This Business Associate Addendum (“Addendum” “BAA”), effective 2018, ("Effective Date"), is entered into by (the “Business Associate”) and The Rector and Visitors of the University of Virginia, (the “Covered Entity”) (each a “Party” and collectively the “Parties”).

The Parties have entered into an agreement/PO dated 2018 (the "Agreement") under which the Covered Entity discloses Protected Health Information (individually identifiable health information of patients, as defined in 45 C.F.R. § 160.103) to the Business Associate for purposes for the obligations described below, or the Business Associate creates, receives, uses or discloses Protected Health Information in its performance of the obligations described below. 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:

1. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

1.1 Services. Pursuant to the Agreement, the Business Associate provides services or goods for the Covered Entity that involves 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 1.2(b) below.

1.2 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).

1.3 Additional Activities of Business Associate The Business Associate also may:

a. at the request of the Covered Entity, aggregate the Protected Health Information in its possession with the Protected Health Information of other covered entities that the Business Associate has in its possession through its capacity as a business associate to said other covered entities provided that the purpose of such aggregation is to provide the Covered Entity with data analyses relating to the Health Care Operations of the Covered Entity. Under no circumstances may the Business Associate disclose Protected Health Information of one Covered Entity to another Covered Entity absent the explicit authorization of the Covered Entity.

b. at the request of the Covered Entity, de-identify any and all Protected Health Information provided that the de-identification conforms to the requirements of 45 C.F.R. § 164.514(b), and further provided that the Covered Entity maintains any documentation required by 45 C.F.R. § 164.514(b) which may be in the form of a written assurance from the Business Associate. Pursuant to 45 C.F.R. § 164.502(d)(2), de-identified information does not constitute Protected Health Information and is not subject to the terms of this Addendum.

2. RESPONSIBILITIES WITH RESPECT TO PROTECTED HEALTH INFORMATION

2.1 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 under this Addendum and/or the Agreement.

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 5 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 in writing 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.

k. to the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) 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 obligation(s);

2.2 HITECH Act and Security Responsibilities of the Business Associate.

The Business Associate agrees to 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 Electronic Protected Health Information (as defined in 45 C.F.R. §160.103) 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 in writing to implement reasonable and appropriate safeguards to protect it, including but not limited to encryption that renders such information as “secured” as defined above;

c. To notify the Covered Entity as soon as possible, but no later than the third 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 business 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 UVA Information Security, Policy and Records Office at (434) 924-4165 with written notice as per section 5.5 of this Addendum. It will include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably 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.

d. 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.

e. In the event of impermissible use or disclosure by the Business Associate or any subcontractor 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, at the discretion of 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 and Business Associate reasonably agree should be offered to affected individuals. For purposes of this paragraph, unsecured PHI means PHI which is not encrypted or destroyed. “Breach” shall have the meaning set forth in 45 CFR 164.402.
f. To report promptly to the Covered Entity any Security Incident, as defined in Section 164.304 of the Security Regulation, of which it becomes aware. However, the Business Associate shall not be obliged to report an immaterial incident consisting solely of an unsuccessful attempt to improperly access information stored in systems under the Business Associate’s control.

3. **ADDITIONAL RESPONSIBILITIES OF THE PARTIES WITH RESPECT TO PROTECTED HEALTH INFORMATION**

3.1 **Responsibilities of the Business Associate with Respect to Handling of Designated Record Set.** In the event that the Parties mutually agree in writing that the Protected Health Information constitutes a Designated Record Set, the Business Associate hereby agrees to do the following:

   a. at the request of, and in the time and manner designated by the Covered Entity, provide access to the Protected Health Information to the Covered Entity or the individual to whom such Protected Health Information relates, or his or her authorized representative, in order to meet a request by such individual under 45 C.F.R. § 164.524.

   b. at the request of, and in the time and manner designated by the Covered Entity, make any amendment(s) to the Protected Health Information that the Covered Entity directs pursuant to 45 C.F.R. § 164.526. Provided, however, that the Covered Entity makes the determination that the amendment(s) are necessary because the Protected Health Information that is the subject of the amendment(s) has been, or could foreseeably be, relied upon by the Business Associate or others to the detriment of the individual who is the subject of the Protected Health Information to be amended.

3.2 **Responsibilities of the Covered Entity with Respect to the Handling of the Designated Record Set.** In the event that the Parties mutually agree in writing that the Protected Health Information constitutes a Designated Record Set, the Covered Entity hereby agrees to do the following:

   a. notify the Business Associate, in writing, of any Protected Health Information that Covered Entity seeks to make available to an individual pursuant to 45 C.F.R. § 164.524 and the time, manner and form in which the Business Associate will provide such access.

   b. notify the Business Associate, in writing, of any amendment(s) to the Protected Health Information in the possession of the Business Associate that the Business Associate will make and inform the Business Associate of the time, form and manner in which such amendment(s) will be made.
4. **TERMS AND TERMINATION**

4.1 **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 5.1 herein.

4.2 **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 10 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 10 days, Business Associate must cure said breach to the satisfaction of the Covered Entity within 10 days. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement and this Addendum.

4.3 **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.

4.4 **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, within 90 days of the termination. 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 with a Certificate of Destruction that 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 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. As noted all actions above must be completed no later than 90 days after the termination.

5. **MISCELLANEOUS**

5.1 **Survival.** The respective rights and obligations of the Business Associate and Covered Entity under the provisions of Sections 2.1, 2.2, 4.4, and 5.4, solely with respect to Protected Health Information that the Business Associate retains in accordance with Section 4.4 because it is not feasible to return or destroy such Protected Health Information, will survive termination of this Addendum indefinitely. In addition, Section 3 will survive termination of this Addendum, provided that the Covered Entity determines that the Protected Health Information being retained pursuant to Section 4.4 constitutes a Designated Record Set.

5.3 **Amendments; Waiver.** This Addendum may not be modified, nor will any provision be waived or amended, except in a writing duly signed by authorized representatives of the Parties. 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.

5.4 **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.

5.5 **Notices.** Any notices to be given will be made via fax or express courier to the address given below, except that notice of a security breach shall also be given as provided in section 2.2(c) of this Addendum.

If to the Business Associate, to:
Name
Title
BUSINESS ASSOCIATE
Address
City, State, Zip
Fax: (XXX) XXX-XXXX

If to Covered Entity, to:
Corporate Compliance and Privacy Officer
University of Virginia Health System
1 Jefferson Park Avenue
Box #800805, McKim #G043D
Charlottesville, Virginia 22908-0805
Phone: (434) 924-2938
Fax: (434) 243-2716
with a copy (which will not constitute notice) to:
Office of the University Counsel
University of Virginia
P.O. Box 400225
Fax: 434-982-3070

5.6 **Interpretation.** Any ambiguity in this Addendum and the Agreement will be resolved to permit Covered Entity to comply with the Privacy and Security Rules and the HITECH Act and applicable regulations and guidance documents.

5.7 **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.

6. **DEFINITIONS.**

Terms used, but not otherwise defined; in this Addendum will have the same meaning as those terms in 45 C.F.R. Parts 160, 162, and 164.

IN WITNESS WHEREOF, each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf effective as of the Effective Date stated above herein.

The Rector and Visitors of the University of Virginia

By: _____________________________
Name: _________________________
Title: ___________________________
Date: __________________________

BUSINESS ASSOCIATE

By: _____________________________
Name: _________________________
Title: ___________________________
Date: __________________________