EXHIBIT __

OMEGA HEALTHCARE MANAGEMENT SERVICES

VENDOR SECURITY REQUIREMENTS ADDENDUM

This Vendor Security Requirements Addendum ("Addendum") is incorporated into and made a part of the vendor services agreement ("Agreement") between OMH-HealthEdge Holdings Inc. dba Omega Healthcare Management Services ("Omega") and [insert legal name] signing the Agreement ("Vendor"). Capitalized terms not defined in this Addendum are defined elsewhere in the Agreement. In the event of any conflict between the terms of this Addendum and any other documents comprising the Agreement, the terms imposing the greater security obligation on Vendor control.

1. **Scope.** This Addendum applies to (a) the access to, collection, receipt, production, storage, use, analysis, alteration, or transmission of, or other operation or set of operations performed on, information that identifies or is identifiable to an individual ("Personal Information") that is provided to or received by Vendor and its personnel, contractors and/or agents of any kind ("Personnel") from or on behalf of Omega, its clients, and/or other confidential or proprietary information of Omega and/or its clients (including Personal Information, "Omega Confidential Information") in electronic form (collectively any of such activities described in this Section 1(a) are "Processing"), or (b) any access by Vendor to the computer network, computers or communications systems of Omega or its affiliates or third parties contracting with either of them ("Covered Systems"). The term "including" herein means by example and not limitation.

a. **International Data Protection Regulation**. Vendor and Omega agree that Omega may have customers that provide data that triggers application of the GDPR, UK GDPR, Brazil LGPD, Colombia Data Protection Law, or Philippines Data Privacy Act, Vendor shall ensure compliance with GDPR, UK GDPR, India data protection laws, Colombia Data Protection Law, or Philippines Data Privacy Act, as applicable. For purposes of this Agreement, "GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); "UK GDPR" means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018; ""Colombia Data Protection Law" means Colombia Law 1581 of 2012 and its Regulatory Decrees; and "Philippines Data Privacy Act" means the Philippines Data Privacy Act of 2012 (Republic Act No. 10173) and its Implementing Rules and Regulations.

b. **U.S. Data Protection Regulation**. If the Services involve the creation, transmission, retention, deletion, use, disclosure, or processing of personal information as that term or similar term is used under applicable federal or state privacy law to describe personally identifiable information linked or reasonably linkable to a natural person subject to the law's protection ("Personal Information"), then Vendor will comply, and will require that its personnel and subcontractors comply, with all applicable requirements of the relevant federal or state privacy law, including but not limited to the obligations set forth in this Agreement. Vendor shall immediately notify Omega if, after the Effective Date, Vendor is unable to meet the requirements of any applicable federal or state privacy law.

c. **Personal Information Use and Security**. Vendor shall only use Personal Information, for the limited and specified purposes provided in this Agreement. As between Omega and Vendor, Personal Information is Confidential Information of Omega. Vendor shall implement and use appropriate administrative, physical, and technical safeguards, including any safeguards set forth in an applicable SOW, to protect the confidentiality, integrity, and accessibility of Personal Information and prevent the unauthorized use or disclosure of Personal Information.

d. **Personal Information Incident Reporting**. Vendor shall take reasonable and appropriate steps to stop, mitigate and remediate the unauthorized use of Personal Information by Vendor, its

subcontractors, or Affiliates, and shall grant Omega, upon notice, the right to take reasonable and appropriate steps to stop, mitigate and remediate the unauthorized use of Personal Information. Vendor agrees, without unreasonable delay and in any event on or before forty-eight (48) hours of Vendor's discovery, to notify Omega of any incident that involves an unauthorized acquisition, access, use, destruction, disclosure, or processing of Personal Information obtained by Vendor from Omega, even if Vendor believes that the incident will not rise to the level of a breach under applicable law. Vendor's notification shall include, to the extent reasonably available, and shall be supplemented on an ongoing basis with: (i) the identification of all individuals whose Personal Information was or is believed to have been involved; and (ii) all other information reasonably necessary to provide notice to individuals that are the subject of the Personal Information and any other entity, regulatory body, or office entitled to receive such notice. Vendor shall cooperate with Omega's efforts to take reasonable and appropriate steps to identify, mitigate, and remediate the root cause of such incidents. Notwithstanding the foregoing, without limiting in any way any other remedy available to Omega at law, equity, or contract, Vendor shall (i) conduct an investigation of any incident required to be reported under this Section, and (ii) provide, and/or pay the costs of providing, the required notices as set forth in this Section. In the event the parties determine it is necessary for Omega to conduct an investigation hereunder in lieu of Vendor, Vendor will reimburse and pay Omega for reasonable costs and expenses Vendor incurred that arise from such investigation. In the event the parties determine it is necessary for Omega to provide the required notices set forth herein in lieu of Vendor, Vendor will reimburse and pay Omega for all costs and expenses Vendor incurred in providing such notices. To the extent Vendor is sending out the notices required hereunder, Vendor shall obtain Omega's written approval of such notices, which notice Omega will not unreasonably withhold or delay, before Vendor sends the required notices.

2. **Operational Provisions.**

a. **Adequate Safeguards.** Vendor will maintain a comprehensive security program under which Vendor documents, implement and maintain adequate physical, technical and operational safeguards to ensure the security, confidentiality and integrity of Omega Confidential Information and its use of Covered Systems consistent with good industry practices for leading U.S. healthcare information technology providers ("Industry Practices"). This requirement applies to all of the provisions of this Addendum and nothing herein limits or restricts the provisions of this Section.

b. **Data Centers.** Each data center in which Vendor locates any of the equipment comprising Vendor's Network will meet the Uptime Institute's standards for a Tier III data center. Each such data center will employ Industry Practices, including physical security, and redundant power, cooling and connectivity.

c. **Audit.** The processes and procedures of Vendor relating to the security, integrity and confidentiality of Personal Information and other Omega Confidential Information stored, processed, analyzed and transmitted to and from Vendor will be subject to a SOC 2 Type II audit with appropriate control objectives, conducted by an auditing firm of national repute on an annual basis. The audit report for each such audit will reveal no material deficiencies, and Vendor will provide a copy of each audit report, and any audit or management letter or other communication from the auditor noting any deficiencies promptly after receipt by Vendor. Without excusing any material deficiency and without limiting the remedies of Omega therefor, if any material deficiencies are identified in any such audit, Vendor will promptly cure all such deficiencies and provide written notice of such cure to Omega.

d. Infrastructure Protection. Service Provider shall maintain industry standard controls to protect Vendor Processing Resources, and maintain its computer and communications network (including all elements and components thereof, physical, logical and otherwise, and including the third party systems and services used by Vendor, "Vendor's Network") in accordance with Industry Practices, including at a minimum the following:

1. **DLP Policy**. Data loss prevention mechanisms designed to segment, monitor, restrict, and prevent Omega Information from moving data to unauthorized internal or external network locations.

2. Router filters, firewalls, intrusion detection and prevention systems, and other network mechanisms to restrict access to the Vendor Processing Resources, including, without limitation, all local site networks that may be accessed via the Internet (whether or not such

sites transmit information);

3. Resources used for mobile access to Omega Information Systems shall be protected against attack and penetration through the use of firewalls, malware detection/prevention, and encryption;

4. **Detection and Monitoring**. Processes to prevent, detect, and eradicate malicious code (e.g., antivirus applications) and to notify Omega of instances of malicious code detected on Vendor Processing Resources that may affect Omega Information or Omega Information Systems; and

5. **Patch Management**. Processes to ensure Vendor Processing Resources have patches applied without undue delay, and operating systems or applications which no longer are supported by the original equipment manufacturers are not used to support Services.

6. **Acceptable Use Policy.** In connection with its performance of Services, Vendor will comply with any acceptable use policy of Omega provided in writing by Omega. Vendor will maintain and enforce an appropriate acceptable use policy for Vendor's Network, and such policy will be consistent with any Omega acceptable use policy provided under this Section.

7. **Virus Scanning.** Vendor will maintain appropriate network and host based intrusion detection systems protecting Vendor's Network to identify any computer virus, worm, Trojan, Ransomware, timebomb, logic bomb, backdoor, exploit, keylogger, timer, infector, instruction, routine, rootkit, surveillance software, disabling code, or other malware or malicious code intended to or that does cause the computers or systems of Vendor, Omega or any third party to fail to act properly or to function in an unintended manner or permit unintended access to such computers or systems by any person, computer or process.

8. **Portal Security**. Service Provider shall implement and maintain the following portal security controls for all web/mobile applications that interact with or contain Omega Information: (a) Multi-factor Authentication; (b) BOT activity monitoring of the environment (monitoring and logging tools); (c) Risk Based Authentication (Time of day, Geo location, device and browser information, user information etc.); and (d) User access must be strictly "need-to-know".

9. **Security Patches.** Vendor will install all security patches and updates to the operating systems, firewalls, virus scanning software and other hardware and software comprising Vendor's Network as follows with respect to vulnerabilities rated by CVSS, EPSS, or inclusion in the CISA Known Exploited Vulnerability (KEV) catalog, or other Industry Practice, as follows, and will use Industry Practices to address such vulnerabilities until an appropriate patch or update is installed: (i) critical, immediate or urgent vulnerabilities, within 48 hours, (ii) high vulnerabilities, within 1 week, (iii) medium vulnerabilities within 30 days.

10. **Monitoring Tools and Utilities.** Vendor will use appropriate monitoring software to monitor Vendor's Network and identify failures in Vendor's Network elements and automatically create trouble tickets for such failures. Vendor will maintain all appropriate logs to track use of Vendor's Network and access to Personal Information.

11. **IDs and Passwords.** Each person accessing Vendor's Network will have a separate ID, with access authorization appropriate to that person's role. Passwords will be required to be strong passwords according to Industry Practices. An ID will be canceled immediately upon termination of the person's employment or similar relationship with Vendor. An ID for Omega staff will be canceled immediately upon notification from appropriate Omega contact to Vendor. Log will be provided to Omega contact regarding termination of Omega Staff from Vendor system indicating date & time of termination. Passwords will be required to be changed at least every six (6) months.

12. **Databases.** To the extent Vendor maintains any database containing Personal Information or other Omega Confidential Information, Vendor will maintain such database in good operating condition using properly skilled database administrators.

13. **Segregation.** Except as agreed by Omega in writing in advance, Vendor will segregate Omega Confidential Information in separately identifiable database(s) solely to contain Omega Confidential Information and not to be mixed with any third party confidential information.

14. **Logging.** Vendor will maintain a log of all access to databases containing Personal Information or other Omega Confidential Information.

15. **Access.** Vendor will restrict access to databases containing Personal Information or other Omega Confidential Information to persons authorized by Vendor based on their role and responsibilities.

16. **Data Encryption.** Omega Confidential Information will be encrypted while in transit within, from or to Vendor's Network, and while at rest in Vendor's Network. Encryption will use encryption standards meeting Industry Practices.

17. **Policies.** Vendor will maintain, train and enforce appropriate policies regarding the use of Vendor's Network and its components. Without limitation, such policies will include the following:

18. **Minimum Necessary.** Processing of Omega Confidential Information will be limited to the minimum, including the minimum personnel, reasonably necessary for performance by Vendor of Services and compliance with its obligations under the Agreement.

19. **Authorized Personnel.** Vendor will limit access to Omega Confidential Information to those personnel whose roles require such access to perform Services, and Vendor will terminate such access immediately upon a person ceasing to require such access whether because of termination, leave of absence, role change or otherwise. Vendor will perform appropriate background checks, including monthly OIG, SAM and OFAC checks, on each person authorized to access any Omega Confidential Information or to have any access to Omega network, and no person whose background check reveals any crime, fraud, dishonesty, or other illegal, wrongful or unethical behavior, or any debarment or ineligibility to participate in or perform services for any government program, will be authorized to perform Services for Omega or to have any access to Omega Confidential Information or Omega's network.

20. **Multi-Factor Authentication.** Vendor will require multi-factor authentication for any access through Vendor's Network to Omega Confidential Information or to Omega network, including media, applications, operating systems and equipment, and including other third-party access.

21. **Passwords and Password Policy.** Each user of Vendor's Network will not share IDs and passwords or permit anyone else to log on with the user's ID and password. Vendor will maintain an updated and appropriate password policy that provides for appropriate delays or lockouts against repeated incorrect log on attempts.

22. **Privileged Access.** Vendor will limit privileged access to the minimum number of users, systems, services and other connections to and within Vendor's Network, and all of such access will include multifactor authentication or other validation mechanisms.

23. **Portable Devices.** Personal Information will not be stored on any laptop, smartphone, thumb drive, flash drive or other portable electronic device (collectively, "Portable Devices"). Any Portable Device used to access any Omega Confidential Information will be fully encrypted and secured.

24. **Destruction.** When Vendor is required to destroy Omega Confidential Information, whether under the Agreement or by applicable law, Vendor will ensure that such Omega Confidential Information is permanently deleted so that it cannot be recovered from the media on which it was stored. When hardware is destroyed by Vendor, Vendor will have the hardware destroyed in a secure and confidential manner to ensure that no Omega Confidential Information is accessible or recoverable from such hardware. Certification of Destruction will

be provided specific to destruction of any Omega hardware, software, or data. Certificate will include date, time, specific item, and signature of responsible individual for destruction.

25. **Compliance with this Addendum.** Vendor will ensure that its Personnel comply with this Addendum.

26. **Sanctions.** Vendor will maintain and enforce reasonable sanctions for personnel violating its policies relating to Vendor's Network, including the Omega Confidential Information therein, and including any breach of this Addendum.

27. **Training.** Vendor will train its personnel on its policies relating to Vendor's Network and ensure that they are fully informed as to their responsibilities relating to Vendor's Network, including the Personal Information therein.

28. **Compliance.** Vendor will maintain an effective compliance and ethics program as defined in the U.S. Sentencing Guidelines and that meets the requirements of all other applicable Laws.

3. **Vendor Contact.** Vendor will provide a single point of contact for privacy and incident issues relating to Vendor's Network, and such contact has the authority to represent Vendor in connection with this Addendum.

4. **Subcontracts.** Vendor will ensure that each contract it enters into with its suppliers and contractors has terms consistent with this Addendum such that each will in performing for Vendor comply with the terms of this Addendum. Vendor is responsible for ensuring that each supplier and contractor complies with the provisions of this Addendum applicable to Vendor. Vendor will from time to time audit its suppliers and contractors to confirm their compliance with their obligations to Vendor, and will document the results of each such audit and maintain such results in its books and records. At Omega request, Vendor will provide a list of its suppliers and contractors and information relating to their compliance with the terms of this Addendum.

5. **Trouble Ticketing System.** Vendor will maintain an electronic trouble ticketing system to track problems arising from or relating to Vendor's Network. To the extent set forth in the Agreement, Vendor will provide trouble tickets in an agreed electronic format.

6. **Offshoring.** No Omega Confidential Information will be Processed, Stored, or Transferred outside the United States without the advance written consent of Omega for the specific location and Processing to occur outside the United States. If Omega consents to the Processing of Omega Confidential Information outside the United States, the Parties will agree on a written offshore plan for each specific location to provide sufficient protections for such offshored Omega Confidential Information and to comply with applicable Law, and Vendor will comply with the provisions of that plan.

7. **Hard Copy Materials.** Vendor will maintain all paper and other hard copy materials containing Omega Confidential Information in locked storage containers with access restricted to those personnel needing to review such materials in accordance with this Addendum. When destruction is required under the Agreement, Vendor will destroy all paper and other hard copy materials containing Omega Confidential Information through a confidential shredding process ensuring that the materials are shredded into sufficiently small pieces that they cannot reasonably be reassembled.

8. **Legal Compliance.** Vendor will comply with all laws, regulations, and other binding government and judicial requirements ("Laws") applicable to it, Vendor's Network and the Omega Confidential Information therein, including all federal, state and local Laws regarding privacy and security of Personal Information. Vendor will work cooperatively with Omega to satisfy requirements of applicable Laws, including those that address third party information security.

9. **Security Incident and Breach Response.**

a. Vendor represents that in the last 5 years, to its knowledge after reasonable inquiry, there has not been any breach of the security of Vendor's Network or involving Vendor's systems, computers, Personal Information or other electronic information in its systems or under its control or direction.

b. Vendor will maintain, operate and enforce an appropriate policy regarding security incidents and security breaches as follows:

i. Vendor will maintain a security incident and event management system that provides real time analysis of security alerts generated by Vendor's Network, including logging and alarming.

ii. Vendor will have an appropriate plan to respond to security incidents to identify threats and address them in accordance with the provisions of the Agreement, and to avoid and address any attempted ransomware attack.

iii. Vendor will provide written notice to Omega by email to legal@omegahms.com and compliance.QA@omegahms.com within forty-eight (48) hours of any actual or reasonably suspected breach of security, confidentiality or privacy ("Security Breach") of Personal Information or other Omega Confidential Information either through Vendor's Network or of hard copy materials.

iv. Vendor will appropriately respond to any Security Breach to identify the Personal Information and other Omega Confidential Information that has been or may have been subject to the Security Breach, including preparing and submitting for approval by Omega a breach response plan meeting the requirements of applicable law, Industry Practices, and the Agreement, and upon such approval, which will not be unreasonably withheld or conditioned, implementing that plan; provided that Omega will have the right to approve in advance any communications to individuals whose Personal Information may be subject to the Security Breach.

v. Omega may participate as an observer in any discussions with regulatory authorities regarding any Security Breach hereunder.

vi. Vendor will employ all appropriate measures to mitigate the adverse effects of the Security Breach, subject to the approval of Omega.

10. **Disaster Recovery and Business Continuity.** Vendor will maintain a disaster recovery and business continuity plan sufficient to recover after a disaster all material features, functions and performance of Vendor's Network with a recovery time objective ("RTO") and recovery point objective ("RPO") appropriate to meet Vendor's obligations under the Agreement. If not otherwise set forth in the Agreement, the RPO will be four (4) hours and the RTO will be twenty four (24) hours. The RTO is the time it takes to recover and the RPO is the maximum period immediately preceding the disaster in which data and system changes might be lost because of the disaster. Vendor will test its disaster recovery and business continuity plan on an annual basis to demonstrate its ability to recover Vendor's Network in the event of a disaster in accordance with the applicable RTO and RPO. Vendor will provide Omega advance notice of such test and permit Omega to observe such test, and at Omega request, provide written results of each such test.

11. **Certifications.** Vendor will during the term maintain any certifications set forth in the Agreement. Any failure or material deficiency identified in any such certification is a breach of the Agreement. Vendor will promptly notify Omega by email to compliance.QA@omegahms.com if it fails to achieve any certification relating to Vendor's Network or its Processing of Personal Information or other Omega Confidential Information, including providing the written notice of failure from the certifying entity, and such other documentation regarding such failure as is requested by Omega.

12. **Testing.** Vendor will on an annual basis test its compliance with this Addendum, including conducting a commercially reasonable vulnerability and penetration test attempting logical penetration of Vendor's Network and testing the resistance of Vendor's Network personnel to social engineering (phishing) activities. Vendor will provide reasonable advance notice to Omega by email to compliance.QA@omegahms.com of each test hereunder, and permit Omega to observe such test if it so desires.

13. **Audits.** Vendor will notify Omega by email to compliance.QA@omegahms.com in advance of any audit or inspection of Vendor's Network by any third party, and except for audits by other customers of

Vendor, Omega will have the right to observe such audit or inspection and to receive a copy of any report of such audit or inspection.

14. **Responses.** Vendor will timely and accurately respond to surveys, questionnaires and other information, inspection and audit requests from Omega regarding Vendor's Network, Vendor's compliance with this Addendum and Vendor's practices and activities relating to Vendor's Network and Omega Confidential Information.

15. **Insurance.** Vendor will maintain at its own expense liability insurance covering Vendor and Omega for response costs, identity protection services, claims, losses, liabilities, judgments, settlements, lawsuits, regulatory actions, and other costs and damages arising out of Vendor's failure to protect Omega Confidential Information and perform under this Addendum, with limits of coverage as set forth elsewhere in the Agreement, or if not, then with a limit of at least $5 million per occurrence.

16. **Secure Software Development.** Vendor will not provide to or make available for use by Omega any software that has not been developed in accordance with secure development Industry Practices, including (a) scanning all code for passwords, keys, certificates and other secrets, third party code, and vulnerabilities and defects, (b) using a secure repository for the management of all code, and (c) performing appropriate testing and quality review of code to identify and remedy any material defects or failure to meet Vendor's obligations under this Addendum and the other portions of the Agreement.

17. **Artificial Intelligence.** Vendor will provide notice to Omega in writing in advance any use of any engineered, machine-based or software-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations or decisions influencing real or virtual environments, or that is otherwise considered artificial intelligence under applicable law or industry standards (each is an "AI Tool") in connection with its performance under the Agreement. Before Vendor materially changes any AI Tool or its use under the Agreement, it will provide notice describing each material change. Omega shall have the right to terminate the Agreement as a result of the use of the AI Tool should it be determined that such AI Tool violates any existing or future-enacted governing laws or regulations relating to the protection of the Personal Information.