Vendor Compliance with Identity, Medical and Financial Information Security Agreement

The Ohio State University Wexner Medical Center ("OSUWMC") maintains confidential patient, staff, faculty and customer information as well as confidential business information ("OSUWMC Confidential Information"). This Confidential Information 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 comply with OSUWMC's Information Security Standard or other comparable industry security framework and/or standards. Vendor and its employees shall maintain the necessary security arrangements to prevent the theft or unauthorized disclosure of OSUWMC's Confidential Information received or accessed in any form.

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

3. Vendor agrees to access and use OSUWMC Confidential Information only for the purpose(s) for which vendor is granted permission. Vendor agrees not to access, use, share or disclose any data or other OSUWMC Confidential Information obtained from the OSUWMC's information systems to any third party, other than those employees of the Vendor with a need to know in the performance of this Agreement, without the prior written permission of OSUWMC.

4. For vendors having access to any OSUWMC electronic data, the following Information Security Standards will apply:
   a. **Data in Use**. Vendor agrees to maintain secure computing environments that are up to date with all appropriate security patches. Vendor agrees to monitor, respond to and log all access and access attempts to OSUWMC data. Vendor also agrees that within 30 days after termination of this Agreement, it shall certify that it will erase, destroy, and render unreadable, all OSUWMC Confidential Information according to Vendor's retention schedules, and the standards enumerated in DOD 5015.2 or NIST 800-88rl, as amended, and that until such time that the Confidential Information is erased, destroyed, and rendered unreadable, the Confidential Information shall retain its confidential nature.

   b. **Data in Motion**. Vendor agrees at all times to maintain network security that at a minimum includes: network firewall protection, intrusion detection/prevention and regular vulnerability scanning and penetration testing. Any and all transmission or electronic exchange of OSUWMC data shall take place via secure encrypted transmissions such as HTTPS or FTPS.

   c. **Data at Rest**. Vendor agrees that any and all OSUWMC data will be stored, processed, and maintained solely on designated servers and that no OSUWMC data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that storage medium is encrypted using no less than 128 bit encryption key.

   d. **Security Risk Assessments**. Vendor agrees to provide reports from third party security assessments, or to allow OSUWMC to conduct random security assessments to certify the Vendor has adequate security controls and practices that meet the above standards. 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. 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 Confidential Information by Vendor or by Vendor's agents or employees to any third party in violation of the terms of this Agreement. The terms of this paragraph shall survive termination of this Agreement.

6. Vendor agrees to notify OSUWMC immediately of any violation of this Agreement, including the misuse or unauthorized disclosure of any OSUWMC Confidential Information. 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.

7. 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 Agreement. 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 Confidential Information survives the termination of this Agreement. Upon termination of this Agreement, all OSUWMC Confidential Information accessed shall either be returned to OSUWMC or destroyed, and certified in writing as such.

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