

EXHIBIT "A"

**UNIVERSITY OF PENNSYLVANIA PURCHASE ORDER
CONFIDENTIALITY AND PRIVACY REQUIREMENTS**

A. **Definitions:** When used in this document, the following definitions shall apply:

Confidential Information - Sensitive Personally Identifiable Information and Proprietary Information provided by, or on behalf of the Buyer, in any form, including without limitation oral or written (paper or electronic) whether presented in text, graphics, charts or other formats.

Sensitive Personally Identifiable Information ("SPII") - Information relating to an individual that reasonably identifies the individual and, if compromised, could cause harm to that individual or to Buyer. Examples may include, but are not limited to: Social Security Numbers, credit card numbers, bank account information, student grades or disciplinary information, salary or employee performance information, donations, patient health information, information Buyer has promised to keep confidential, and account passwords or encryption keys used to protect access to SPII. SPII shall not include information that can not reasonably be used to identify the individual to whom it pertains.

Proprietary Information ("PI") - Data, information, or intellectual property in which the Buyer has an exclusive legal interest or ownership right which, if compromised could cause harm to Buyer. Examples may include, but are not limited to, business planning, financial information, trade secret, copyrighted material, and software together with comparable material from a third party when the Buyer has agreed to keep such information confidential.

B. **Service Provider** – The Supplier under the Purchase Order is a Service Provider hereunder.

In General: Service Provider agrees to maintain strict confidentiality concerning Confidential Information in accordance with the requirements and conditions set forth in this Section.

Exclusions: These requirements shall not apply to any information or data which:

1. is lawfully possessed by Service Provider prior to entering into this Agreement;
2. shall be lawfully acquired by Service Provider in circumstances or in a manner not resulting from, or related to, this Agreement or the performance of the Services;
3. becomes part of the public domain in any manner other than the publication thereof in violation of this Agreement or otherwise unlawfully;
4. is disclosed by Service Provider with the prior written approval of the Buyer; or
5. is otherwise required by applicable law to be disclosed by Service Provider (but then only to the extent that, and only to the recipient or recipients to whom or which such disclosure is required; and only after Buyer has failed to obtain a protective order or other appropriate relief governing disclosure of the data within 10 days after notice from Supplier of any disclosure request).

C. **Property of Buyer:** Confidential Information shall remain the sole property of Buyer. Service Provider expressly acknowledges and agrees that Service Provider has no property right or interest whatsoever in any such data.

D. **Security Safeguards:** Service Provider shall maintain adequate administrative, technical and physical safeguards against unauthorized access, use, or disclosure of Confidential Information. This requirement includes but it is not limited to, the following components.

1. Confidential information may only be stored on electronic computing devices that are current in their anti-virus software and security patches and that are protected by a firewall.
2. All access to confidential information electronically shall be via a unique user ID and unique password that is not shared with others.
3. Confidential information shall not be downloaded to a portable device, such as Laptop computers, PDAs and USB drives, unless such data is protected with strong encryption.

4. Confidential information transmitted electronically must be encrypted in transmission, unless otherwise authorized by the Buyer.
5. Any use or handling of Social Security Numbers must be specifically approved by the Buyer.
6. Confidential information shall not be removed from the Service Provider's work site unless such removal is authorized by the Buyer as necessary for Agreement-related purposes.
7. When Confidential Information is no longer required to perform services required under this Agreement, and is not longer required to be maintained by applicable law or the terms of this Agreement, the Service Provider shall securely destroy such information whenever such destruction is practicable.
8. If Service Provider is retains backups of Confidential Information, such backups shall be maintained in conformity with these Security Safeguards.

Any question regarding the applicability of or interpretation of these requirements must be directed to Buyer's Office of Audit, Compliance and Privacy or Buyer's Office of Information Security.

E. Compliance.

1. **Laws.** Service Provider shall comply with all applicable laws, ordinances, statutes regulations and other requirements established by federal, state and local governmental authorities regarding privacy and security protections for Confidential Information. Applicable statutes may include but are not limited to The Family Education Rights and Privacy Act, the Gramm-Leach-Bliley Act and The Health Insurance Portability and Accountability Act.
2. **Other.** Service Provider shall comply with the Payment Card Industry Data Security Standard, as applicable.

F. Use and Disclosure Limitation: Service Provider shall not use, provide, trade, give away, barter, lend, sell, or otherwise disclose Confidential Information, and shall not make any copies of such data or any type whatsoever, in readable or encrypted form, or in individually identifiable or aggregate form, except

1. as necessary for the services described in this Agreement to be performed; or
2. as expressly permitted by Buyer in a separate writing.

G. Restricted Access: Service Provider shall only permit access to Confidential Information acquired by Service Provider in connection with this Agreement, and only to employees, agents or independent contractors of Service Provider (1) who are directly involved in performing the Services for the Buyer and have a specific need to know such information, and (2) who have entered into written confidentiality agreements which impose, or are otherwise bound by, restrictions on the Confidential Information at least equivalent to those imposed under this Agreement.

H. Breach: Service Provider shall immediately report to Buyer any unauthorized access, use, disclosure, modification, or destruction of Buyer's Confidential Information or interference with system operations in an information system containing Buyer's Confidential Information ("Breach") of which Service Provider becomes aware.

I. Remediation/ Mitigation: When Service Provider learns of a Breach it shall (1) use best efforts to determine the scope and nature of the Breach, (2) work with the Buyer, in light of the circumstances and applicable law, to determine what risks are posed by the Breach and whether and how those persons whose data was accessed, acquired or disclosed should be notified, and (3) restore the reasonable integrity of the data system which hosts the Buyer's Confidential Information without compromise to forensic investigation.

J. Indemnification: Service Provider agrees to indemnify, defend and hold harmless Buyer, its trustees, officers and employees (individually, an "Indemnified Party", and collectively, the "Indemnified Parties"), from and against any and all liability, loss, damage, action, claim or expense ("Claims") suffered or incurred by the Indemnified Parties (including reasonable attorney's fees and expenses) that results from or arises out of any unauthorized access, use or disclosure of Buyer's Confidential Information by Service Provider. With regard to Service Provider's obligation to defend, the Buyer shall have the right to select the legal counsel whom Service Provider shall provide to defend any Indemnified Party, subject to Service Provider's approval of the qualifications

of such legal counsel and the reasonableness of counsel's hourly rates as compared to the rates of attorneys with similar experience and qualifications in the relevant area of legal expertise and in the jurisdiction where the Claims will be adjudicated . If the Buyer elects, in its sole discretion, to retain separate legal counsel, in addition to or in lieu of the counsel to be provided by Service Provider, then all costs and expenses incurred by the Buyer for such separate counsel shall be borne by the Buyer and the Service Provider shall reasonably cooperate with the Buyer and its separate legal counsel in the investigation and defense of any such claim or action. Service Provider shall not settle or compromise any claim or action giving rise to Claims in a manner that imposes any restrictions or obligations on Buyer without Buyer's prior written consent. If the Buyer elects to require that Service Provider defend a Claim pursuant to this paragraph, and Service Provider fails or declines to assume the defense of such Claim within thirty (30) days after notice thereof, the Buyer may assume the defense of such Claim for the account and at the risk of Service Provider, and any Liabilities related thereto shall be conclusively deemed a liability of Service Provider. Service Provider agrees that if it is named as a party in an action that results from or arises out of any unauthorized access, use or disclosure of Buyer's Confidential Information, and Buyer is not named as a party to such action, Service Provider shall, immediately upon receiving notice of such action, notify Buyer of the action. The indemnification rights of the Indemnified Parties contained herein are in addition to all other rights which such Indemnified Party may have at law or in equity or otherwise.

- K. **Return of Confidential Information:** Upon the expiration or earlier termination of the Agreement or at the request of Buyer, Service Provider will either (1) at its own expense, immediately return to Buyer all Confidential Information embodied in tangible form, whether or not reduced to such form by Service Provider including all copies thereof, or (2) at the Buyer's option, certify in writing to Buyer that all such Confidential Information has been destroyed, except that Service Provider may retain Confidential Information to the extent that retention is required by law or is needed to document performance under this Agreement.
- L. **External Request for Confidential Information:** In the event that the Service Provider receives a request for Confidential Information by subpoena or other legal process or from a court, governmental authority, or accrediting agency, the Service Provider shall give prompt written notice to the Buyer in order to allow the Buyer the opportunity to seek a protective order or to take other appropriate action to protect the Confidential Information.