneficiary to applicable provisions of the subcontract.

DHHS has the right, but not the obligation, to review or approve the terms and conditions of the subcontract by virtue of this Subcontractor Agreement Form.

Contractor and Subcontractor assure DHHS that any Breach as defined by the DUA that Subcontractor Discovers shall be reported to DHHS by Contractor in the time, manner and content required by the DUA.

If Contractor knows or should have known in the exercise of reasonable diligence of a pattern of activity or practice by Subcontractor that constitutes a material breach or violation of the DUA or the Subcontractor's obligations, Contractor shall:

1. Take reasonable steps to cure the violation or end the violation, as applicable;
2. If the steps are unsuccessful, terminate the contract or arrangement with Subcontractor, if feasible;
3. Notify DHHS immediately upon Discovery of the pattern of activity or practice of Subcontractor that constitutes a material breach or violation of the DUA and keep DHHS reasonably and regularly informed about steps Contractor is taking to cure or end the violation or terminate Subcontractor's contract or arrangement.

This Subcontractor Agreement Form is executed by the parties in their capacities indicated below.

FOR CONTRACTOR:

FOR SUBCONTRACTOR:

\_\_\_\_\_

\_\_\_\_\_

Name  
Title  
Contractor Name

Name  
Title  
Subcontractor name

DATE: \_\_\_\_\_

DATE: \_\_\_\_\_