Vendor Information Security Exhibit

The Ohio State University Wexner Medical Center ("OSUWMC") maintains information ("OSUWMC Data"). OSUWMC Data includes, but is not limited to, patient, staff and customer identifying information, patient demographics, patient medical information, patient medical insurance and third party payor information, credit card information, employee demographics, OSUWMC financial information, and other proprietary information.

1. Vendor agrees to maintain an Information Security Program ("ISP") made up of policies, procedures, technical and organizational safeguards, and training designed to protect OSUWMC Data against unauthorized loss, destruction, alteration, access or disclosure.

2. Vendor hereby acknowledges that all OSUWMC Data, including information from OSUWMC's information systems, is confidential and the property of OSUWMC. Vendor shall cause any and all OSUWMC Data to be kept in strict confidence and not disclose or release to any other person or entity.

3. Vendor shall not use or disclose OSUWMC Data received from or on behalf of OSUWMC except as appropriate to perform the services under the Agreement; as required by law, order, regulation, rule, industry standard, subpoena or other legal or administrative process; or as otherwise authorized in writing by OSUWMC. Vendor agrees to require this same compliance in any of its subcontractor or agency agreements related to this underlying transaction.

4. Security Standards. Vendor represents, warrants and covenants, as applicable, that its ISP protects OSUWMC Data by implementing an industry security and privacy standard and including, at minimum:

i. **Network Security.** Vendor maintains network security that includes network firewall provisioning, intrusion detection, network device logging and alerting, and vulnerability scans on externally facing systems in accordance with industry standards.

i. **OSUWMC Data Security.** Vendor complies with applicable standards governing the patch management criticality rankings and patching time frame requirements for its systems and applications including, but not limited to, switches, routers, appliances, servers, workstation PC's, commercial software, and open-source software.

ii. **OSUWMC Data Transmission.** Vendor implements secure transmission protocols such as SFTP, SSH, TLS/SSL, and HTTPS when transmitting sensitive OSUWMC Data.

iii. **Identity and Access Management.** Vendor implements access standards designed to authenticate users, permit authorized access to OSUWMC Data, maintain segregation of duties, and revoke access as part of employee termination or transition.

iv. **OSUWMC Data Storage.** Vendor maintains appropriate policies, procedures, and controls reasonably designed to secure OSUWMC Data stored by Vendor, its employees, and its suppliers. Vendor or its employee mobile devices, portable or laptop computing devices, or portable media that stores OSUWMC Data shall use appropriate encryption designed to reduce the risk of compromise or misuse.

v. **Return or Destruction of OSUWMC Data.** Vendor maintains a record retention policy that determines how records are retained, managed, stored and, where appropriate, destroyed. Vendor also agrees it will erase, destroy, and render unreadable, all OSUWMC Data according to the standards enumerated in DOD 5015.2 or NIST 800-88rl, as amended. Where appropriate, Vendor will maintain a record of destruction, shared with OSUWMC, for all types of OSUWMC Data in its possession. Since certain information cannot be erased or deleted from electronic systems, Vendor maintains the confidentiality of all retained information until such time as the information is destroyed.

vi. **Resiliency.** Vendor maintains appropriate and effective business continuity and disaster recovery plans to ensure resiliency of OSUWMC Data and business operations.

vii. **U.S. Storage.** All OSUWMC Data shall be stored in the United States.

viii. **Privacy.** Vendor maintains a privacy policy, which includes, at minimum, processes for accessing, correcting, and requesting deletion of personal information. If required by law, regulation, rules or industry standards to fulfill the terms of the Agreement, Vendor will implement processes to obtain individual's consent and requests to opt out. Vendor may not transfer to third parties (unless pursuant to the requirements of the Agreement, and third party uses the OSUWMC Data only for the requirements of the Agreement) or sell, market, or sublicense OSUWMC Data, even in de-identified or anonymized format, or re-identify OSUWMC Data that has been de-identified.

ix. **Notification of Network or Data Breach.** Vendor shall immediately report in writing to OSUWMC any network breach and/or use or disclosure of OSUWMC Data not authorized by the Agreement, including any reasonable belief that unauthorized access to or acquisition of the OSUWMC Data has occurred. Vendor shall make the report to OSUWMC at security@osu.edu not more than two (2) business days after Vendor reasonably believes there has been such unauthorized use or disclosure. Vendor's report shall identify: (1) the nature of the unauthorized use or disclosure; (2) the network element(s) and/or OSUWMC Data used or disclosed; (3) who made the unauthorized use or received the unauthorized disclosure; (4) what Vendor has done, or shall do, to mitigate any negative effect of the unauthorized disclosure; and (5) what corrective action Vendor has taken, or shall take, to prevent future unauthorized use or disclosure.

x. **Security Risk Assessments**. OSUWMC reserves the right to perform audits of Vendor's ISP as necessary. OSUWMC will provide its request in writing and will work with Vendor to schedule time to conduct the audit.

xi. Vendor agrees to provide reports from third party security assessments, or to allow OSUWMC to conduct a security assessments to certify the Vendor's ISP. Vendor agrees to meet with OSUWMC to discuss any noted deficiencies from such an assessment and reasonably treat them in a mutually agreed time frame based upon risk severity. Vendor agrees to annual security assessments of its security practices to ensure any deficiencies have been fully addressed and that such security practices continue to meet the terms and requirements herein. The security assessments will occur during normal business hours and at a mutually agreed-upon time. Each party will be responsible for its own costs related to the security assessments.

5. Vendor shall comply with all applicable laws, regulations, rules and industry standards that require the notification of individuals in the event of unauthorized release of personally identifiable information, any other event requiring such notification ("Notification Event"). OSUWMC may, in its sole discretion, choose to provide notice to any or all parties affected by a network or data breach, but Vendor shall reimburse OSUWMC for the cost of providing such notification. Vendor further agrees to provide, or to reimburse OSUWMC for its costs in providing, any credit monitoring or similar services that are necessary as a result of Vendor's network or data breach.

6. Both parties agree that any breach of the confidentiality obligations of this Agreement will result in irreparable damage for which there is no adequate remedy at law. Therefore, it is agreed that OSUWMC shall be entitled to equitable relief, including an injunction enjoining any such breach by any court of competent jurisdiction. Such injunction shall be without prejudice to any other right or remedy to which OSUWMC may be entitled, including damages. Vendor hereby agrees to defend, indemnify and hold OSUWMC, its officers, agents, and employees harmless from any and all claims, suits, demands, awards and judgments for personal or bodily injury resulting from any disclosure of OSUWMC Data by Vendor or by Vendor's agents or employees to any third party in violation of the terms of this Exhibit. The terms of this paragraph shall survive termination of this Agreement.

7. Vendor agrees to notify OSUWMC immediately of any violation of this Exhibit, including the misuse or unauthorized disclosure of any OSUWMC Data. Vendor shall be deemed to have knowledge of a violation if such violation is known, or by exercising reasonable diligence would have been known, to any person, other than a person involved in the violation, who is a workforce member, subcontractor, or agent of Vendor.

8. Vendor agrees that OSUWMC may immediately terminate this Agreement and deny Vendor access to OSUWMC's facilities and information systems without notice whenever OSUWMC, in its sole opinion, has determined that Vendor, its agents, or employees has violated any of the provisions of this Exhibit. In the event of such termination, Vendor agrees that OSUWMC shall not be liable to Vendor for any damages resulting from Vendor's inability to access facilities or information within OSUWMC information systems. The obligation to maintain the confidentiality of the OSUWMC Data survives the termination of this Agreement.

9. If either party becomes legally compelled by law, process or order of any court or governmental agency to disclose any OSUWMC Data, that party shall notify the other, if legally permitted, so that it may seek a protective order or take other appropriate action.

(rev. 8/30/2021)