OLD DOMINION UNIVERSITY

Hosted Technology Services

Regulated ODU Data with HIPAA-BAA

CONTRACT FORM ADDENDUM TO CONTRACTOR'S FORM

CONTRACTOR NAME: _____

DATE: _____

The University and the Contractor are this day entering into a contract and, for their mutual convenience, the parties are using the standard form agreement provided by the Contractor, _____. This addendum, duly executed by the parties, is attached to, and hereby made a part of the contract.

The Contractor represents and warrants that it is a(n) ☐individual proprietorship ☐association ☐partnership ☐corporation ☐governmental agency or authority authorized to do in Virginia the business provided for in this contract. (Check the appropriate box.)

Notwithstanding anything in the Contractor's form to which this Addendum is attached, the payments to be made by the University for all goods, services and other deliverables under this contract shall not exceed fee schedule provided by Contractor and mutually agreed upon by the University and Contractor. Payments will be made only upon receipt of a proper invoice, detailing the goods/services provided and submitted to ***Old Dominion University, Finance Office, Rollins Hall Room 202, Norfolk, Virginia 23529 (or to invoice@odu.edu)***. The total cumulative liability of the University, its officers, employees, and agents in connection with this contract or in connection with any goods, services, actions, or omissions relating to the contract, shall not under any circumstance exceed payment of the above maximum purchase price plus liability for an additional amount equal to such maximum purchase price. In its performance under this contract, the Contractor acts and will act as an independent contractor, and not as an agent or employee of the University.

1. Definitions:
    a. "End User" means the individuals authorized by the University to access and use the Services provided by the Selected Firm/Vendor under this agreement.
    b. The "Agreement" includes the contract, this addendum and any additional addendums and attachments to the contract.
    c. "University" or "the University" means Old Dominion University, its trustees, officers, and employees. The point of contact for the University is the contract administrator for this Agreement.
    d. "Vendor" or "the Vendor" means the contractor, firm or organization that is selected to fulfill this Agreement, including any subcontractor selected by the Vendor to fulfill any portion of this Agreement.
    e. "University Data" includes all Personally Identifiable Information and other information that is not intentionally made available by the University on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and patient, student, and personnel data.
    f. "Personally Identifiable Information" includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or personnel identification number; "personal information" as defined in Virginia Code section 18.2-186.6 and/or any successor laws of the Commonwealth of Virginia; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights

and Privacy Act, 20 USC 1232g; "medical information" as defined in Virginia Code Section 32.1-127.1:05; "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license numbers; and state- or federal-identification numbers such as passport, visa or state identity card numbers.

g. "Security Breach" means a security-relevant event in which the security of a system or procedure involving University Data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.

h. "Service" or "Services" means any goods or services acquired by the University from the Vendor.

i. "Securely Destroy" means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-88 guidelines relevant to data categorized as high security.

2. ***PATIENT/HEALTH PLAN PARTICIPANT INFORMATION:*** Since the named Contractor will receive, create, and/or come into non-incidental contact with individually identifiable health information of ODU faculty, staff, students, or patients -- "Protected Health Information" as that term is defined in regulations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), at 45 C.F.R. Part 160.103 – Attachment A, Business Associate Addendum ("BAA"), shall also apply in addition to this Data Protection Addendum. Should there be any conflict between the language in this Data Protection Addendum and the attached BAA, the language in the BAA shall govern and superseded this Data Protection Addendum.

3. The Contractor's form contract is, with the exceptions noted herein, acceptable to the University. Nonetheless, because certain standard clauses that may appear in the Contractor's form agreement cannot be accepted by the University, and in consideration of the convenience of using that form, and this form, without the necessity of specifically negotiating a separate contract document, the parties hereto specifically agree that, notwithstanding any provisions appearing in the attached Contractor's form contract, none of the following provisions a. through s. shall have any effect or be enforceable against the University:

    a. Requiring or stating that the terms of the attached Contractor's form agreement shall prevail over the terms of this addendum in the event of conflict;

    b. Requiring that the contract be "accepted" or endorsed by the home office or by any other officer subsequent to execution by an official of the University before the contract is considered in effect;

    c. Requiring the application of the law of any state other than Virginia in interpreting or enforcing the contract or requiring or permitting that any dispute under the contract be resolved in the courts of any state other than Virginia;

    d. Requiring the University to indemnify or to hold harmless the Contractor for any act or omission;

    e. Requiring transportation terms other than 'FOB Destination,' with potential risk loss passing to University at delivery by Contractor to 'FOB Origin/Point.'

    f. Requiring or stating that during term of agreement the Contractor shall be the sole and exclusive provider of the associated goods and/or services.

    g. Renewing or extending the agreement beyond the initial term or automatically continuing the contract period from term to term;

h. Requiring the University to maintain any type of insurance either for the University's benefit or for the contractor's benefit;

i. Binding the University to any arbitration or to the decision of any arbitration board, commission, panel, or other entity;

j. Obligating the University to pay costs of collection or attorney's fees;

k. Granting the Contractor a security interest in property of the University.

l. Requiring any total or partial compensation or payment by the University of unpaid fees, whether current or future, for lost profit and/or as liquidated damages in the event of early termination of the then current term if for other than breach by the University, i.e., the University shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement, etc.;

m. Imposing interest charges contrary to that specified by the *Code of Virginia*, § 23-38.90, Specifically, §46 of the *Rules Governing Procurement of Goods, Services, Insurance, and Construction by a Public Institution of Higher Education of the Commonwealth of Virginia;*

n. Delaying the acceptance of this contract or its effective date beyond the date of execution;

o. Limiting or adding to the time period within which claims can be made or actions can be brought;

p. Limiting the liability of the Contractor for property damage or personal injury;

q. Permitting unilateral modification of this contract by the Contractor;

r. Bestowing any right or incurring any obligation that is beyond the duly granted authority of the undersigned agency representative to bestow or incur on behalf of the University.

s. Requiring the 'confidentiality' of the agreement, in whole or part, without exclusion to allow for the disclosure and/or release of specified confidential information in accordance with applicable law.

4. This Addendum and the Contract, including maintenance and support Services, may be renewed annually by University after the expiration of the initial term under the terms and conditions of the original Contract except as noted herein. If the University elects to exercise the option to renew the contract for an additional renewal period, the contract price(s) for the succeeding renewal period shall not exceed the contract prices(s) of the previous contract term increased/decreased by no more than the lesser of (1) the percentage increase/decrease of the "Other Services" category of the CPI-W of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available or (2) 5%.

5. No less than sixty (60) days prior to the expiration of the then current term, Contractor shall provide the University with a new contract agreement/price quote/proposal that must include (i) the new term dates, (ii) associated services and deliverables, (iii) new term pricing structure, and (iv) all associated terms and conditions and/or other documentation for University review, approval, and execution.

6. Upon University's decision to renew and/or extend any agreement, no less than thirty (30) days prior to the expiration of the then current term, the Contractor shall provide a valid invoice to the University.

7. Contractor certifies that the software does not contain any locks, worms, counters, CPU references, virus, or any other device capable of halting the operations of the software and/or altering the data or the program(s).

8. This agreement is subject to the Vendor related provisions of the Purchasing Manual for Institutions of Higher Education and their Vendors and any revisions thereto, which are hereby incorporated into this contract in their entirety. This manual can be found at: VASCUPP Higher Ed Manual

9. Payment terms shall be 30 days from the latter of the receipt of a valid invoice or the goods and services.

10. The University reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon 60 days written notice to the contractor. Any contract cancellation notice shall not relieve the contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

11. The Contract, and any future modification/addendums thereto, shall survive the assignment or change in control by the Contractor and as such shall remain in full force and apply to the successor, assignee, or acquirer as if no assignment or change in contract had occurred.

12. The cost of annual maintenance services of the hardware or software specified in any resulting Contract shall not exceed the lesser of the fair market price for like maintenance services or 15% of the quoted contract price.

13. Upon expiration of the specified warranty period and at the University's option, the contractor shall provide additional one-year periods of maintenance (including labor, parts, and travel). Maintenance shall not include external electrical work, providing supplies, and adding or removing accessories not provided for in the contract. Maintenance shall also not include repairs of damage resulting from: acts of God, transportation between state locations, negligence by state personnel, or other causes not related to ordinary use in the production environment in which installed.

14. Any software product(s) provided under the contract shall be the latest version available to the general public.

15. The University shall be entitled to all upgraded versions of the software covered in the contract that becomes available from the contractor if the software is covered under a maintenance/support agreement with the contractor. If the software is not continually covered under a maintenance/support agreement, then the maximum charge for upgrade shall not exceed the total difference between the cost of the Commonwealth's current version and the price the contractor sells or licenses the upgraded software under similar circumstances.

16. Unless otherwise stated, the software license(s) identified in the pricing schedule shall be purchased on a perpetual basis and shall continue in perpetuity. However, the University reserves the right to terminate the license at any time, although the mere expiration or termination of this contract shall not be construed as an intent to terminate the license. All acquired license(s) shall be for use at any computing facilities, on any equipment, by any number of users, and for any purposes for which it is procured. The Commonwealth further reserves the right to transfer all rights under the license to another state agency to which some or all its functions are transferred.

17. By submitting a proposal, the Contractor represents and warrants that it is the sole owner of the software or, if not the owner, that it has received all legally required authorizations from the owner to license the software, has the full power to grant the rights required by this agreement, and that neither the software nor its use in accordance with the contract will violate or infringe upon any patent, copyright, trade secret, or any other property rights of another person or organization.

18. All necessary software, to include any required client licenses, is provided as part of the offering from the Contractor at no additional charge to the University.

19. **Rights and License in and to University Data:** The parties agree that as between them, all rights including all intellectual property rights in and to University Data shall remain the exclusive property of the University, and the Vendor has a limited, nonexclusive license to use these data as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

20. **Disclosure:** Unless expressly agreeing to the contrary in writing, all goods, products, materials, documents, reports, writings, video images, photographs or papers of any nature including software or computer images prepared or provided by the Vendor (or its subcontractors) for the University will not be disclosed to any other person or entity without the written permission of the University.

21. **Data Privacy:**

a. The Vendor will use University Data only for the purpose of fulfilling its duties under this Agreement and will not share such data with or disclose it to any third party without the prior written consent of the University, except as required by this Agreement or as otherwise required by law.
b. University Data will not be stored outside the United States without prior written consent from the University.
c. The Vendor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill obligations under this Agreement. The Vendor will ensure that the Vendor's employees who perform work under this Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Agreement.
d. If the Vendor will have access to the University's Education records as defined under the Family Educational Rights and Privacy Act (FERPA), the Vendor acknowledges that for the purposes of this Agreement it will be designated as a "school official" with "legitimate educational interests" in the University Education records, as those terms have been defined under FERPA and its implementing regulations, and the Vendor agrees to abide by the limitations and requirements imposed on school officials. The Vendor will use the Education records only for the purpose of fulfilling its duties under this Agreement for University's and its End User's benefit, and will not share such data with or disclose it to any third party except as provided for in this Agreement, required by law, or authorized in writing by the University.

22. **Data Security:**
    a. The Vendor will store and process University Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.
    b. Without limiting the foregoing, Selected Firm/Vendor warrants that all electronic University Data will be encrypted in transmission (including via web interface) in accordance with latest version of National Institute of Standards and Technology Special Publication 800- 53.
    c. If the Selected Firm/Vendor stores Personally Identifiable Information as part of this agreement, the Selected Firm/Vendor warrants that the information will be stored in accordance with latest version of National Institute of Standards and Technology Special Publication 800-53.
    d. Selected Firm/Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this agreement.
    e. The University may inspect the data center used to store and process University Data at any time upon request.

23. **Data Authenticity, Integrity, and Availability:**
    a. The Vendor shall maintain a formal security program in accordance with industry standards that is designed to: (i) ensure the security and integrity of University Data; (ii) protect against threats or hazards to the security or integrity of University Data; and (iii) prevent unauthorized access to University Data.
    b. The Vendor shall be responsible for ensuring that University Data, per the Virginia Public Records Act, "is preserved, maintained, and accessible throughout their lifecycle, including converting and migrating electronic data as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration."
    c. The Vendor will ensure backups are successfully completed daily or more frequently and that restoration capability is maintained for restoration to a point-in-time and\or to the most current backup available.

d. The Vendor will maintain an uptime of 99.99% or greater, as agreed to for the contracted services via the use of appropriate redundancy, continuity of operations and disaster recovery planning and implementations.

24. **Employee Background Checks and Qualifications:**
    a. The Vendor shall ensure that its employees who will have potential access to University Data have passed appropriate, industry standard, background screening and possess the qualifications and training to comply with the terms of this agreement.

25. **Security Breach:**
    a. Response. Upon becoming aware of a Security Breach, or of circumstances that are understood to suggest a Security Breach, the Vendor will notify the University within 72 hours, fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Except as otherwise required by law, the Vendor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the University.
    b. Liability. In addition to any other remedies available to the University under law or equity, the Vendor will pay for or reimburse the University in full for all costs incurred by the University in investigation and remediation of such Security Breach caused by the Vendor, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Breach. The Vendor agrees to indemnify, hold harmless and defend the University from and against any and all claims, damages, or other harm related to such Security Breach.

26. **Requests for Data, Response to Legal Orders or Demands for Data:**
    a. Except as otherwise expressly prohibited by law, the Vendor will:
        i. immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by the Vendor seeking University Data;
        ii. consult with the University regarding its response;
        iii. cooperate with the University's requests in connection with efforts by the University to intervene and quash or modify the legal order, demand, or request; and
        iv. upon the University's request, provide the University with a copy of its response.
    b. If the University receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Virginia Freedom of Information Act) or request seeking University Data maintained by the Vendor, the University will promptly provide a copy to the Vendor. The Vendor will promptly supply the University with copies of data required for the University to respond, and will cooperate with the University's reasonable requests in connection with its response
    c. The University may request and obtain access to University Data and related logs at any time for any reason.

27. **Data Transfer Upon Termination or Expiration:**
    a. The Vendor's obligations shall survive termination of this Agreement until all University Data has been returned or Securely Destroyed
    b. Upon termination or expiration of this Agreement, the Vendor will ensure that all University Data are securely transferred, returned, or destroyed as directed by the University in its sole discretion. Transfer/migration to the University or a third party designated by the University shall occur without significant interruption in service within a reasonable time. The Vendor shall ensure that such

transfer/migration uses facilities and methods that are compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to University Data during the transition.

c. In the event that the University requests destruction of its data, the Vendor agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which the Vendor might have transferred University data. The Vendor agrees to provide documentation of data destruction to the University and to complete any required Commonwealth of Virginia documentation regarding the destruction of University Data.

d. The Vendor will notify the University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the University access to the Vendor's facilities to remove and destroy University-owned assets and data. The Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. The Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the University. The Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.

28. **Audits:**

a. The University reserves the right in its sole discretion to perform audits of the Vendor at the University's expense to ensure compliance with the terms of this Agreement. The Vendor shall cooperate in the performance of such audits. This provision applies to all agreements under which the Vendor must create, obtain, transmit, use, maintain, process, or dispose of University Data.

b. If the Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, protected health information, or financial or business data that is considered restricted data such as transaction data, the Vendor will at its expense conduct or have conducted at least annually a(n):

   i. American Institute of CPAs Service Organization Controls (SOC) Type II audit, or other security audit with audit objectives deemed sufficient by the University, which attests the Vendor's security policies, procedures, and controls;

   ii. Vulnerability scan, performed by a scanner approved by the University, of the Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this Agreement; and

   iii. Formal penetration test, performed by a process and qualified personnel approved by the University, of the Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this Agreement.

c. Additionally, the Vendor will provide the University upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this Agreement. The University may require, at University expense, the Vendor to perform additional audits and tests, the results of which will be provided promptly to the University.

29. **Compliance:**

a. The Vendor will comply with all applicable laws and industry standards in performing services under this Agreement. Any Vendor personnel visiting the University's facilities will comply with all applicable University policies regarding access to, use of, and conduct within such facilities. The University will provide copies of such policies to the Vendor upon request.

b. The Vendor warrants that the service it will provide to the University is fully compliant with and will enable the University to be compliant with relevant requirements of all laws, regulation, and guidance applicable to the University and/or the Vendor, including but not limited to: the Family Educational Rights and Privacy Act (school), Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), Section 508 of the Rehabilitation Act via a Voluntary Product Accessibility Template (VPAT), Federal Export Administration Regulations, Defense Federal Acquisition Regulation, and NIST 800-171 for Controlled Unclassified Information. Vendor is required to monitor all subservice providers and inform the University of any changes to subservice providers.

c. If the Payment Card Industry Data Security Standards (PCI-DSS) are applicable to the Vendor's service provided to the University, the Vendor will furnish proof of compliance with PCI-DSS.

30. **No End User Agreements:** This Addendum and the Vendor's Contract are the entire agreement between the University (including University employees and other End Users) and the Vendor. If the Vendor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with University employees or other End Users, such agreements shall be null, void and without effect, and the terms of this Addendum and the Vendor's Contract shall apply.

This Addendum has been reviewed by staff of the agency. Its substantive terms are appropriate to the needs of the agency and sufficient funds have been allocated for its performance by the agency. Any resulting contract is subject to appropriations by the Virginia General Assembly.

OLD DOMINION UNIVERSITY:	***CONTRACTOR:***
By: _____	By: _____
Signed: _____	Signed: _____
Title: _____	Title: _____

ATTACHMENT A

BUSINESS ASSOCIATE ADDENDUM

This Addendum is applicable only in those situations where the Vendor providing goods or services under a purchase order will receive or created Protected Health Information as defined in 45 C.F.R. § 164.501 (e.g., individually identifiable health information of patients of the Old Dominion University Health Services or Clinics or employees covered by the Old Dominion University Health Plan.)

This Business Associate Addendum ("Addendum") becomes effective when the Vendor accepts the Purchasing Terms and Conditions. It is entered into by the Vendor (the "Business Associate") and Old Dominion University (the "Covered Entity") (each a "Party" and collectively the "Parties").

The Business Associate has agreed to provide goods or services which necessitate the disclosure of Protected Health Information (individually identifiable health information of patients, as defined in 45 C.F.R. § 160.103) by the Covered Entity to the Business Associate, or the V. DEFINITIONS Business Associate creates, receives, uses or discloses Protected Health Information. Both Parties are committed to complying with the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Regulation") and the Security Standards for the Protection of Electronic Protected Health Information (the "Security Regulation") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This Addendum sets forth the terms and conditions pursuant to which Protected Health Information that is provided by, or created or received by, the Business Associate from or on behalf of the Covered Entity, will be handled between the Business Associate and the Covered Entity and with third parties during the term of their Agreement and after its termination. The Parties agree as follows:

I. ***Permitted Uses and Disclosures of Protected Health Information:***

1. **Services**. Pursuant to the Agreement, the Business Associate provides services or goods for the Covered Entity that involve the use and disclosure of Protected Health Information. Except as otherwise specified herein, the Business Associate may make any and all uses of Protected Health Information necessary to perform its obligations under the Agreement, provided that such use or disclosure of protected health information would not violate the Privacy Regulation if done by the Covered Entity or the minimum necessary policies and procedures of the Covered Entity. All other uses not authorized by this Addendum are prohibited. Moreover, Business Associate may disclose Protected Health Information for the purposes authorized by this Addendum only, (i) to its employees, subcontractors, and agents, in accordance with Section 2.1(f), (ii) as directed by the Covered Entity, or (iii) as otherwise permitted by the terms of this Addendum including, but not limited to, Section I.2(b) below.

2. **Business Activities of the Business Associate**. Unless otherwise limited herein, the Business Associate may:
    a. use the Protected Health Information in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of the Business Associate provided that such uses are permitted under state and federal confidentiality laws.

b. disclose the Protected Health Information in its possession to third parties for the purpose of its proper management and administration or to fulfill any present or future legal responsibilities of the Business Associate, if (i) the disclosures are required by law; or (ii) the Business Associate has received from the third party reasonable assurances regarding its confidential handling of such Protected Health Information as required under 45 C.F.R. § 164.504(e)(4).

II. ***Responsibilities with Respect to Protected Health Information:***

1. Privacy Responsibilities of the Business Associate. With regard to its use and/or disclosure of Protected Health Information, the Business Associate hereby agrees to do the following:
    a. request from the Covered Entity, access, and disclose to its subcontractors, agents or other third parties, only the minimum amount of Protected Health Information necessary to perform or fulfill a specific function required or permitted hereunder.
    b. use and/or disclose the Protected Health Information only as permitted or required by this Addendum or as otherwise required by law.
    c. report to the designated Privacy Officer of the Covered Entity, in writing, any use and/or disclosure of the Protected Health Information that is not permitted or required by this Addendum of which Business Associate becomes aware within five days of the Business Associate's discovery of such unauthorized use and/or disclosure.
    d. establish procedures for mitigating, to the greatest extent possible, any deleterious effects from any improper use and/or disclosure of Protected Health Information that the Business Associate reports to the Covered Entity.
    e. implement appropriate administrative, technical, and physical safeguards to maintain the security of the Protected Health Information and to prevent its unauthorized use and/or disclosure.
    f. ensure that all of its subcontractors and agents that receive or use, or have access to, Protected Health Information under this Agreement agree to the same restrictions and conditions on the use and/or disclosure of Protected Health Information that apply to the Business Associate pursuant to this Addendum.
    g. make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of Protected Health Information to the Covered Entity, or at the covered entity's request, to the Secretary of HHS, in a time and manner designated by the Secretary, for purposes of determining the Covered Entity's compliance with the Privacy Regulation, subject to attorney-client and other applicable legal privileges.
    h. upon prior written request, make available during normal business hours at Business Associate's offices all records, books, agreements, policies and procedures relating to the use and/or disclosure of Protected Health Information to the Covered Entity within 15 days for purposes of enabling the Covered Entity to determine the Business Associate's compliance with the terms of this Addendum.

i. within 30 days of receiving a written request from the Covered Entity, provide to the Covered Entity such information as is requested by the Covered Entity to permit the Covered Entity to respond to a request by an individual for an accounting of the disclosures of the individual's Protected Health Information in accordance with 45 C.F.R. §164.528.
j. document such disclosures of Protected Health Information and information related to such 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 C.F.R. § 164.528.

2. HITECH Act and Security Responsibilities of the Business Associate. Notwithstanding any other provision in the Agreement or this Addendum, no later than February 17, 2010, unless a separate effective date is specified by law or the Agreement or this Addendum for a particular requirement (in which case the separate effective date will be the effective date for that particular requirement), the Business Associate will comply with the HITECH Standards. "HITECH Standards" means the privacy, security, and security breach notification provisions applicable to a Business Associate under Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), which is Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5), and any regulations promulgated thereunder. The parties recognize that additional regulations and guidance documents may be issued implementing and interpreting the HITECH Act during the term of the Agreement. The Business Associate agrees to comply with all applicable requirements of such additional regulations and guidance as they become effective and agrees that to the extent such regulations or guidance require the Covered Entity to impose such requirements on the Business Associate, they are deemed imposed as and when they become effective.

   The Business Associate further agrees:
   a. To implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Health Information that it creates, receives, maintains or transmits on behalf of Covered Entity, and more specifically to secure all electronic Protected Health Information with technologies and methodologies, including encryption, that render such information "secured" as defined in the guidance issued in 74 FR 19006 (April 27,2009), pursuant to the HITECH Act;
   b. To ensure that any agent, including a subcontractor, to whom it provides Protected Health Information agrees to implement reasonable and appropriate safeguards to protect it, including but not limited to encryption that renders such information as "secured" as defined above; To notify the Covered Entity on the first day on which a security breach is known by Business Associate or an employee, officer or agent of Business Associate other than the person committing the breach, or as soon as possible following the first day on which Business Associate or an employee, officer or agent of the Business Associate other than the person committing the breach should have known by exercising reasonable diligence of such breach. "Security Breach" as used herein is defined as an acquisition, access, use, or disclosure of Protected Health Information in a

manner not permitted under the HIPAA Privacy Rule. Notification will be made to Old Dominion University Information Security, Policy and Records Office at (434) 924-4165. It will include, to the extent possible, the identification of each individual whose unsecured PHI has been or is believed by the Business Associate to have been, accessed, acquired, used or disclosed during the breach. The Business Associate will also provide any other available information at the time of notification or promptly thereafter as information becomes available. Such additional information will include (i) a brief description of what happened, including the date of the breach; (ii) a description of the types of unsecured PHI that were involved in the breach; (iii) the originals, or if not applicable, complete copies, of all documents containing exposed Protected Health Information and any related correspondence that come into the Business Associate's possession. (iv) any steps the Business Associate believes individuals should take to protect themselves from potential harm resulting from the breach; and (v) a brief description of what the Business Associate is doing to investigate the breach, mitigate harm to individuals, and protect against any future breaches.

c. To cooperate with the Covered Entity as needed to further investigate and evaluate any Security Breach involving the Business Associate or of which the Business Associate has become aware

d. In the event of impermissible use or disclosure by the Business Associate of unsecured Protected Health Information that constitutes, in the reasonable judgment of the Covered Entity a breach requiring notification under applicable provisions of the HITECH Act and implementing regulations, at the discretion of the Covered Entity either the Business Associate or the Covered Entity will notify in writing all affected individuals as required by Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act. The Business Associate will be responsible for all costs associated with such notification, including any costs of credit monitoring services that the Covered Entity determines should be offered to affected individuals. For purposes of this paragraph, unsecured PHI means PHI which is not encrypted or destroyed. Breach means the acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule or this contract which compromises the security or privacy of the PHI by posing a significant risk of financial, reputational, or other harm to the individual, as reasonably determined by the Covered Entity.

III. ***Term and Termination:***

1. Term. This Addendum will become effective on the Effective Date and will continue in effect until all obligations of the Parties have been met, unless terminated as provided in this Section. In addition, certain provisions and requirements of this Addendum will survive its expiration or other termination in accordance with Section IV.1 herein.

2. Termination by the Covered Entity. As provided for under 45 C.F.R. § 164.504(e)(2)(iii), the Covered Entity may immediately terminate the Agreement and this Addendum if the Covered Entity makes the determination that the Business Associate has breached a material term of this Addendum. Alternatively, the Covered Entity may choose to: (i) provide the Business Associate with ten days written notice of the existence of an alleged material breach; and (ii) afford the Business Associate an opportunity to cure said alleged material breach upon mutually agreeable terms. Nonetheless, in the event that mutually agreeable terms cannot be achieved within ten days, Business Associate must cure said breach to the satisfaction of the Covered Entity within ten days. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement and this Addendum.

   If neither termination nor cure are feasible, Covered Entity will report the violation to the Secretary.

3. Automatic Termination. This Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Agreement between the Parties.

4. Effect of Termination. Upon the event of termination pursuant to this Section, the Business Associate agrees to return or destroy all Protected Health Information pursuant to 45 C.F.R. § 164.504(e)(2)(I) if it is feasible to do so. Prior to doing so, the Business Associate further agrees to recover any Protected Health Information in the possession of its subcontractors or agents. If it is not feasible for the Business Associate to return or destroy said Protected Health Information, the Business Associate will notify the Covered Entity in writing. Said notification will include: (i) a statement that the Business Associate has determined that it is infeasible to return or destroy the Protected Health Information in its possession, and (ii) the specific reasons for such determination. The Business Associate further agrees to extend any and all protections, limitations and restrictions contained in this Addendum to the Business Associate's use and/or disclosure of any Protected Health Information retained after the termination of this Addendum or the Agreement, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the Protected Health Information infeasible. If it is infeasible for the Business Associate to obtain, from a subcontractor or agent any Protected Health Information in the possession of the subcontractor or agent, the Business Associate must provide a written explanation to the Covered Entity and require the subcontractors and agents to agree to extend any and all protections, limitations and restrictions contained in this Addendum or the Agreement to the subcontractors' and/or agents' use and/or disclosure of any Protected Health Information retained after the termination of this Addendum, and to limit any further uses and/or disclosures to the purposes that make the return or destruction of the Protected Health Information infeasible.

IV. ***Miscellaneous:***

1. Survival. The respective rights and obligations of the Business Associate and Covered Entity under the provisions of Sections II.1, II.2, and III.4, solely with respect to Protected Health Information that the Business Associate retains in accordance with Section III.4 because it is not feasible to return or destroy such Protected Health Information, will survive termination of this Addendum indefinitely.

2. Waiver. A waiver with respect to one event will not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

3. No Third-Party Beneficiaries. Nothing express or implied in this Addendum is intended to confer, nor will anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

4. Notices. Any notices to be given will be made via U.S. Mail or express courier to the address given below:
    a. If to the Business Associate, to the address provided by the Business Associate to Procurement Services.
    b. If to the Covered Entity, to:

        HIPAA Privacy Official
        4700 Elkhorn Avenue, Suite 4302
        Norfolk, Virginia 23529
        Fax: 757-683-5155

        With a copy (which will not constitute notice) to:

        Office of General Counsel
        Old Dominion University
        Koch Hall, Suite 2018
        Norfolk, Virginia 23529
        Fax: 757-683-5041

5. Interpretation. Any ambiguity in this Addendum and the Agreement will be resolved to permit Covered Entity to comply with the Privacy Rule.

6. Counterparts; Facsimiles. This Addendum may be executed in any number of counterparts, each of which will be deemed an original. Facsimile copies hereof will be deemed to be originals.

V. ***Definitions:***

Terms used, but not otherwise defined, in this Addendum will have the same meaning as those terms in 45 C.F.R. § 160.103 and 164.501.