

## Attachment 3

Department of Health & Human Services



### BUSINESS ASSOCIATE AGREEMENT

**THIS BUSINESS ASSOCIATE AGREEMENT** is made and entered into this \_\_\_day of \_\_\_\_ Month, \_\_\_\_Year by and between the Nebraska Department of Health and Human Services also hereinafter referred to as “Covered Entity” and **Name of Business Associate Here**, hereinafter also referred to as “Business Associate”.

#### Preamble

THIS BUSINESS ASSOCIATE AGREEMENT (“Agreement”) constitutes a non-exclusive agreement between Covered Entity, and the Business Associate named above. The purpose of this Agreement is to authorize the Business Associate to use and disclose to specifically identified entities Protected Health Information as more fully described in this Agreement and in the attached Scope-of-Work.

The Covered Entity and Business Associate, have entered into this Agreement to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Final Privacy and Security Rule requirements for such an agreement.

The Covered Entity and Business Associate intend to protect and provide for the security of Protected Health Information disclosed to a Business Associate pursuant to the contract in compliance with HIPAA, the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (“the HITECH Act”), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (the “HIPAA Regulations”) and other applicable laws.

This Agreement also defines our duty to protect the confidentiality and integrity of Protected Health Information as required by the HIPAA regulations, Covered Entity policy, professional ethics, and accreditation requirements. Parties executing this Agreement understand that they mutually agree to comply with the provisions of the regulations implementing HIPAA.

The Covered Entity and the Business Associate may be parties to existing contracts that involve duties and obligations regulated by HIPAA and may enter into other such contracts in the future. This Agreement is intended to amend all such existing contracts and to be incorporated into all such future contracts between the parties.

The purpose of the Scope-of-Work Attachment is to identify specific requirements in such contracts for the safeguarding of Protected Health information and to identify any procedures necessary to the work performed on behalf of the Covered Entity by the Business Associate that is unique to its operation involving the use and disclosure of Protected Health Information.

**This Agreement will have, at a minimum, the following attachments:**

- Scope-of-Work Attachment;

**This Agreement may include the following attachments:**

- If this Agreement involves the use of Electronic Transactions regulated by HIPAA, 45 CFR Parts 160 and 162, then a Trading Partner Attachment must be included to facilitate the provision of billing, processing, collecting, modifying or transferring of Protected Health Information in agreed formats and to assure that such uses and disclosures comply with relevant laws, regulations and standards.
  - Other attachments as appropriate and mutually agreed between the parties.
- 

**NOW THEREFORE, the parties intending to be legally bound agree to the following General Conditions:**

**I. Definitions** As used in this Agreement the terms below shall have the following meanings: The following terms used in this Agreement shall have the same meaning as those terms in the Health Insurance Portability and Accountability Act Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

1. **Business Associate:** Business Associate shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party in this Agreement, shall mean [Insert Name of Business Associate].
2. **Covered Entity:** Covered Entity shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean DHHS.
3. **HIPAA Rules:** HIPAA Rule shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

**II Performance**

1. The specific work that is performed by the Business Associate on behalf of the Covered Entity involving the minimum necessary use and disclosure of Protected Health Information for the performance of this Agreement is presented in the attached “Scope-of-Work”.
2. The Scope-of-Work identifies, defines and delineates the Covered Entity and Business Associate’s contracted performance responsibilities in this Agreement, existing contracts or any future contract that involves the Business Associate’s use and disclosure of Protected Health Information (as identified within existing or future contracts) while performing a function on behalf of the Covered Entity.

3. The specific functions of performance and the authorized individuals or subcontractors is presumed to be identified within this Agreement, existing contracts or any future contract. Existing or future associated contract deliverables are considered unique and applicable to this Agreement's performance.
4. Based upon the written assurances specified in Section IV of this Agreement, the performance of work under this Agreement, existing and future contracts is considered to be in compliance with the HIPAA regulations regarding use, disclosure and safeguarding of the Protected Health Information involved in the performance of work in this Agreement and any associated contracts.

### **III. Notices.**

1. Written notices to the Covered Entity concerning performance of this Agreement, or amendments shall be sent through U.S. Postal Service, First Class Mail, pre-paid, to the attention of:
  - 1.1 Contact: **Name of Contact Here**
2. Written notices to the Business Associate concerning performance of this Agreement, or amendments shall be sent through U.S. Postal Service, First Class Mail, pre-paid, to the attention of:
  - 2.1 Contact: **Name of Contact Here**
3. When either party changes the contact or the contact's address, they shall give the other party written notice of the change.
4. Notices shall be deemed received within three days after the date of mailing.

### **IV. HITECH Act**

#### Business Associate – HITECH Section 13408

The HITECH Act requires that each entity that provides data transmission of protected health information to a covered entity and requires access on a routine basis shall be treated as a business associate and required to have a written contract.

#### Security Rule Duties HITECH Section 13401(a)

The HITECH Act requires that a business associate of a covered entity is required to comply with the HIPAA Security Rules including policies and procedures. If the business associate violates any of the Security Rules, the business associate may be subject to the HIPAA civil and criminal penalties.

#### Privacy Rules Duties HITECH Section 13404(a)

The HITECH Act requires that business associates use or disclose protected health information only if such use or disclosure is consistent with the terms of the business associate agreement between the entity and the business associate. If a business associate violates a Business Associate Agreement with respect to the new privacy requirement, the business associate may be subject to the same HIPAA civil and criminal penalties previously only applicable to covered entities.

#### Cure a Breach HITECH Section 13404(b)

The HITECH Act requires that a business associate take reasonable steps to cure breach of, or terminate, a business associate agreement if it becomes aware of a pattern of activity or practice by a covered entity that violates the agreement. The business associate may be liable for civil and or criminal penalties under HIPAA.

#### Breaches Treated as Discovered HITECH Section 13402(c)

A breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which the breach is known.

#### Notification in the Case of a Breach HITECH Section 13402

A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h) (1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach. Notifications shall be made no later than 60 days after the discovery of a breach. 13402(b) a business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify to the covered entity of such breach.

#### Civil and Criminal Penalties Tiers of Penalties

The HITECH Act specifies that business associates will be subject to the same civil and criminal penalties previously only imposed on covered entities. As amended by the HITECH Act, civil penalties range from \$100 to \$50,000 per violation, with caps of \$1,500,000 for all violations of a single requirement in a calendar year. The amount of the civil penalty imposed will vary depending on whether the violation was not knowing, due to reasonable cause, or due to willful neglect. Criminal penalties include fines up to \$50,000 and imprisonment for up to one year. In some instances, fines are mandatory.

### **V. Special Provisions to General Conditions:**

#### **1. Assurance of the Confidential Use and Disclosure of Protected Health Information.**

- 1.1 Use of Protected Health Information. Business Associate shall not use or further disclose Protected Health Information other than as permitted or required by this Agreement or as required by law. Business Associate may use Protected Health Information for the purposes of managing its internal business processes relating to its functions and performance under this Agreement.
- 1.2 Business Associate shall use appropriate safeguards to prevent unauthorized use or disclosure of Protected Health Information, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of Protected Health Information other than as provided for by the Agreement. Failure to comply could result in civil and criminal penalties.
- 1.3 To the extent the Business Associate is to carry out one or more of the Covered Entity's obligations under Subpart E of 45 CFR Part 164, comply with the

requirements of Subpart E that apply to the Covered Entity in the performance of such obligations.

## **2. Permitted Uses and Disclosures**

- 2.1 Covered Entity authorizes the use and disclosure of Protected Health Information by the Business Associate as follows:
  - 2.1.1 To identified individuals and entities: Business Associate's employees, agents and subcontractors associated with the performance of this specific Agreement and other existing or future contracts involving the use and disclosure of Protected Health Information that are deemed minimally necessary to perform the work as identified in the attached Scope-of-Work; and,
  - 2.1.2 For the purposes of: Business Associate's performance of work on behalf of the Covered Entity as specified in this Agreement and any existing or future contracts of this Agreement's attached Scope-of-Work.
- 2.2 Disclosure to Third Parties. Business Associate shall ensure that any of its agents and subcontractors that, create, receive, maintain, or transmit Protected Health Information received from Covered Entity (or created by or received from the Business Associate on behalf of Covered Entity) agree in writing to the same restrictions, and conditions relating to the, confidentiality, care, custody, and minimum use of Protected Health Information that apply to Business Associate in this Agreement by providing satisfactory assurances in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2).
- 2.3 Disclosure to the Workforce. Business Associate shall not disclose Protected Health Information to any member of its workforce except to those persons who have been authorized access to this information.
- 2.4 Disclosure and Confidentiality. Business Associate may maintain a confidentiality agreement with the individuals of its workforce, who have access to Protected Health Information. This confidentiality agreement should be substantially similar to the sample Authorized Workforce Confidentiality Agreement included as Exhibit "A" to this Agreement.
- 2.5 Minimum Necessary Standard. Pursuant to 45 CFR §164.502(b); §164.514(d): The Business Associate shall make reasonable efforts to limit the use and disclosure of Protected Health Information to the minimum necessary to accomplish the intended purpose of the use or disclosure. The Business Associate must limit access to those persons within its workforce, agents or subcontractors who are authorized and need the information in order to carry out their duties, and provide access only to the category of information that is required.
- 2.6 The Business Associate is authorized to use Protected Health Information to de-identify the information in accordance with 45 CFR 164.514(a)-(c).
- 2.7 The Business Associate shall obtain reasonable assurances from the person to whom the information is disclosed that the information will remain confidential

and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.

- 2.8 A violation of this Agreement may result in civil and criminal penalties to the Business Associate.

**3. Assurance of Reasonable Safeguards of Protected Health Information.**

- 3.1 Safeguards. Business Associate shall implement and maintain appropriate administrative, physical and technical safeguards to prevent access to and the use and disclosure of Protected Health Information, other than as provided for in this Agreement. The Business Associate agrees to assess potential risks and vulnerabilities to the individual health data in its care and custody and develop, implement and maintain reasonable security measures.

**4. Assurance of Accounting for Disclosures of Protected Health Information.**

- 4.1 Accounting for Protected Health Information Disclosures. Business Associate shall maintain an accounting of disclosures of Protected Health Information as required by the HIPAA regulations.
- 4.2 Disclosure to the U.S. Department of Health and Human Services (USDHHS). Business Associate shall make its internal practices, books and records relating to the use and disclosure of Protected Health Information received from Covered Entity (or created or received by Business Associate on behalf of Covered Entity) available to the Secretary of USDHHS or its designee for purposes of determining Covered Entity's compliance with HIPAA and with the Privacy and Security regulations. Business Associate shall provide Covered Entity with copies of any information it has made available to USDHHS under this section of this Agreement.

**5. Assurance for the Reporting and Remediation of Known Unauthorized Use and Disclosure of Protected Health Information.**

- 5.1 Reporting of unauthorized use, disclosures, or breach and remediation of risk conditions. Business Associate shall report to Covered Entity within fifteen (15) days from when it becomes aware of, any unauthorized use or disclosure of Protected Health Information made in violation of this Agreement or the HIPAA regulations, including any security incident that may put electronic Protected Health Information at risk. Business Associate shall, as instructed by Covered Entity, take immediate steps to mitigate any harmful effect of such unauthorized disclosure of Protected Health Information pursuant to the conditions of this Agreement through the preparation and completion of a written Corrective Action Plan subject to the review and approval by the Covered Entity. The Business Associate shall report any breach to the individuals affected and to the Secretary of USDHHS as required by the HIPAA regulations.

**6. Assurance of Access and Amendments to Protected Health Information.**

- 6.1 Right of Access. Business Associate shall make an individual's Protected Health Information available to the Covered Entity, an individual, or an individual's designee within fifteen (15) days of notice under this Agreement.
- 6.2 Right of Amendment. Business Associate shall make an individual's Protected Health Information available to the Covered Entity for amendment and correction within fifteen (15) days of notice under this Agreement, and shall incorporate any amendments or corrections to Protected Health Information within fifteen (15) days of notice under this Agreement that such amendments or corrections are approved.

## **7. Termination and Duties Upon Termination.**

- 7.1 Termination. Covered Entity may immediately terminate this Agreement and any and all associated Agreements identified in the Scope of Work if Covered Entity determines that the Business Associate has violated a material term of a performance condition of this Agreement.
- 7.2 Covered Entity, at its sole discretion, may choose to issue a plan of correction to the Business Associate to set the conditions for remediation of any material breach of performance in an effort to mitigate the cause for breach or consequent termination. The plan of correction issued by the Covered Entity under this subsection shall supercede the provisions of any Corrective Action Plan prepared by the Business Associate that are in conflict.
- 7.3 This Agreement may be terminated by either party with not less than fifteen (15) days prior written notice to the other party, which notice shall specify the effective date of the termination; provided whenever a notice provision for termination in any associated Agreement identified in the Scope of Work specifies a longer notice period for termination, the longer period shall apply; provided further that any termination of this Agreement shall not affect the respective obligations or rights of the parties arising under any existing contracts or otherwise under this Agreement before the effective date of termination.
- 7.4 Within thirty (30) days of expiration or termination of this Agreement, or as agreed, unless Business Associate requests and Covered Entity authorizes a longer period of time, Business Associate shall return or at the written direction of the Covered Entity destroy all Protected Health Information received from Covered Entity (or created or received by Business Associate on behalf of Covered Entity) that Business Associate still maintains in any form and retain no copies of such Protected Health Information. Business Associate shall provide a written certification to the Covered Entity that all such Protected Health Information has been returned or destroyed (if so instructed), whichever is deemed appropriate. If such return or destruction is determined by the Covered Entity to be infeasible, Business Associate shall use such Protected Health Information only for purposes that makes such return or destruction infeasible and the provisions of this Agreement shall survive with respect to such Protected Health Information.
- 7.5 Upon termination of this agreement for cause of violation of the performance conditions of this Agreement, or the HIPAA Privacy Rule standards for use and

disclosure, all associated existing contracts as identified or referred to in the Scope of Work Attachment are deemed terminated, except as provided in 45 CFR 164.504(e)(1)(ii)(B).

7.6 The obligations of the Business Associate under this Section shall survive the termination of this Agreement.

## **8. Amendment.**

8.1 Upon the enactment of any law or regulation affecting the use or disclosure of Protected Health Information required by the HIPAA regulations, or the publication of any decision of a court of the United States or of the State of Nebraska relating to any such law, or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, Covered Entity may provide written notice to the Business Associate to amend this Agreement in such a manner as Covered Entity determines necessary to comply with such law or regulation. If Business Associate disagrees with any such amendment, it shall so notify Covered Entity in writing within fifteen (15) days of Covered Entity's notice. If the parties are unable to agree on an amendment within fifteen (15) days thereafter, either of them may terminate this Agreement by reasonable written notice to the other.

## **9. Term of the Agreement.**

9.1 The date of this Agreement is \_\_\_\_\_, upon the signature of both parties, and continue for the longest applicable period, as follows:

9.1.1 If this Agreement is attached to any existing contract through an amendment process, then the term of the Agreement shall coincide with the term of the existing contract.

9.1.2 If this Agreement is attached to and incorporated into any renegotiated existing contract, or new contract as identified within the Scope-of-Work Attachment to this Agreement, then the term of the Agreement shall coincide with the term of the renewed contract or the new contract.

9.1.3 If this Agreement is not attached to or incorporated into any other contract between the Covered Entity and the Business Associate, then the term of the Agreement shall be from the commencement date for a period of five (5) years.

## **10. Hold Harmless.**

10.1 Business Associate agrees to hold the Covered Entity harmless for all loss or damage sustained by any person as a direct result of the negligent or willful acts by the Business Associate, its employees or agents in the performance of this Agreement, including all associated costs of defending any action.

**11. Execution.**

EACH PARTY has caused this Agreement to be properly executed on its behalf as of the date signed.

**For: DHHS Covered Entity**

**For: Contractor/ Business Associate**

Signature: \_\_\_\_\_

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Date \_\_\_\_\_

Date \_\_\_\_\_



**HIPAA/HITECH Business Associate Agreement  
SCOPE-OF-WORK ATTACHMENT**

THIS Scope-of-Work ATTACHMENT supplements and is incorporated into, and considered part of the Business Associate Agreement (herein referred to as (“Agreement”) by and between the Nebraska Department of Health and Human Services consisting of the agencies of Division of Public Health, Division of Behavioral Health, Division of Children and Family Services, Division of Medicaid & Long Term Care, Division of Developmental Disabilities, Division of Veteran’s Homes and represented herein collectively or singularly as the “Department of Health and Human Services” (DHHS also hereinafter referred to as “Covered Entity”), and **Name and address of Business here**, (hereinafter also referred to as “Business Associate”).

**I. GENERAL CONDITIONS**

1. Covered Entity agrees to provide the following:

1.1 Covered Entity will provide technical assistance directly to assist Business Associate with the use of any electronic formats for the transmission of Protected Health Information, such as magnetic tape. Covered Entity will provide advance notice whenever possible before making changes to the format or to the codes used in information processing.

2. Business Associate agrees to the following:

2.1 The Business Associate must adhere to all relevant confidentiality and privacy laws, regulations, and contractual provisions as provided within the Agreement.

2.2 The Business Associate shall have in place reasonable administrative, technical, and physical safeguards to ensure security and confidentiality of Protected Health Information.

2.3 A Corrective Action Plan (CAP) will be developed by the Business Associate to address and remediate any condition of contractual non-performance.

**II. SPECIAL PROVISIONS TO GENERAL CONDITIONS**

**This Scope-of-Work Attachment amends any contract between the parties listed in this attachment and all other existing contracts between the parties that involve the performance of work on behalf of the Covered Entity and that involve the processing, handling, use or disclosure of Protected Health Information. This Scope-of-Work Attachment shall also incorporate the provisions of the Agreement and this Attachment into all renewals of such existing contracts and into all new contracts between the parties that involve performance of work on behalf of the Covered Entity and that involve the processing, handling, use or disclosure of Protected Health Information.**

[Specifics to be included in this Scope of Work Attachment are:]

- **Scope of Work description.**
- **Contract Number, if available.**
- Specific information required if this Scope of Work applies to the Agreement as a distinct standalone instrument. This information identifies:
  1. The Protected Health Information to be used or disclosed during the term of this Agreement;
  2. The authorized individuals or entities that are associated with the performance of this Agreement;
  3. The permitted uses and disclosures of Protected Health Information allowed during the term of this Agreement.
  4. The description of the administrative, physical and technical security safeguards used to prevent use or disclosure of the Protected Health Information other than as provided for during the term of this Agreement.