**BUSINESS ASSOCIATE ADDENDUM TO AGREEMENT**

THIS BUSINESS ASSOCIATE ADDENDUM (“Addendum”) is attached to and is made a part of a certain written agreement by and between The Nebraska Medical Center, a Nebraska non-profit corporation (“Covered Entity”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, (“Business Associate”) which agreement is dated the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (collectively, “Services Agreement”).

**RECITALS**

 WHEREAS, Business Associate performs certain services for Covered Entity described in Services Agreement; and

 WHEREAS, Covered Entity and Business Associate desire to comply with the Privacy, Security, Enforcement, and Breach Notification Rules promulgated by the Department of Health and Human Services at 45 CFR parts 160 and 164 under the Health Insurance Portability and Accountability Act of 1996.

 NOW, THEREFORE, the foregoing recitals are incorporated into this Addendum as if fully set forth herein, and the parties agree to as follows:

**1. DEFINITIONS.**

a. The following terms used in this Addendum shall have the same meaning as those terms in the HIPAA 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 have the same meaning as the term “business associate” at 45 CFR 160.103.
	2. Covered Entity. Covered Entity shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103.
	3. HIPAA Rules. HIPAA Rules shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Part 160 and Part 164.

**2. OBLIGATIONS OF THE BUSINESS ASSOCIATE.**

1. Business Associate shall not and shall ensure that its directors, officers, employees, contractors, subcontractors and agents do not use or further use or disclose Protected Health Information in any manner that would constitute a violation of HIPAA Rules other than as permitted or required by this Addendum or as Required By Law.
2. Business Associate acknowledges Business Associate is required by law to use appropriate safeguards and comply with the HIPAA Security Rule at 45 CFR 164 Subpart C.

c. When applicable, Business Associate shall comply with the Business and Academic Partner Network Access Technical Requirements as detailed in Exhibit A if Business Associate has access to Covered Entity network.

d. Business Associate agrees to mitigate, to the extent practicable, any potential business pattern, practice or effect that is known to the Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Addendum.

e. Business Associate agrees, within ten (10) calendar days of becoming aware of any use or disclosure of Protected Health Information not specifically allowed for by this Addendum and in violation of the HIPAA Rules, including Breaches of Unsecured Protected Health Information as required at 45 CFR 164.410, that it will report in writing to Covered Entity any such use or disclosure.

f. In the event that Covered Entity determines a Breach of Unsecured Protected Health Information has occurred, Business Associate agrees to provide Covered Entity a report including patient name, contact information, nature/cause of the breach, Protected Health Information breached and the date or period of time during which the breach occurred, within five (5) business days from the date the Covered Entity determines a Breach of Unsecured Protected Health Information has occurred. Business Associate shall be responsible for any and all costs incurred by Covered Entity related to notification of individuals or next of kin (if the individual is deceased) of any breach of Unsecured Protected Health Information reported by Business Associate to Covered Entity.

g. Business Associate agrees to immediately report to the Covered Entity any security incident of which it becomes aware.

h. Business Associate agrees to ensure that any employee, agent or third party, including but not limited to a subcontractor, to whom the Business Associate provides Protected Health Information received from, created by, or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions, conditions and requirements that apply through this Addendum to Business Associate with respect to such information.

i. Where Business Associate keeps a Designated Record Set of Protected Health Information, Business Associate agrees to make available Protected Health Information in a designated record set to Covered Entity, within five (5) business days of the request of Covered Entity or, as directed by Covered Entity, to an Individual or an Individual’s designee, as necessary in order to meet the Covered Entity’s obligations under 45 CFR 164.524(c)(2)(ii).; and (3)(ii) with respect to an Individual’s request for an electronic copy of Protected Health Information.

j. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to, at the request of Covered Entity or an Individual, in a time and manner necessary to satisfy Covered Entity’s obligations under 45 CFR 164.526.

1. Business Associate agrees to document any such use or disclosures of Protected Health Information and information related to such use or disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.
2. To the extent Business Associate is to carry out one or more of Covered Entity’s obligation(s) under 45 CFR Part 164 Subpart E, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).

m. Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, within ten (10) days of the request of the Covered Entity in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with HIPAA Rules**.**

n. Business Associate agrees to disclose to Covered Entity its policies, plans and procedures for compliance with regard to applicable HIPAA Rules, and this Addendum upon the request of Covered Entity.

1. Business Associate shall maintain at its own expense professional liability insurance or self-insurance coverage in the amount of $1,000,000 per occurrence and $3,000,000 in the annual aggregate for alleged errors or omissions or negligent acts in the performance of professional services rendered or that should have been rendered.

**3. PERMITTED USES AND DISCLOSURES OF BUSINESS ASSOCIATE.**

* 1. Except as otherwise limited in this Addendum, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, only the Covered Entity as specified in Services Agreement.
	2. Business Associate may use or disclose Protected Health Information as required by law.
	3. Business Associate will limit the uses and disclosures of, or requests for, Protected Health Information for purposes described in Services Agreement to the minimum necessary as is required by the HIPAA Rule, or through additional guidance published by the Secretary.
	4. Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains 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 Business Associate of any instances of which it is aware in which confidentiality of the information has been breached.
	5. Business Associate may provide data aggregation services relating to health care operations of the covered entity.
1. **OBLIGATIONS OF THE COVERED ENTITY**
	1. Covered Entity shall notify Business Associate of any limitation(s) in the Notice of Privacy Practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate’s use or disclosure of Protected Health Information.
	2. Covered Entity shall provide Business Associate with any changes in, or revocation of, the permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.
	3. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate’s use or disclosure of Protected Health Information.
	4. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under 45 CFR 164 Subpart E if done by the Covered Entity.
2. **TERM AND TERMINATION**
	1. Term. The Term of this Addendum shall be effective as of the effective date of the Services Agreement. This Addendum shall only terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity; or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.
	2. Termination for Cause. Upon Covered Entity's knowledge of any material breach by Business Associate of this Addendum, Covered Entity shall provide an opportunity for Business Associate to cure the breach or end the violation. In the event that Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, Covered Entity may immediately terminate the Services Agreement.
	3. Effect of Termination.
		1. Except as provided in paragraph (b) of this Section, upon termination of the Services Agreement, for any reason, Business Associate shall return or destroy, to the satisfaction of Covered Entity, all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
		2. In the event that Business Associate and Covered Entity agree that returning or destroying the Protected Health Information is infeasible, Business Associate agrees to extend the protections of this Addendum to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information. The obligations of Business Associate under this Section shall survive the termination of this Addendum.
3. **MISCELLANEOUS**
	1. Injunctive Relief. Any breach of this Addendum will result in irreparable harm to Covered Entity; therefore Covered Entity reserves the right to seek injunctive relief and all other legal and equitable remedies available under the law.
	2. Owner of Protected Health Information. Covered Entity is the owner of all Protected Health Information under this Addendum and the Services Agreement. Business Associate agrees to notify Covered Entity prior to any disclosure of Protected Health Information pursuant to a subpoena or other discovery request Required by Law for Protected Health Information.
	3. Regulatory References. A reference in this Addendum to a section of HIPAA means the section as in effect or as amended, and for which compliance is required.
	4. Amendment. The Parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for compliance with the HIPAA Rules and any other applicable law.
	5. Survival. All statements, representations, warranties, covenants and agreements contained in this Addendum shall be deemed to be material and shall survive the termination of the Services Agreement.
	6. Interpretation. Any ambiguity in this Addendum or the Services Agreement shall be interpreted to permit compliance with HIPAA Rules.

 IN WITNESS WHEREOF each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf this \_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_, 201\_\_.

**Covered Entity: Business Associate:**

**The Nebraska Medical Center** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**EXHIBIT A**

**Business and Academic Partner Network Access Technical Requirements**

**A**. **Non-Disclosure**. All access control information given to Business Associates must be kept confidential and must not be disclosed to any other individual/organization without the written permission of the University of Nebraska Medical Center (UNMC) computer network team.

**B.** **Connectivity Options.**  All connection methods to Covered Entity resources will be evaluated on a case-by-case basis. The UNMC Network Team is responsible for installation and configuration of the Business Associate connection. Business associate connection options include but are not limited to the following technologies:

1. Site to site VPN

2. On premise

3.  On Demand VPN Connectivity

**C**. **Remote Site Continuous Connectivity.** The requirements for providing continuous network connectivity between the Covered Entity network and a Business Associate network include but are not limited to:

1. Business associate will provide TCP/IP addressing for their networked devices that is unique to the Covered Entity environment. IP addresses which the Business Associate provides must be:
	1. Licensed to the organization for use on the public Internet; or
	2. Comply with RFC1918-Address Allocation for Private Internets
2. The Business Associate site will provide the TCP/IP address for each networked device resident on the Business Associate site's LAN that requires access to Covered Entity network resources.
3. The Business Associate site is responsible for the security of the remote site's Local Area Network (LAN).
4. The Business Associate site must have a firewall installed and maintained.
5. Connectivity to the Covered Entity network will be provided through a UNMC Network Team routed interface.
6. UNMC Network Team will maintain ACL's on the routed interface that will permit the Business Associate site to access only approved Covered Entity network resources.
7. UNMC Network Team will provide network support to the routed interface.
8. The Business Associate site will provide contact(s) for technical networking and workstation needs.
9. Business associate will not install or use peer-to-peer software or any remote administration software without coordination with IT Technical Services.

**D**. **Services Provided.** In general, services provided over the Business Associate connections should be limited only to those services needed, and only to those devices (hosts, servers, etc.) required to conduct necessary business. Blanket access will not be provided. The default setup will only allow access to those specific services that are needed. In no case shall the connection to the Covered Entity be used as the Internet connection for the Business Associate.

Any changes to the services require the Business Sponsor of the Covered Entity to request those changes. Business Associates are not allowed to request changes to their connectivity.

**E.** **Authentication for Business Associate Connections**. All Business Associate connections will be authenticated using a strong authentication process. A separate account will be established specifically for each Business Associate. A site to site connection relies on the security of the connecting site.

**F.** **Covered Entity Equipment at Business Associate Sites**. In some cases it may be necessary to have Covered Entity owned and maintained equipment at the Business Associate site. All such equipment will be documented by the UNMC Network Team. Access to network devices such as routers and switches will only be provided to UNMC support personnel. All Covered Entity owned equipment located at Business Associate sites is to be used for business purposes only. Any misuse of access or tampering with Covered Entity provided hardware will result in termination of the connection agreement between said parties.

**G**. **Business Associate Equipment located at the Covered Entity.** The Covered Entity will protect equipment which belongs to third parties in the same manner that Covered Entity equipment is protected. If networking equipment is found whose ownership is in question, UNMC Network Team will work to identify the owner of the equipment and ensure that the equipment is in compliance with all policies.

**H.** **Protection of Network Resources.** The UNMC Network Team will be responsible for ensuring all reasonable measures have been taken to ensure the integrity of the network. At no time will the Covered Entity rely solely on security and control mechanisms at the Business Associate site to protect Covered Entity confidential information.

**I. Acceptable Use.** Third party network connections are to be used for business purposes only. Any violation of these guidelines will be reported to the Business Associate sponsor and Covered Entity management. A joint decision will be made regarding the action to be taken. Action may result in the immediate termination of the connection/ agreement with said Business Associate.

1. All technical information provided to the Covered Entity by Business Associates must be accurate and current.
2. Covered Entity equipment located on partner premise will only be configured for the necessary protocols to facilitate Covered Entity related data transfers.
3. Configuration changes will be coordinated between the Business Associate, Business Associate sponsor and UNMC Network Team.
4. The UNMC Network Team will set the password on Covered Entity devices located on the partner premise. These devices will be actively monitored and any attempt to compromise these devices will result in termination of the connection.
5. Only employees of the Business Associate who have approved access shall use the resources associated with the Business Associate connection. Accounts should not be shared on Covered Entity owned and maintained devices.

**J. Audit and Review of Business Associate Connections.** The Covered Entity reserves the right to monitor their half of the mutually configured connections with Business Associates. The Covered Entity will not perform scans, penetration tests or other security related activities against the Business Associates’ networks. Likewise, the Business associate will not perform scans, penetration tests or other security related activities against the Covered Entity. The UNMC Security Team will review all Business Associate connections on an annual basis and information regarding specific Business Associate connections will be updated as necessary. Obsolete Business Associate connections will be terminated.