

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered into between the Arizona Board of Regents for and on behalf of Northern Arizona University ("NAU") ("Covered Entity") and _____ ("Business Associate"), with an effective date of _____ ("Effective Date"). This Agreement sets out the responsibilities and obligations of Business Associate as a business associate of Covered Entity under the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act").

RECITALS:

A. Business Associate and Covered Entity have entered into a written agreement titled _____ (the "Written Agreement"), with an effective date of _____. Business Associate performs the services described in Written Agreement ("Services").

B. Covered Entity may make available to Business Associate Protected Health Information of Individuals in conjunction with Services. Business Associate will Use or Disclose such Protected Health Information only in accordance with this Agreement.

AGREEMENT:

Business Associate and Covered Entity agree to the terms and conditions of this Agreement in order to comply with the rules on handling of Protected Health Information under the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E ("Privacy Rule"), the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C ("Security Rule"), and the HIPAA Breach Notification Regulations, 45 C.F.R. Part 164, Subpart D ("Breach Notification Rule"), all as amended from time to time.

1. DEFINITIONS

- a. **Terms Defined in Regulation:** Unless otherwise provided in this Agreement, all capitalized terms in this Agreement will have the same meaning as provided under the Privacy Rule, the Security Rule and the Breach Notification Rule.
- b. **Protected Health Information or PHI:** Protected Health Information ("PHI") means PHI that is received or created on behalf of Covered Entity by Business Associate.

2. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

- a. **Performance of Services:** Business Associate will Use or Disclose PHI only for those purposes necessary to perform Services, or as otherwise expressly permitted in this Agreement or required by law, and will not further Use or Disclose such PHI.
- b. **Subcontractors:** Business Associate agrees that, when one of its subcontractors creates or receives PHI on behalf of Business Associate, Business Associate first will enter into an agreement with such

subcontractor that contains the same restrictions and conditions on the Use and Disclosure of PHI as contained in this Agreement.

- c. **Business Associate Management, Administration and Legal Responsibilities:** Business Associate may Use PHI for Business Associate's management and administration, or to carry out Business Associate's legal responsibilities. Business Associate may Disclose PHI to a third party for such purposes only if: (1) the Disclosure is required by law; or (2) Business Associate secures written assurance from the receiving party that the receiving party will: (i) hold the PHI confidentially; (ii) Use or Disclose the PHI only as required by law or for the purposes for which it was Disclosed to the recipient; and (iii) notify the Business Associate of any other Use or Disclosure of PHI.
- d. **Data Aggregation and De-Identification:** Business Associate may Use PHI to perform data aggregation services as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B). Business Associate also may de-identify PHI in accordance with 45 C.F.R. § 164.514.
- e. **Covered Entity Responsibilities:** To the extent Business Associate is to carry out Covered Entity's obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that apply to Covered Entity's compliance with such obligations.

3. SAFEGUARDS FOR PROTECTED HEALTH INFORMATION

- a. **Adequate Safeguards:** Business Associate will implement and maintain appropriate safeguards to prevent any Use or Disclosure of PHI for purposes other than those permitted by this Agreement, including administrative, physical and technical safeguards to protect the confidentiality, integrity, and availability of any electronic protected health information ("ePHI"), if any, that Business Associate creates, receives, maintains, and transmits on behalf of Covered Entity. Upon request of Covered Entity, Business Associate will provide evidence to Covered Entity that these safeguards are in place and are properly managed.
- b. **Compliance with HIPAA Security Rule:** Business Associate will comply with the HIPAA Security Rule, as of the date by which Business Associate is required to comply with such regulations.

4. REPORTS OF IMPROPER USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION, SECURITY INCIDENTS AND BREACHES

- a. **Use or Disclosure Not Permitted by This Agreement:** Business Associate will report in writing to Covered Entity any Use or Disclosure of PHI for purposes other than those permitted by this Agreement within 10 business days of Business Associate's learning of such Use or Disclosure.
- b. **Security Incidents:** Business Associate will report in writing to Covered Entity any Security Incident of which Business Associate becomes aware. Specifically, Business Associate will report to Covered Entity any successful unauthorized access, Use, Disclosure, modification, or destruction of ePHI or interference with system operations in an information system containing ePHI of which Business Associate becomes aware as soon as practicable, but no later than 10 business days from the date Business Associate learned of such Security Incident. Business Associate also will report the aggregate number of unsuccessful, unauthorized attempts to access, Use, Disclose, modify, or destroy ePHI or interfere with system operations in an information system containing ePHI, of which Business Associate becomes aware, provided that: (i) such reports will be provided only as frequently as the parties mutually agree, but no more than once per month; and (ii) if the definition

of “Security Incident” under the Security Standards is amended to remove the requirement for reporting “unsuccessful” attempts to Use, Disclose, modify or destroy ePHI, the portion of this Section 4 addressing the reporting of unsuccessful, unauthorized attempts will no longer apply as of the effective date of such amendment.

- c. **Breaches of Unsecured PHI:** Business Associate will report in writing to Covered Entity any Breach of Unsecured Protected Health Information, as defined in the Breach Notification Rule, as soon as practicable, but no later than 10 business days from the date Business Associate learns of the incident giving rise to the Breach. Business Associate will provide such information to Covered Entity as required in the Breach Notification Rule. Business Associate will reimburse Covered Entity for any reasonable expenses Covered Entity incurs in notifying Individuals of a Breach caused by Business Associate or Business Associate’s subcontractors or agents, and for reasonable expenses Covered Entity incurs in mitigating harm to those Individuals.

5. ACCESS TO PROTECTED HEALTH INFORMATION

- a. **Covered Entity Access:** Within 10 business days of a request by Covered Entity for access to PHI, Business Associate will make requested PHI available to Covered Entity and will provide a copy upon request.
- b. **Individual Access:** If an Individual makes a request for access directly to Business Associate, Business Associate will within 10 business days forward such request in writing to Covered Entity. Covered Entity will be responsible for making all determinations regarding the grant or denial of an Individual’s request for PHI and Business Associate will make no such determinations. Only Covered Entity will release PHI to an Individual pursuant to such a request.

6. AMENDMENT OF PROTECTED HEALTH INFORMATION

- a. **Covered Entity Request:** Within 10 business days of receiving a request from Covered Entity to amend an Individual’s PHI, Business Associate will provide such PHI to Covered Entity for amendment. Alternatively, if Covered Entity’s request includes specific instructions on how to amend the PHI, Business Associate will incorporate such amendment into the PHI it holds within 10 business days of receipt of the Covered Entity request.
- b. **Individual Request:** If an Individual makes a request for an amendment directly to Business Associate, Business Associate will within 10 business days forward such request in writing to Covered Entity. Covered Entity will be responsible for making all determinations regarding amendments to PHI and Business Associate will make no such determinations.

7. ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

- a. **Disclosure Records:** Business Associate will keep a record of any Disclosure of PHI that Business Associate makes, if Covered Entity would be required to provide an accounting to Individuals of such Disclosures under 45 C.F.R. § 164.528. Business Associate will maintain its record of such Disclosures for six years from the termination of this Agreement.
- b. **Data Regarding Disclosures:** For each Disclosure for which it is required to keep a record under paragraph 7(a), Business Associate will record and maintain the following information: (1) the date of Disclosure; (2) the name of the entity or person who received the PHI and the address of such

entity or person, if known; (3) a description of the PHI Disclosed; and (4) a brief statement of the purpose of the Disclosure.

- c. **Provision to Covered Entity:** Within 10 business days of receiving a notice from Covered Entity, Business Associate will provide to Covered Entity its records of Disclosures.
- d. **Request by Individual:** If an Individual requests an accounting of Disclosures directly from Business Associate, Business Associate will forward the request and its record of Disclosures to Covered Entity within 10 business days of Business Associate's receipt of the Individual's request. Covered Entity will be responsible for preparing and delivering the accounting to the Individual. Business Associate will not provide an accounting of its Disclosures directly to any Individual.

8. ACCESS TO BOOKS AND RECORDS

- a. **Covered Entity Access:** Business Associate will, within 10 business days of Covered Entity's written request, make available during normal business hours at Business Associate's offices, all records, books, agreements, policies and procedures relating to the Use or Disclosure of PHI for the purpose of allowing Covered Entity or its agents or auditors to determine Business Associate's compliance with this Agreement.
- b. **Government Access:** Business Associate will make its internal practices, books and records on the Use and Disclosure of PHI available to the Secretary of the Department of Health and Human Services to the extent required for determining compliance with the Privacy Rule, Security Rule, or Breach Notification Rule.

9. TERMINATION

Covered Entity may terminate this Agreement and the Written Agreement, if any, upon written notice to Business Associate if Covered Entity determines that the Business Associate or its subcontractors breached a material term of this Agreement. Covered Entity will provide Business Associate with written notice of the breach of this Agreement and afford Business Associate the opportunity to cure the breach to the satisfaction of Covered Entity within 30 days of the date of such notice. If Business Associate or its subcontractors fail to timely cure the breach, as determined by Covered Entity in its sole discretion, Covered Entity may terminate this Agreement and the Written Agreement, if any.

10. RETURN OR DESTRUCTION OF PROTECTED HEALTH INFORMATION

- a. **Return or Destruction of PHI:** Within 30 days of termination of this Agreement, Business Associate will return to Covered Entity all PHI that Business Associate or its subcontractors maintain in any form or format. Alternatively, Business Associate may, upon Covered Entity's consent, destroy all such PHI and provide written documentation of such destruction. Business Associate will be responsible for recovering any PHI from its subcontractors, or documenting their destruction of such PHI, consistent with the terms of this Section.
- b. **Retention of PHI if Return or Destruction is Infeasible:** If Business Associate believes that returning or destroying PHI at the termination of this Agreement is infeasible, it will provide written notice to Covered Entity within 30 days of the effective date of termination of this Agreement. Such notice will set forth the circumstances that Business Associate believes makes the return or destruction of PHI infeasible and the measures that Business Associate will take for assuring the continued confidentiality and security of the PHI. Covered Entity promptly will notify Business Associate of

whether it agrees that the return or destruction of PHI is infeasible. If Covered Entity agrees that return or destruction of PHI is infeasible, Business Associate may keep the PHI but will extend all protections, limitations and restrictions of this Agreement to Business Associate's Use or Disclosure of PHI retained after termination of this Agreement and will limit further Uses or Disclosures to those purposes that make the return or destruction of the PHI infeasible. Business Associate will also ensure that any such extended protections, limitations and restrictions apply to its subcontractors for whom return or destruction of PHI is determined by Covered Entity to be infeasible. If Covered Entity does not agree that the return or destruction of PHI from Business Associate or its subcontractors is infeasible, Covered Entity will provide Business Associate with written notice of its decision, and Business Associate and its subcontractors will proceed with the return or destruction of the PHI pursuant to the terms of this Section within 30 days of the date of Covered Entity's notice.

11. RESTRICTIONS ON USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION

If Covered Entity advises Business Associate of any changes in, or restrictions to, the permitted Use or Disclosure of PHI, Business Associate will restrict the Use or Disclosure of PHI consistent with the Covered Entity's instructions.

12. MITIGATION PROCEDURES

Business Associate will mitigate, to the maximum extent practicable, any deleterious effect from its or its subcontractors' Use or Disclosure of PHI in a manner that violates this Agreement.

13. OBLIGATIONS REGARDING BUSINESS ASSOCIATE PERSONNEL

Business Associate will inform all of its employees, agents and subcontractors ("Business Associate Personnel") who will be involved in providing Services, of the Business Associate's obligations under this Agreement. Business Associate represents and warrants that the Business Associate Personnel are under legal obligation to Business Associate, by contract or otherwise, sufficient to enable Business Associate to fully comply with the provisions of this Agreement. Business Associate will maintain a system of sanctions for any Business Associate Personnel who violate this Agreement.

14. COMPLIANCE WITH HITECH ACT AND REGULATIONS

Business Associate will comply with the requirements of Title XII, Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act, codified at 42 U.S.C. §§ 17921-17954, which are applicable to Business Associate, and will comply with all regulations issued by the Department of Health and Human Services (HHS) to implement these referenced statutes, as of the date by which Business Associate is required to comply with such referenced statutes and HHS regulations.

16. MISCELLANEOUS

- a. **COMPLIANCE WITH LAWS:** The parties are required to comply with federal and state laws. If this Agreement must be amended to secure such compliance, the parties will meet in good faith to agree upon such amendments.
- b. **CONSTRUCTION OF TERMS:** The terms of this Agreement will be construed in light of any applicable interpretation or guidance on the Privacy Rule, Security Rule or Breach Notification Rule issued by HHS.

- c. **NO THIRD PARTY BENEFICIARIES:** Nothing in this Agreement will confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
- d. **NOTICES:** All notices required under the Agreement will be given in writing and will be delivered by (1) personal service, (2) first class mail, or (3) messenger or courier. All notices shall be addressed and delivered to the contact designated in the signature block, or other address provided by the party from time to time in writing to the other party. Notices given by mail will be deemed for all purposes to have been given forty-eight hours after deposit with the United States Postal Service. Notices delivered by any other authorized means will be deemed to have been given upon actual delivery.
- e. **ENTIRE AGREEMENT:** This Agreement constitutes the entire agreement between the parties with regard to the Privacy Standards, Security Standards and Breach Notification Regulations. There are no understandings or agreements relating to this Agreement that are not fully expressed in this Agreement and no change, waiver or discharge of obligations arising under this Agreement will be valid unless in writing and executed by the party against whom such change, waiver or discharge is sought to be enforced.
- f. **WRITTEN AGREEMENT:** This Agreement will be considered an attachment to Written Agreement, if any, and is incorporated as though fully set forth within the Written Agreement. This Agreement will govern in the event of conflict or inconsistency with any provision of Written Agreement.
- g. **COUNTERPARTS AND SIGNATURE:** This Agreement may be executed in two or more counterparts, each of which shall be deemed an original and when taken together shall constitute one agreement. Facsimile and electronic signatures shall be deemed to be original signatures for all purposes of this Agreement.

BUSINESS ASSOCIATE

By: _____

Print Name: _____

Title: _____

Date: _____

COVERED ENTITY

By: _____

Print Name: _____

Title: _____

Date: _____

Contacts for Notices under this Agreement:

Print Name: _____

Title: _____

Address: _____

Print Name: _____

Title: _____

Address: _____

Phone: _____

Phone: _____