Data Protection Addendum

This Data Protection Addendum ("Addendum") is by and between **Virginia Commonwealth University** ("VCU") and the **Firm**[1] (each a "Party" and collectively the "Parties"). It is applicable only in those situations where the Firm provides goods or services under which necessitate that the Firm create, obtain, transmit, use, maintain, process, or dispose of VCU Data[2] (as defined in the Definitions Section of this Addendum) in order to fulfill its obligations to VCU.

1. DEFINITIONS

   a. "End User" means an individual authorized by VCU to access and use the Services provided by the Firm under this agreement.

   b. "Protected VCU Data" includes all data defined as Highly Sensitive, Sensitive, or Internal Use data that is not intentionally made generally available by VCU on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and patient, student, and personnel data.

   c. "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, REV 1 guidelines relevant to data categorized as high security.

   d. "Security Breach" means the unauthorized access, use or disclosure that compromises or threatens to compromise the confidentiality, integrity, or availability of VCU Data

   e. "Services" means any goods or services acquired by VCU from the Firm.

   f. "VCU Data" includes Protected VCU Data and any other information that is created, possessed or used by VCU or is intentionally made generally available by VCU on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and patient, student, and personnel data.

   g. "Audit" includes or may include a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.

2. RIGHTS AND LICENSE IN AND TO VCU DATA

   The parties agree that as between them, all rights including all intellectual property rights in and to VCU Data shall remain the exclusive property of VCU, and Firm 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.

---

[1] The term "Firm" shall have the same meaning and be interchangeable with the terms "Vendor", "Supplier" and/or "Contractor" as such terms may be used/referenced in this Addendum or the underlying agreement.

[2] If the Firm providing goods or services to VCU will receive, create, or come into non-incidental contact with patient or VCU health plan participant Protected Health Information (PHI) as that term is defined in 45 C.F.R. § 160.103, the Firm may be a Business Associate, and agrees to abide by the terms and conditions of the Business Associate Addendum in addition to the Data Protection Addendum should a determination be made that the Firm is a BAA.

3. DATA PRIVACY

a. Firm will use VCU 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 VCU, except as required by this agreement or as otherwise required by law.

b. Protected VCU Data will not be stored outside the United States without prior written consent from VCU.

c. Firm will provide access to VCU Data only to its employees and subcontractors who need to access the data to fulfill Firm obligations under this agreement. Firm will ensure that 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. The following provision applies only if Firm will have access to VCU's education records as defined under the Family Educational Rights and Privacy Act (FERPA): The Firm acknowledges that for the purposes of this agreement it will be designated as a "school official" with "legitimate educational interests" in VCU education records, as those terms have been defined under FERPA and its implementing regulations, and the Firm agrees to abide by the limitations and requirements imposed on school officials. Firm will use the education records only for the purpose of fulfilling its duties under this agreement for VCU'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 VCU.

4. DATA SECURITY, INTEGRITY, AND CONFIDENTIALITY

a. Firm will take reasonable measures, including the use of industry standard administrative, technical, and physical controls, such as redundant backups, access control and auditing, to protect VCU Data to ensure the integrity and availability of VCU Data against deterioration or degradation of data quality and authenticity. The Selected Firm will be responsible during the terms of this agreement, unless otherwise specified elsewhere in this agreement, for converting and migrating electronic data as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration.

b. Firm will store and process VCU Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, such as network and system protection, access controls, and security auditing and monitoring, and to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will ensure the confidentiality and overall security of VCU Data, and be no less protective than those used to secure Firm'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. Without limiting the foregoing, Firm warrants that all electronic VCU Data will be encrypted in transmission (including via web interface) in accordance with industry best practices in data encryption.

c. If the Firm stores, transmits, or processes Protected VCU Data as part of this agreement, the Firm warrants that the information will be stored in accordance with the practices and controls stated in the latest version of National Institute of Standards and Technology Special Publication 800-53 Moderate or the International Organization for Standardization and the International Electrotechnical Commission 27002 (ISO/IEC 27002).

d. Firm will use reasonable, appropriate industry-standard and up-to-date security tools and technologies in providing Services under this agreement.

5. EMPLOYEE BACKGROUND CHECKS AND QUALIFICATIONS

Firm shall ensure that its employees who will have potential access to VCU Data have passed reasonable and appropriate background screening and possess the qualifications and training to comply with the terms of this agreement.

6. SECURITY BREACH

a. Response. Upon becoming aware of a Security Breach, or of circumstances that are reasonably understood to suggest an actual or suspected Security Breach of VCU Data, Firm will immediately notify VCU consistent with applicable state or federal laws, fully investigate the incident, and cooperate fully with VCU's investigation of and response to the incident. Except as otherwise required by law, Firm will not provide notice of an actual or suspected Security Breach directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from VCU.

b. Liability. If Firm must under this agreement create, obtain, transmit, use, maintain, process, or dispose of Protected VCU Data, the following provisions apply:

1) In addition to any other remedies available to VCU under law or equity, Firm will reimburse VCU in full for all costs not covered by vendor's insurance incurred by VCU in investigation and remediation of any Security Breach caused by Firm, 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 Protected VCU Data 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.

2) In addition to any other insurance coverage required by another contract/agreement with VCU, the Firm will for the duration of the term of the agreement, maintain at least $5 million Cyber Liability coverage with insurance companies that hold at least an A- financial rating with A.M. Best Company. In no event, should the Firm construe these minimum required limits to be their limit of liability to VCU.

3) VCU must be named as an Additional Insured on the Cyber Liability Insurance, and the proper name is "The Commonwealth of Virginia, and Virginia Commonwealth University, its officers, employees and agents." Upon VCU's request, the Selected/Firm Vendor will provide a Certificate of Insurance (COI).

7. RESPONSE TO LEGAL ORDERS, DEMANDS OR REQUESTS FOR DATA

a. Except as otherwise expressly prohibited by law, Firm will immediately notify VCU of Firm's receipt of any subpoenas, warrants, or other legal orders, demands or requests seeking VCU Data; consult with VCU regarding its response; cooperate with VCU's reasonable requests in connection with efforts by VCU to intervene and quash or modify the legal order, demand or request; and provide VCU with a copy of its response.

b. If VCU receives a subpoena, warrant, or other legal order, demand or request (including request pursuant to the Virginia Freedom of Information Act) seeking VCU Data maintained by Firm, VCU will promptly provide a copy to Firm. Firm will promptly supply VCU with copies of data required for VCU to respond in a timely manner, and will cooperate with VCU's reasonable requests in connection with its response.

8. DATA TRANSFER UPON TERMINATION OR EXPIRATION

a. Upon termination or expiration of this agreement, Firm will ensure that all VCU Data are securely returned or destroyed as directed by VCU in its sole discretion. Transfer to VCU or a third party designated by VCU shall occur within a reasonable period of time, and without significant interruption in service. Firm shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of VCU or its transferee, and to the extent technologically feasible, that VCU will have reasonable access to VCU Data during the transition.

b. Upon termination or expiration of this agreement, and after any requested transfer of data, Firm must Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which the Firm might have transferred VCU data. The Firm agrees to provide documentation of data destruction to VCU.

c. Firm will notify VCU of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing VCU access to Firm's facilities to remove and destroy VCU- owned assets and data. Firm shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to VCU. Firm 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 VCU. Firm will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on VCU, all such work to be coordinated and performed in advance of the formal, final transition date.

9. AUDITS

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

b. If the Firm must under this agreement create, access, obtain, transmit, use, maintain, process, or dispose of Protected VCU Data or financial or business data which has been identified to the Firm as having the potential to affect the accuracy of VCU's financial statements, Firm will at its expense complete and keep up-to-date the latest Higher Education Collaborative Vendor Assessment Toolkit (HECVAT) Full Version questionnaire; conduct or have conducted, at least annually, a security audit by a third party with audit scope and objectives deemed sufficient by VCU, which attests the Firm's security policies, procedures, and controls; vulnerability scan by a third party of Firm's electronic systems and facilities that are used in any way to deliver electronic services under this agreement; assessments of the Firm's own service providers ("subservice providers") that are used by the firm to provide services to VCU; and formal penetration test by a third party of Firm's electronic systems and facilities that are used in any way to deliver electronic services under this agreement.

c. Additionally, the Firm will provide VCU 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. VCU may require, at VCU expense, the Firm to perform additional audits and tests, the results of which will be provided promptly to VCU.

10. COMPLIANCE

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

b. Firm warrants that the service it will provide to VCU is fully compliant with all state and federal laws, regulations, industry codes, and guidance that may be applicable to the service, which may include:

1) any applicable national, federal, state or local law, rule, directive or regulation relating to the privacy of personal information, including, without limitation, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g, and its implementing regulations ("FERPA), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Privacy and Security Rules issued thereunder, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), the Financial Modernization Act of 1999 ("Gramm-Leach-Bliley Act"), the Fair Credit Reporting Act as amended by the Fair and Accurate Credit Transactions Act, the Americans

with Disabilities Act, Section 508 of the Rehabilitation Act (29 U.S.C. 794d, as amended, and the Virginia Consumer Data Protection Act;

2) any privacy policy or practice applicable to any personal information that Customer or any User accesses, uses, collects, or maintains hereunder, including, without limitation any practice required in connection with the processing of credit card data, including the Payment Card Industry Data Security Standards ("PCI-DSS"); and

3) Federal Export Administration Regulations, Federal Acquisitions Regulations, Defense Federal Acquisitions Regulations and Department of Education guidance.

c. If PCI-DSS is applicable to the Firm service provided to VCU, the Firm agrees to: Store, transmit, and process VCU Data in scope of the PCI-DSS in compliance with the PCI-DSS; and Attest that any third-party providing services in scope of PCI-DSS under this agreement will store, transmit, and process VCU Data in scope of the PCI-DSS in compliance with the PCI-DSS; and Provide either proof of PCI-DSS compliance or a certification (from a recognized third-party security auditing firm), within 10 business days of the request, verifying Firm/Vendor and any third party who stores, transmits, or processes VCU data in scope of PCI-DSS as part of the services provided under this agreement maintains ongoing compliance under PCI-DSS as it changes over time; and Store, transmit, and process any VCU Data in scope of the PCI DSS in a manner that does not bring VCU's network into PCI-DSS scope; and Attest that any third-party providing services in scope of PCI-DSS under this agreement will store, transmit, and process VCU Data in scope of the PCI-DSS in a manner that does not bring VCU's network into PCI DSS scope.

11. SURVIVAL

The Firm's obligations under Section 8 shall survive termination of this agreement until all VCU Data has been returned or Securely Destroyed.