EXHIBIT A

UNIVERSITY OF PENNSYLVANIA
CONFIDENTIALITY AND PRIVACY REQUIREMENTS

A. **Definitions:** When used in these University of Pennsylvania Confidentiality and Privacy Requirements (this "**Exhibit A**"), the following definitions shall apply:

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

2. **Personally Identifiable Information ("PII") -** Information relating to an individual that reasonably identifies the individual and, if compromised, could cause harm to that individual or to University. 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 the University has promised to keep confidential, and account passwords or encryption keys used to protect access to PII. PII shall not include information that cannot reasonably be used to identify the individual to whom it pertains.

3. **Proprietary Information -** Data, information, or intellectual property in which the University has an exclusive legal interest or ownership right which, if compromised could cause harm to University. 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 University has agreed to keep such information confidential.

B. **Service Provider:** The Company under the Agreement is a Service Provider hereunder.

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

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

    a. Is lawfully possessed by Service Provider prior to entering into the Agreement;

    b. Shall be lawfully acquired by Service Provider in circumstances or in a manner not resulting from, or related to, the Agreement or the performance of the Services;

    c. Becomes part of the public domain in any manner other than the publication thereof in violation of this Exhibit G, the Agreement or otherwise unlawfully;

    d. Is disclosed by Service Provider with the prior written approval of the University; or

    e. 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 University 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 University:** Confidential Information shall remain the sole property of University. 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, cellular telephones, 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 University.

5. Any use or handling of Social Security numbers must be specifically approved by the University.

6. Confidential Information shall not be removed from the Service Provider's work site unless such removal is authorized by the University as necessary for Agreement-related purposes.

7. When Confidential Information is no longer required to perform Services under the Agreement, and is no longer required to be maintained by applicable law or the terms of this Exhibit G, the Service Provider shall securely destroy such information whenever such destruction is practicable.

8. If Service Provider 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 University's Office of Audit, Compliance and Privacy or University'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 Educational Rights and Privacy Act ("FERPA"), the Gramm-Leach-Bliley Act ("GLBA"), The Health Insurance Portability and Accountability Act ("HIPAA"), and the European Union's General Data Protection Regulation ("GDPR").

2. **FERPA**. Service Provider is a "school official with legitimate educational interests" under FERPA. Service Provider acknowledges that the education records it collects, maintains, uses and/or discloses are the property of the University and are under the direct control of the University.

3. **DOJ Bulk Data Security Regulations**. This Section applies with respect to any Access to University's

or its affiliates' Bulk U.S. Sensitive Personal Data or Government-Related Data ("Covered Data") by a Country of Concern or Covered Person, including any Covered Data Transaction, as each term is defined under Executive Order 14117 of February 28, 2024, and its implementing rules. Service Provider represents, warrants, and covenants that:

a. Service Provider, its affiliates, and their respective employees and contractors who have Access to Covered Data are not Covered Persons;

b. Service Provider, its affiliates, and their respective employees and contractors, will not engage in any Covered Data Transaction; and

c. Service Provider will immediately notify University in writing if any representation in this section is no longer true.

4. **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 required to perform Services under the Agreement; or

2. As expressly permitted by University in a separate writing.

G. **Restrictions on Use of Artificial Intelligence**: Service Provider, its affiliates, and subcontractors shall not: (1) utilize any artificial intelligence model or system in a manner that would permit University's Confidential Information to be shared with any third party; or (b) use University's Confidential Information, in any form, to develop or improve its products or services, including but not limited to, training any artificial intelligence model or system.

H. **Restricted Access:** Service Provider shall only permit access to Confidential Information acquired by Service Provider in connection with the Agreement, and only to employees, agents or independent contractors of Service Provider: (1) who are directly involved in performing the Services for the University 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 Exhibit A.

I. **Subcontractors**: Service Provider is responsible for the reasonable protection of Confidential Information that Service Provider and/or its subcontractors create, maintain, use or disclose. Service Provider maintains procedures to ensure that Service Provider only selects and retains subcontractors who are capable of maintaining reasonable physical, technological, and administrative safeguards to protect Confidential Information.

Service Provider's contracts with subcontractors require subcontractors to maintain appropriate measures designed to ensure that Confidential Information is kept confidential, secure, and is only be used for the purposes set forth in the Agreement.

Service Provider's subcontractors are responsible for ensuring that any security breach involving Confidential Information will be reported to the Service Provider promptly and the Service Provider will then promptly report such security breach to University.

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

K. **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 University, 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 University's Confidential Information without compromise to forensic investigation.

L. **Data Subject Requests:** Service Provider shall promptly notify the University of any data subject requests concerning their PII. Service Provider will reasonably cooperate with University in relation to any data subject requests concerning their PII.

M. **Indemnification and Limitation of Liability:** 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.

N. **Return of Confidential Information:** Upon the expiration or earlier termination of the Agreement or

at the request of University, Service Provider will either (1) at its own expense, immediately return to University 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 University's option, certify in writing to University 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 the Agreement or this Exhibit A.

O. **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 University in order to allow the University the opportunity to seek a protective order or to take other appropriate action to protect the Confidential Information.