University of Cincinnati Data Security Rider

Last Updated: January 29th, 2024

Background: This contract Data Security Rider (the "Rider") must be added to all contracts with any service provider (also known as "Vendor" or "data processor"), that in connection with its services creates, obtains, accesses (via records, systems, or otherwise), receives from or on behalf of the University of Cincinnati ("UC"), or uses in the course of its performance of the contract, any UC Covered Data and Information (hereinafter defined). Vendor agrees to the terms of this Rider.

Definitions:

Covered Data and Information (CDI) includes any and all nonpublic paper, digital, or electronic UC data supplied by UC or any individuals to Vendor. CDI is a broad category of nonpublic UC data that includes, but is not limited to:

- Social Security numbers,
- Credit card numbers, data protected by the Payment Card Industry Data Security Standard (PCI DSS), or other financial account information (collectively, "PCI Data"),
- Data protected by the Family Educational Rights and Privacy Act, as set forth in 20 U.S.C. § 1232g ("FERPA"),
- Data protected by the Gramm-Leach-Bliley Act ("GLBA"), Public Law No: 106-102, and
- Any other sensitive data as defined by UC or protected by any other applicable federal or state law or regulation.

If UC's Protected Health Information ("PHI") as defined by the Health Information Portability and Accountability Act of 1996 ("HIPAA") is being accessed, a Business Associate Agreement, not a Data Security Rider, is required. Contact UC's Director of Privacy for assistance.

Compliance with Law and Security Standards: Vendor shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically

maintained or transmitted CDI received from or on behalf of UC or any individuals. Vendor must supply documentation of compliance with any applicable laws and regulations upon request. All of Vendor's systems and activities undertaken in performance of the service provided to UC for collecting, storing, accessing, processing, and/or sharing CDI must comply with federal, state and local laws concerning data privacy, the latest version of National Institute of Standards and Technology Publication 800-171, or the International Organization for Standardization and the International Electrotechnical Commission 27002 (ISO/IEC 27002), or comparable frameworks, and where applicable, the laws of other countries including, but not limited to, the European Union's General Data Protection Regulation ("GDPR"). Vendor agrees that UC may determine the scope, purposes, and manner by which the CDI may be collected, accessed and/or processed, or shared by Vendor. Vendor shall collect, access, process, and/or share the CDI only as set forth in UC's written instructions.

Payment Card Industry:

Additionally, if the Payment Card Industry Data Security Standard ("PCI-DSS") is applicable to the services provided to UC, Vendor agrees to:

- Store, transmit, and process UC's PCI Data in scope of the PCI DSS in compliance with the latest version of PCI DSS; and
- Attest that any third-party providing services in scope of PCI DSS under this Rider shall store, transmit, and process UC PCI Data in scope of the PCI DSS in compliance with the PCI DSS; and
- Provide either proof of PCI DSS compliance or certification (from a recognized third-party security auditing firm), within 10 business days of the request, verifying Vendor and any third party who stores, transmits, or processes UC PCI Data in scope of PCI DSS as part of the services provided under this Rider maintains ongoing compliance under PCI DSS as it changes over time; and
- Store, transmit, and process any UC PCI Data in scope of the PCI DSS in a manner that does not bring UC's network into PCI DSS scope; and
- Attest that any third-party providing services in scope of PCI DSS under this Rider shall store, transmit, and process UC PCI Data in scope of the PCI DSS in a manner that does not bring UC's network into PCI DSS scope.

Audits: Vendor shall agree to undergo regular security audits, preferably by certified third parties, occurring at least annually, and any identified issues must be resolved within 90 days of the audit report. UC may demand written proof of the occurrence of such audits at any time during the term of the contract to which this Rider is added.

AICPA SOC Report (Type II)/per SSAE18: Vendor must provide UC with its most recent Service Organization Control ("SOC") audit report and that of all subservice provider(s) relevant to the underlying contract. It is further agreed that the SOC report, which will be free of cost to UC, shall be provided to UC annually, within 30 days of its issuance by the auditor. The SOC report should be directed to the appropriate representative identified by UC. Vendor also commits to providing UC with a designated point of contact for the SOC report, addressing issues raised in the SOC report with relevant subservice provider(s), and responding to any follow up questions posed by UC in relation to the SOC report

Data Security: All Vendor systems and applications shall undergo vulnerability assessments, such as testing patch level, password security, and application security in accordance with industry best practices, and Vendor shall provide reports to UC upon request if such assessments are conducted by a third party.

- Routine security, operational, and performance event monitoring shall be performed by Vendor; Vendor shall immediately identify and remediate events related to unauthorized activity and unauthorized access. Vendor agrees to provide all logs upon request by UC, and Vendor shall cooperate with UC, government authorities, and law enforcement during incident investigations. All services collecting, storing, accessing processing, and/or sharing CDI must utilize secure communication and storage methods, encryption in transit and at rest using commercially supported encryption solution in accordance with the latest version of Federal Information Processing Standards Publication (FIPS) Publication 140-2, role-based access control, least privilege, sensitive data obfuscation, and use a certificate from an approved independent authority.

Vendor agrees to allow the use of UC single sign-on ("SSO") solution (or comparable authentication mechanism with UC approval) if and when appropriate as requested by UC.

Physical Facilities: Physical access to Vendor facilities where CDI is stored, whether production or backup, must be restricted and reside within the continental United States.

Any damage or unauthorized access to Vendor facilities, systems, or data housing CDI must be reported to UC within 72 hours of identifying the security incident. If any unauthorized access to CDI occurs, Vendor must consult with UC officials before notifying those parties or individuals affected by the unauthorized access of CDI.

Data Storage and Backup: All CDI must be backed up on a regular basis, at least every 24 hours, and backups tested and encrypted in accordance with the latest version of Federal Information Processing Standards Publication (FIPS) Publication 140-2. Vendor shall disclose to UC the backup type, cadence, and testing schedule upon request. Vendor shall notify UC of any changes to the backup services provided by Vendor prior to enacting such changes.

Access to CDI: Vendor acknowledges that the Rider allows Vendor limited access to CDI as set forth in the underlying contract and for the sole purpose of Vendor's performance of the services. Access to CDI shall be limited to those with a "need to know" and controlled by specific individual(s). If required by U.S federal or state law, at no time will CDI be accessible to a non-U.S. person or foreign national, as required by law. Vendor must have procedures and solutions implemented to prevent unauthorized access, and the procedures will be documented and available for UC to review upon request.

Responding to Individuals Regarding Data Privacy Rights: Vendor shall, without delay, refer to UC any individual requests concerning data privacy rights and shall not respond directly, unless otherwise required by law.

International Data Transfers: Vendor shall rely on a valid transfer mechanism to transfer personal data for processing (whether performed by Vendor or by a sub-contractor) from the European Economic Area to another country.

Third-Party Subcontracting: Vendor shall ensure that all data protection obligations imposed on Vendor under this Rider shall be imposed upon any sub-contractor through written agreement. Notwithstanding any agreement between Vendor and its sub-contractor, Vendor shall remain fully liable to UC as set forth in this Rider for the performance of the obligations with respect to CDI collected, stored, accessed, processed or shared under any sub-contractor agreement. Vendor shall indemnify, defend, and hold UC (and its officers, employees, trustees, directors, and agents – together with UC, the "UC Indemnitees"), harmless from and against all claims and suits of any kind ("Claims") and all resulting damages, judgements or other losses (including attorneys' fees) (collectively, "Damages") resulting from Claims against UC based on strict liability in tort, negligence, breach of expressed or implied warranties, or infringement of intellectual property, or use of CDI, to the extent arising from or caused by Vendor's performance under an agreement with UC or Vendor's use of CDI under this Rider.

Retention, Return or Destruction of CDI: Unless otherwise agreed by Vendor and UC in writing, upon termination, cancellation, expiration or other conclusion of the Agreement, Vendor shall promptly return to UC all CDI in a mutually agreed upon

format or, if return is not feasible, destroy any and all CDI. Destruction of CDI shall be carried out in accordance with UC's data retention policies. UC shall approve the method and timeline of data destruction prior to destruction. If Vendor destroys CDI, Vendor shall provide UC with a certificate confirming the date and method of destruction.

Unauthorized Disclosures, Re-Use or Misuse of Covered Data and Information: Vendor agrees to hold CDI in strict confidence. Vendor shall not use or disclose CDI received from or on behalf of UC (or any individuals) except as permitted or required by the underlying contract, as required by law, or as otherwise authorized in writing by UC. Vendor agrees not to use CDI for any purpose other than the purpose for which the disclosure was made. CDI shall not be distributed, repurposed or shared across other applications, environments, or business units of Vendor. Vendor further agrees that no CDI of any kind shall be revealed, transmitted, exchanged or otherwise provided to other vendors or interested parties except on a case-by-case basis as specifically agreed to in writing by UC. Vendor agrees to provide all logs upon request by UC, and Vendor shall cooperate with UC, government authorities, and law enforcement during incident investigations.

Reporting an unauthorized disclosure or misuse of data: Vendor shall, within 72 hours of discovery, report to UC any potential or actual access or disclosure of CDI not authorized by this Rider or otherwise authorized in writing by UC. Vendor's report shall identify:

- The nature of the unauthorized potential or actual access or disclosure,
- The CDI used or disclosed,
- Who made or received the potential or actual unauthorized disclosure,
- Vendor's completed or planned response to mitigate any deleterious effect of the unauthorized potential or actual access or disclosure,
- The corrective action Vendor has taken or shall take to prevent future similar unauthorized potential or actual access or disclosure, and
- Vendor shall provide such other information, including a written report, as reasonably requested by UC.

Remedies: If UC reasonably determines in good faith that Vendor has materially breached any of its obligations detailed herein, UC, in its sole discretion, shall have the right to (a) require Vendor to submit a plan of monitoring and reporting, (b) provide Vendor with a 15 day period to cure the breach, or (c) terminate the underlying contract between the parties immediately if cure is not possible or if UC, in its sole discretion, does not believe Vendor is able to meet its continuing obligations detailed herein. Before exercising any of these options, UC shall provide

written notice to Vendor describing the violation and the action it intends to take. Vendor shall indemnify, defend and hold UC harmless from all claims, liabilities, damages, or judgments involving a third party, including UC's costs and attorney fees, which arise as a result of Vendor's failure to meet any of its obligations detailed herein. Nothing in this paragraph limits any other remedies available to UC.

Note: Inclusion of CDI provided by individuals into the terms of the Rider will depend upon the contract and may not be needed.