September 20, 2016

EXHIBIT I (IT Clauses)

1. Data Privacy

a. Contractor will use data either supplied by University or to which Contractor has access to under this Agreement ("SUNY Data") only for the purpose of fulfilling its duties under this Agreement and will not share SUNY Data with or disclose it to any third party without the prior written consent of University, except as required by this Agreement or as otherwise required by law. Contractor may disclose SUNY Data to the extent that disclosure is based on the good-faith written opinion of Contractor's legal counsel that disclosure is required by law or by order of a court or governmental agency. Contractor may exercise this right only if it has requested this disclosure and communicated the legal opinion in writing and in advance to the University.

b. All SUNY Data shall be considered to be confidential and shall be treated as such by Contractor, its employees and subcontractors. Contractor shall implement and maintain appropriate policies and procedures to safeguard the confidentiality of SUNY Data in accordance with this Agreement. Contractor shall notify University promptly of any requests, from any source, for copies of or access to, or other disclosure of SUNY Data. If there is an impermissible disclosure, unauthorized use, loss or destruction of SUNY Data, Contractor shall immediately notify the University and take all reasonable steps to mitigate any potential harm or further disclosure, loss or destruction of such SUNY Data. Upon the expiration or termination of this Agreement, and at any other time at the written request of the University, Contractor shall promptly return to the University all SUNY Data (and all copies of this information) that is in Contractor's or any of its subcontractor's possession or control, in a form useable and agreeable to Stony Brook.

c. SUNY Data must be stored, housed, processed, backed-up, archived and otherwise retained on systems physically located in the continental United States, unless an exception is explicitly approved in writing by Stony Brook. This requirement applies to all of Contractor's subcontractors.

d. Contractor will provide access to SUNY Data only to its employees and subcontractors who need to access the SUNY Data to fulfill Contractor's obligations under this Agreement.

e. Contractor will ensure that employees and subcontractors 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. Contractors and its employees and subcontractors who may access SUNY Data must have executed agreements concerning access protection and data/software security that are consistent with the terms and conditions of this Agreement prior to being provided such access and which require them to comply with all University, Stony Brook University Hospital or State University of New York policies and procedures regarding data access, privacy and security, including those prohibiting or restricting remote access to University's systems and data.

f. If Contractor will have access to University Education records as defined under the Family Educational Rights and Privacy Act ("FERPA"), Contractor 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 Contractor shall abide by the limitations and requirements imposed on school officials under FERPA. Contractor shall use the Education records only for the purpose of fulfilling its obligations under this Agreement for University'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 University.

g. Contractor's failure to comply with the provisions of this Section or that of its employees or subcontractor may result in University restricting offending individuals from access to University computer systems or SUNY Data, or immediately terminating this Agreement. Contractor shall be responsible for maintaining and ensuring the confidentiality and security of SUNY Data.

2. Data Security

a. Contractor shall maintain, during the term of the Agreement, network security which includes: network firewall provisioning, intrusion detection, and regular third party vulnerability assessments, and share such assessment results with University. Contractor shall maintain network security that conforms to generally recognized "Industry Standards "and best practices and University security policies (https://it.stonybrook.edu/policies), procedures and requirements. Generally recognized industry standards include, but are not limited to, the current standards and benchmarks set forth and maintained by the Center for Internet Security (see http://www.cisecurity.org) or Payment Card Industry/Data Security Standards (PCI/DSS) - see http://www.pcisecuritystandards.org/

b. Contractor shall implement and use network management and maintenance applications and tools, appropriate intrusion prevention and detection, and data confidentiality/protection/encryption technologies for endpoints, servers and mobile devices. This must include mechanisms to identify vulnerabilities and apply security patches. Contractor will also physically and logically separate different customers' networks where applicable.

c. Contractor shall establish, maintain, and provide documentation of a continuous security program throughout the term of the Agreement. The contractor will provide information in the form requested by Stony Brook, including but not limited to the completion of a security questionnaire and relevant diagrams and/or whitepapers. The security program must enable University (or its selected third party) to:

i) Define the scope and boundaries, policies, and organizational structure of an information security management system.
ii) Conduct periodic risk assessments to identify the specific threats to and vulnerabilities of University.
iii) Implement appropriate mitigating controls and training programs, and manage resources.
iv) Monitor and test the security program to ensure its effectiveness. Contractor shall review and adjust the security program in light of any assessed risks.

d. In no event shall Contractor's action or inaction result in any situation that is less secure than the greater of:

a) The security that University provided as of the date of the Agreement.
b) The security that Contractor then provides for its own systems and data.
c) Contractor will provide access of any third-party certifications held, including but not limited to SOC II, FedRAMP, ISO2700 or PCI.

f. Contractor shall ensure physical security of SUNY Data. This includes:

i) Physical access to any equipment that contains any SUNY Data.
ii) Any mobile storage devices, laptops, or any other access on desktops that allow Contractor's employees or subcontractor's to access, transmit, or store. These devices must be encrypted and employ appropriate authentication mechanisms to assure access is limited to authorized individuals (e.g. two factor authentication.)
iii) Scenarios for moving and storing electronic data off-site in a secure manner.
iv) Physical Transport of Data – Contractor shall use reputable means to transport data. Deliveries must be made either via hand delivery by an employee of the Contractor, by reputable moving company complying with University specified security measures or by restricted delivery via courier (e.g., FedEx, United Parcel Service, United States Postal Service) with shipment tracking and receipt confirmation. This applies to transport between the Contractor's offices, to and from subcontractors, and to the University.

g. University will authorize, and Contractor will issue, any necessary information access mechanisms, including access identities (IDs) and passwords, to be used by Contractor and its employees and subcontractors.

Contractor shall provide these individuals with only the minimum level of access necessary to perform the tasks and functions for which they are responsible under this Agreement. Contractor shall update, as necessary, a list of those employees and subcontractors of Contractor who have access to University's systems, software and SUNY Data, and the level of such access. Remote access for support to resources on-premise at Stony Brook will be granted only through methods approved by Stony Brook University. Access will be limited to named individuals and require logging and security controls that will assure access is limited to authorized individuals (e.g. two factor authentication). These logs will be provided to Stony Brook upon request.

h. University and Contractor will collaborate on security monitoring and incident response, define points of contact on both sides, establish monitoring and response procedures, set escalation thresholds, and conduct training. Contractor shall, at the request of University, and, quarterly, provide University Information with a report of the incidents that it has identified and take measures to resolve.

3. Contractor Personnel

a. If consistent with Contractor's employment policies, Contractor shall conduct a drug screening and background check on all individuals that Contractor provides access to SUNY Data and review the results of such screening and check of each person to verify that the person meets the Contractor standards for employment.

4. New York Information Breach and Notification Requirements

a. Contractor shall use commercially reasonable efforts to maintain the security of private information (as defined in the New York State Information Security Breach and Notification Act, as amended("ISBNA")(General Business Law § 889-aa; State Technology Law § 208) that it creates, receives, maintains or transmits on behalf of the University and to prevent unauthorized use and/or disclosure of that private information; and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic private information that it creates, receives, maintains or transmits on behalf of the University ("Contractor University Data"). Contractor shall disclose to the University pursuant to the ISBNA, and any other applicable law, any breach of the security of a system involving Contractor University Data following discovery or notification of the breach in the system as to any resident of New York State whose private information was, or is reasonably believed to have been acquired by a person without valid authorization ("Security Incidents"). The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Contractor shall be liable for the costs associated with such breach if caused by the Contractor's, or that of its employees or subcontractors, negligent or willful acts or omissions, including indemnifying the University for the cost of notifying individuals, in the event of such a breach. Upon termination or expiration of this Agreement, Upon the expiration or termination of this Agreement, and at any other time at the written request of the University, Contractor shall promptly return to the University all Contractor University Data (and all copies of this information) that is in Contractor's or any of its subcontractor's possession or control, in whatever form.

5. Enforcement

a. To the extent permissible under law, the University may seek specific enforcement of Contractor's obligation of the foregoing sections, if Contractor or its employees or subcontractors breach any obligation set forth therein. In addition, Contractor shall indemnify and hold harmless the University for all damages, claims, losses, charges, and costs and expenses, including, but not limited to, counsel fees and disbursement, arising out of, related to or in connection with any such breach.