



Date March 2024

Request for Proposal: Diabetic Retinal Screening Solution

Table of Contents

1	General Overview	2
1.1	UMMS Corporate Overview	2
2	Vendor Response	2
2.1	Confidentiality Statement.....	2
2.2	Guidelines & Contact Information.....	2
2.3	Submission Requirements	2
3	Selection Process	3
3.1	Key Dates and Activities.....	3
	Appendix A: Past Performance Questionnaire	4
	Appendix B: About UMMS.....	5
	Appendix C: Vendor Data Security Addendum.....	6
	Appendix D: Insurance Coverage Requirements	12
	Appendix E: Provider’s Disclosure	14
	Appendix F: UMMS Business Associate Agreement 9/21/2017	15

1 General Overview

The University of Maryland Medical System (UMMS) is soliciting proposals for a Diabetic Retinal Screening solution.

1.1 UMMS Corporate Overview

UMMS was created in 1984 when the state-owned University Hospital became a private, nonprofit organization. It has since evolved into a multi-hospital system with academic, community and specialty service missions, reaching every part of the state and beyond. As one of the largest private employers in the state, the health system's 29,000+ team members and 4,500+ affiliated physicians provide primary and specialty care in more than 150 locations and at 13 hospitals across the state of Maryland. Please see [Appendix D](#) for more information about UMMS.

2 Vendor Response

2.1 Confidentiality Statement

Respondents must treat any information received from UMMS as privileged and strictly confidential, including information about our networks, computer systems, staff, care givers or other aspects of the business. Please note that UMMS and its affiliates are not responsible for time, effort, or costs expended to respond to this request. There are no contractual obligations until a contract is signed.

Selected vendor will be required to sign a Business Associated Agreement, must be HIPAA compliant, maintain HIPAA compliance, and submit to an UMMS Onboarding process that may include a security and compliance assessment.

2.2 Guidelines & Contact Information

All questions regarding the RFP should be directed to erika.munoz@umm.edu no later than 5:00 PM Eastern Standard Time (EST) on the date specified in the Key Dates and Activities section.

Questions will all be answered in writing and distributed to all invited vendors.

Beyond this, you may **not** contact UMMS employees, board members or trustees, subcontractors, agents or affiliates regarding this RFP without the express prior written approval of UMMS. Any respondent that attempts to contact any UMMS personnel directly during this period will be in violation of this restriction, and may be disqualified.

2.3 Submission Requirements

In order to be considered for selection, potential vendors must submit a complete response to this RFP by completing and submitting all three parts of the response. Parts One, Two and Three of the response must be submitted **electronically** no later than 5:00 PM Eastern Standard Time (EST) than the date specified in the Key Dates and Activities section of this document. Proposals received after the deadline will not be considered or reviewed. Proposals are to be submitted via email to the contact in [Guidelines & Contact Information](#) section above. UMMS emails will not be able to accept attachments totaling 10MB or higher. UMMS emails will not accept ZIP files.

In order to facilitate the analysis of responses to this RFP, **vendors are required to follow the outline and instructions below when preparing their proposals**. Proposals should be prepared as simply as possible and provide a straightforward, concise description of the vendor's capabilities to satisfy the requirements of this RFP. As closely as is possible, please follow the sequence of information requested below. Emphasis should be concentrated on accuracy, completeness, and clarity of content. All parts, pages, figures, and tables should be numbered and clearly labeled.

UMMS reserves the right to have the final authority in the design and implementation of the project.

Each part of the response must have:

- **Title Page** – that should include: the Request for Proposal subject, the name of company, address, telephone number, e-mail address, name of contact person and date.
- **Table of Contents** - Clearly identify material provided by section and page number.
- **Response Requirements**- respond to the requirements in the following excel spreadsheet.



Diabetic Retinal
Screening RFP Excel F

3 Selection Process

UMMS will evaluate all vendor responses. A multi-department, UMMS team will review all information submitted. Upon completion of the review, you may be asked to provide an in-depth presentation. Please note that the University of Maryland Medical System and its affiliates are not responsible for time and effort expended to respond to this request. There are no contractual obligations until a contract is signed.

Bidders to this RFP must agree to treat any information they are given about UMMS, including information about their networks, computer systems, staff, care givers or other aspects of the business, as privileged.

3.1 Key Dates and Activities

Activities	Dates
RFP Announcement	March 20, 2024
Questions to UMMS Due	March 26, 2024
RFP Responses Due to UMMS	April 10, 2024
Demonstration Presentations	May 2024
Selection and Notification	Summer 2024

Please note that above dates are subject to change by UMMS depending on organizational priorities. Response due date changes will be communicated through the same method as publishing the RFP, although timeline for decision may be subject to change without notice.

Responses may be submitted via email to Erika.munoz@umm.edu by 5:00pm Eastern time on date noted above. At that time, the RFP will be closed to responses. Respondents can expect an emailed acknowledgement of receipt within an hour of receipt (during business hours) on the due date. Please watch for this acknowledgement email, if you don't receive this acknowledgment, your response may not be received by the deadline. UMMS emails will not be able to accept attachments totaling 10MB or higher or .zip files for security reasons.

Appendix A: Past Performance Questionnaire

The vendor must complete three to five (3-5) past performance questionnaires (PPQ). Sub-contractors must also complete PPQs per [Part 2: Past Performances](#). UMMS reserves the right to contact references listed in PPQs.

Past Performance Questionnaire # :		
Name of Organization that performed work:		
Name of Organization for which work was performed and location		Corporate Phone Number
Point of Contact (full name and title)	Contact E-mail	Contact Phone Number
	Implementation Start Date (dd/mm/yyyy)	Implementation End Date (dd/mm/yyyy)


1. Description of Onboarding.

Please indicate whether the client was on boarded on time and on budget? Describe how project changes were handled if any were encountered?

2. Description of Scope of Services Provided.

3. Description of Vendor's Responsibilities.

Appendix B: About UMMS



UNIVERSITY of MARYLAND MEDICAL SYSTEM

FACTS

University of Maryland Medical System (UMMS) delivers comprehensive health care services throughout Maryland. UMMS physicians and patient care teams work hand-in-hand with University of Maryland School of Medicine specialists to provide primary, urgent, emergency and specialty care at more than 150 locations across the state. The UMMS network includes academic, community and specialty hospitals that together provide 25% of all hospital-based care in Maryland.

UMMS Member Organizations

University of Maryland Medical Center (UMMC) is the flagship academic medical center at the heart of UMMS and includes the 739-bed downtown Baltimore campus and the 201-bed midtown campus one mile north. The medical staff comprises more than 1,500 attending physicians who are faculty members at the University of Maryland School of Medicine, as well as more than 950 residents and fellows in all medical specialties. UMMC is home to the Marlene and Stewart Greenebaum Comprehensive Cancer Center, the R Adams Cowley Shock Trauma Center and the University of Maryland Children's Hospital.

University of Maryland Baltimore Washington Medical Center in Anne Arundel County provides primary and specialty care, including cancer, orthopaedic, cardiac, women's, vascular and neuroscience services.

University of Maryland Capital Region Health provides primary and specialty health care in Prince George's County, Southern Maryland and the Washington metro area, and includes:

- UM Capital Region Medical Center
- UM Bowie Health Center
- UM Laurel Medical Center

University of Maryland Charles Regional Medical Center is an acute-care community hospital serving Southern Maryland.

University of Maryland Rehabilitation & Orthopaedic Institute is the state's largest rehabilitation and orthopaedic hospital, serving both adults and children.

University of Maryland St. Joseph Medical Center is a Catholic acute-care hospital in Towson, with centers of excellence in heart, cancer, orthopaedics and women's and children's services.

University of Maryland Shore Regional Health serves Maryland's Eastern Shore and includes:

- UM Shore Medical Center at Easton
- UM Shore Medical Center at Cambridge
- UM Shore Medical Center at Chestertown
- UM Shore Emergency Center at Queenstown

University of Maryland Upper Chesapeake Health serves Northeast Maryland and includes:

- UM Upper Chesapeake Medical Center
- UM Harford Memorial Hospital

Mt. Washington Pediatric Hospital in Northwest Baltimore is a pediatric rehabilitation hospital operated as a joint venture by UMMS and Johns Hopkins Medicine.

University of Maryland Physician Network is a group of physicians and advanced practice providers that offer primary care and specialty services throughout Maryland. UMMS-affiliated practices provide expert care across all specialties, including primary care, pediatrics, women's health, orthopaedics, neurology and neurosurgery, heart and vascular care and more. A trusted partner of University of Maryland Faculty Physicians Inc., UM Physician Network is focused on providing high-quality, patient-centered care.

University of Maryland Urgent Care provides walk-in care, pre-operative testing, vaccinations and other ambulatory services at 10 locations in Maryland, coordinating with the UMMS network and other providers across the state.




QUICK NUMBERS

12	Hospitals
2,458	Licensed Beds
27,413	Employees*
5,500	Active Medical Staff Members**

FISCAL 2022 FIGURES***

100,985	Hospital Admissions
1,230,086	Outpatient Visits
329,547	Emergency Visits
68,520	Outpatient Surgical Cases
\$4.86 Billion	Annual Revenue

* Includes employees of UMMS member organizations plus corporate staff
** Approximate, across all medical centers and including residents and fellows
*** FY 2022 figures are unaudited.

umms.org

Appendix C: Vendor Data Security Addendum

This Vendor Security Addendum (“Addendum”) dated concurrently with the underlying Master Purchase Agreement to which this Addendum is attached (the “Effective Date”) is by and between University of Maryland Medical System Corporation, a Maryland non-stock corporation with its principal office located at 250 West Pratt Street, 24th Floor, Baltimore, MD 21201 (“Customer”), for itself and on behalf of its Affiliates and the undersigned vendor (“Vendor”). This Addendum amends and forms part of that certain Master Purchase Agreement between Vendor and Customer dated concurrently with this Addendum (“Agreement”). Capitalized terms used but not defined will have the meanings set forth in the Agreement.

1. Vendor Data Security Program Overview.

- 1.1. Vendor shall implement and maintain administrative, physical and technical safeguards that prevent any unauthorized use or disclosure of, or access to, Customer’s Confidential Information. Such safeguards shall include, without limitation, an information security program (the “Vendor Data Security Program”) designed to:
 - 1.1.1. ensure the security and confidentiality of Customer Confidential Information;
 - 1.1.2. protect against any anticipated threats or hazards to the security or integrity of Customer’s Confidential Information;
 - 1.1.3. protect against unauthorized access to or use of Customer’s Confidential Information; and
 - 1.1.4. comply with data protection laws for Confidential Information retained on Vendor’s and Customer’s systems.
- 1.2. The Vendor Data Security Program shall include, without limitation:
 - 1.2.1. adequate physical security of all premises in which Customer’s Confidential Information will be processed and/or stored;
 - 1.2.2. reasonable precautions with respect to the employment of and access to Confidential Information granted to Vendor Personnel, including background checks and security clearances that assign specific access privileges to individuals; and
 - 1.2.3. appropriate network security protections.
- 1.3. Vendor shall update the Vendor Data Security Program as necessary to comply with changes in federal, state, and local laws and regulations pertaining to the privacy and security of Customer’s Confidential Information.
- 1.4. Upon written request by Customer, Vendor shall provide independent third-party evaluation of the efficacy of the Vendor Information Security Program. This evaluation must be based on at least one of the following compliance standards: (1) SSAE 16; (2) SOC 1 and SOC 2 reports; (3) HITRUST certification; (4) NIST certification; (5) Vendor’s statement of security standards; (6) evidence that Vendor’s Personnel have received HIPAA training; and (7) other documentation or information as reasonably requested by Customer.

2. Security Assessments by Vendor.

- 2.1. Vendor’s Security Program shall provide for regular assessment of the risks to the security of Confidential Information, the Customer Systems or to Vendor’s, or any third party’s systems.
- 2.2. On an annual basis, Vendor shall provide Customer with an independent third-party information security report prepared in accordance with an industry benchmark such as: NIST 800-53, NIST CSF, MARS 2.0, HIPAA, HITRUST, PCI, ISO, or SOC.

3. Security Assessment by Customer.

- 3.1. Vendor shall perform an independent third-party security assessment at least annually and vendor shall share the report with the customer.
- 3.2. Findings not mitigated during this assessment shall be documented in a Plan of Action and Milestone document. A detailed POAM document shall be shared with the customer in which all findings should be addressed in a reasonable time frame.
- 3.3. Customer and Vendor shall work together in good faith to address and implement reasonable corrective actions. However, notwithstanding anything contained herein to the contrary, Customer shall have the right to terminate the Agreement in the event that Vendor cannot or does not, in Customer's sole and reasonable discretion, address and correct such concerns.

4. Vendor Data Security Program Elements. The Vendor Data Security Program shall include the following elements. Vendor shall provide Customer with documentation evidencing compliance with these requirements upon request.

- 4.1. Background Checks, Drug Screening and Training. Prior to assigning any Personnel to positions in which they are expected to have access to Confidential Information. Vendor shall provide documentation or evidence of employees receiving the necessary Background Checks, Drug Screening and security training to safeguard customer data in accordance with industry best practices. All personnel processing, transmitting, and storing customer confidential data must receive appropriate security training in data security and data governance policy.
- 4.2. Personnel Security. Vendor must notify their Human Resources and IT department of Vendor Personnel transfers or terminations, including sub-contractors and/or third-party Personnel within 24 hours of departure.
 - 4.2.1. Vendor must immediately notify Customer Human Resources and IT Security Team of Vendor Personnel who are to be terminated or transferred for misconduct. Notification should be communicated by phone call and email not less than 1 hour following Vendor Personnel termination or transfer for cause/misconduct to ensure all Customer technology, credentials, authenticators, and badges have been disabled.
 - 4.2.2. Vendor must establish requirements including roles and responsibilities for Personnel, including sub-contractors and third-party providers.
 - 4.2.3. If Vendor has access to Customer-managed infrastructure, Vendor agrees to comply with Customer personnel security policies and procedures.
- 4.3. Vulnerability Scans. Vendor shall perform internal and external host/network vulnerability scans at least quarterly and after any material change in the host/network configuration, and suspected or substantiated IT security or privacy incidents.
- 4.4. Security Event Logs. Security event-related logs must be preserved and be available online for a minimum of two (2) years and available offline for six (6) years. Logs should be stored in a secondary location, and shall have tamper resistant mechanisms in place to protect the integrity of the logs from malicious users. This requirement applies to the data sources that are capable of logging data that can be used to enforce accountability, detect a violation of security policy, detect an attempt to exploit vulnerabilities, and/or detect compromises resulting in losses of integrity, confidentiality and availability of Confidential Information, environments, services, systems, and applications. Customer reserves the right to monitor event logs accordingly.
- 4.5. Password Requirements. At a minimum, passwords must be unique and exclusive, at least 8 characters in length, changed at least every ninety (90) days, and must include at least three of the following character types: numeric, upper and lower case letters, and special characters (!@#\$\$%, etc.). Passwords associated with privileged user ids (such as those with administrator/root access privileges) and service accounts (used for machine to machine communications with no humans involved in providing the authentication at time of log in or job submission) must expire within

- 365 days. The minimum password length for privileged user IDs is 12 characters and 16 characters for service accounts.
- 4.6. Access and Authorization. Vendor will employ physical and logical access control mechanisms to prevent unauthorized access to Customer's Confidential Information and/or Customer Systems and shall limit access to Personnel with a business need to know. Such mechanisms will have the capability of detecting, logging, and reporting access to Customer Systems and Confidential Information, as well as, actions taken while accessing Customer Systems and/or information.
- 4.6.1. Each person must have an individual account that authenticates the individual's access to Confidential Information. Vendor must not allow sharing of accounts.
- 4.6.2. Vendor will utilize two-factor authentication for network access/VPN. Vendor will not use e-mail for providing authenticator information to Personnel.
- 4.6.3. Vendor will revoke Personnel's access to physical locations, systems, and applications that contain or process Confidential Information within twenty-four (24) hours of the cessation of such Personnel's need to access the system(s) or application(s) or immediately if warranted or requested by Customer.
- 4.6.4. Vendor will notify Customer of any Vendor Personnel transfers or terminations, including sub-contractors, who possess Customer credentials and/or badges within 24 hours of the decision to transfer or terminate.
- 4.6.5. Vendor shall maintain the principle of least privilege for user accounts, computing processes and privilege accounts allowed to access customer Confidential information. Vendor shall revoke all access for personnel who no longer need access.
- 4.7. Documentation. Vendor must maintain current, accurate, and complete documentation on overall system, network, and application architecture, data flows, process flows, and security functionality for all applications that process or store Customer's Confidential Information.
- 4.8. Data Transmission and Storage. Vendor shall have security controls in place to prevent its employees, agents, or subcontractors from downloading, extracting, storing, or transmitting Confidential Information through personally owned computers, laptops, personal digital assistants, tablet computers, cell phones, or similar personal electronic devices.
- 4.9. Change Management. Vendor will employ an effective and documented change management program. This includes logically or physically separate environments from production, development and testing. No Confidential Information will be transmitted, stored or processed in a non-production environment.
- 4.10. Network Security. Vendor will deploy appropriate firewall, intrusion detection/prevention, and network security technology in the operation of the Vendor's systems and facilities.
- 4.11. Malicious Code Protection. All workstations and servers must run anti-virus software. Virus definitions must be updated within twenty-four (24) hours. Vendor will have current anti-virus software configured to run real-time scanning of machines on a regularly scheduled interval not to exceed seven (7) calendar days. Vendor will scan incoming content for malicious code on all gateways to public networks including email and proxy servers.
- 4.12. Encryption. Vendor will encrypt, using industry standard encryption tools that meet the NIST's FIPS 140-2, AES 256 or TLS 1.2 or higher requirements, all Confidential Information that Vendor: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or storage media, and (iii) stores on portable devices or within the Vendor System.
- 4.13. Vulnerability Management. Vendor shall have a vulnerability scanning tool to scan internal and external facing assets. The tool shall be used to operate Vendor's vulnerability management program.
- 4.14. Penetration Testing. Vendor shall test the security of its assets, systems and software used to store, process, transmit or maintain Confidential Information as frequently as necessary to confirm that system integrity and security are consistent with current leading industry accepted standards and practices. Vendor is responsible for and shall conduct penetration testing of its own products, assets, systems and software to identify and remediate vulnerabilities in its own environment and to

communicate identified vulnerabilities and remediation steps to Customer based on current leading industry accepted penetration testing approaches. Vendor shall provide Customer penetration test results summary as it relates to assets that store, process, transmit or maintain Customer's Confidential Information.

4.15. **Business Continuity and Disaster Recovery.** Vendor shall have BC and DR plans to identify all critical assets that process, transmit, and store company confidential data. The BC and DR plan must be tested and monitored to ensure the effectiveness of its safeguards, controls, systems, and procedures. The Plan shall have essential missions and business functions, and their associated contingency requirements.

4.16. **Maintenance.** Vendor shall keep and maintain appropriate logs of all maintenance carried out on the system directly or indirectly impacting customer confidential information. Security Impact Analysis should be performed before and after any changes in the configuration of a software, hardware, or process that might affect the confidentiality, integrity or availability of customer data.

5. **PCI Compliance.** Vendor acknowledges that to the extent it is responsible for the security of the credit, debit or other cardholder payment information it processes, and hereby represents and warrants that it will comply with the most current PCI Standard in connection with the processing of such data, including, but not limited to: (a) creating and maintaining a secure network to protect cardholder data; (b) using all technical and procedural measures reasonably necessary to protect cardholder data it maintains or controls; (c) creating and implementing security measures to limit access to cardholder data; (d) monitoring access to cardholder data it maintains or controls; and (e) creating and implementing an information security policy that assures employee compliance with the foregoing. Vendor acknowledges that it is responsible for maintaining compliance with the then-current PCI DSS requirements and monitoring the PCI DSS compliance of all associated third parties Vendor may provide with access to cardholder data.

6. **Subcontractors.** Vendor shall conduct appropriate due diligence on any subcontractors that will access Confidential Information or Customer Systems to ensure such subcontractors can meet the requirements set forth in this Exhibit. Vendor shall include substantially similar terms and conditions as specified in this Exhibit in all contracts with subcontractors that access Confidential Information or Customer Systems.

7. **Security Breach.**

7.1. Vendor will notify Customer without undue delay, but no later than within 48 hours, upon learning of any suspected or actual accidental or unlawful destruction, loss, alteration, misuse, unauthorized disclosure of or access to Customer's Confidential Information in its possession (a "Security Incident").

7.2. In the event of a Security Incident, Vendor shall take immediate steps to remedy the Security Incident at Vendor's expense in cooperation with Customer and in accordance with applicable law, and shall immediately notify Customer by email [to compliance@umm.edu](mailto:to_compliance@umm.edu).

7.3. Such notice shall include a full description of the Security Incident, as well as the name and contact information for a primary security contact within Vendor. Vendor agrees to fully cooperate with Customer in Customer's handling of the matter, including without limitation any investigation, reporting or other obligations required by applicable law or regulation, or as otherwise required by Customer, and will work with Customer to otherwise respond to and mitigate any damages caused by the Security Incident.

7.4. Vendor shall not notify any third party, other than Vendor's agents and/or vendors who are subject to the obligations of confidentiality to Vendor, of the Security Incident without Customer's prior, written authorization. Vendor shall reimburse Customer for all costs and expenses incurred in responding to and/or mitigating damages caused by a Security Incident.

7.5. Notwithstanding the provisions of this Section 7, the parties agree that breaches of Protected Health Information shall be governed by the terms of the Business Associate Agreement (Exhibit 1).

8. Cooperation, Audit, and Inspection.

Vendor agrees that if Customer identifies vulnerabilities or technology practices within Vendor's information systems that in Customer's reasonable opinion or generally accepted information security practices, poses an unacceptable ongoing risk to Customer, then Vendor will remediate the vulnerabilities or technology practices and describe compensating or mitigating controls. This remediation will include the creation of a timeline mutually agreeable to both parties, not more than 30 days for a vulnerability or practice that is reasonably classified as critical or severe, and not more than 90 days in other circumstances. If an unacceptable ongoing cyber security risk is identified, the Vendor bears the cost of such remediation. For the avoidance of doubt, Vendor's failure to comply with this Section 8 or any other Section of this Addendum shall constitute a material breach of the Agreement.

9. Return and Destruction of Data.

9.1. Within ten (10) days of termination of the Agreement or if requested by Customer, Vendor shall provide a copy of all Confidential Information in a format specified by Customer at no cost.

9.2. Vendor shall permanently delete all Confidential Information from its systems and destroy all physical copies of Confidential Information stored at its facilities as requested by Customer. Upon request, Vendor shall provide a certification signed by an officer of the corporation that all Confidential Information was destroyed. The certification shall specify the method and/or tools used to delete the files.

9.3. Notwithstanding the foregoing, the parties agree that the return and destruction of Protected Health Information shall be governed by the Business Associate Agreement between the parties.

10. Survival. The provisions of this Exhibit shall survive termination of the Agreement for as long as the Vendor has Confidential Information in its possession.

IN WITNESS WHEREOF, the parties hereto, through their duly authorized designees, have executed this Addendum as of the Effective Date.

VENDOR

**UNIVERSITY OF MARYLAND MEDICAL
SYSTEM CORPORATION**

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Appendix D: Insurance Coverage Requirements

Insurance Coverage Requirements. Provider shall maintain the following insurance:

Workers' compensation and employers' liability insurance:

Workers' compensation – statutory

Employer's Liability - each employee \$1,000,000 BI by accident
each employee \$1,000,000 BI by disease

Commercial general liability insurance on an occurrence form, with minimum limits of coverage of:

\$3,000,000 annual aggregate

\$1,000,000 each occurrence

\$1,000,000 bodily injury and property damage each occurrence

\$1,000,000 personal injury and advertising injury each occurrence

\$1,000,000 products/completed operations

Business automobile liability insurance with combined single limit of \$1,000,000.

Umbrella liability insurance on an occurrence form with minimum limits of five million dollars (\$5,000,000).

Professional liability insurance with minimum limits of coverage of \$1,000,000 per occurrence and \$3,000,000 annual aggregate.

Cyber/Network Security Liability insurance covering liability arising from or out of the Service provided under this Agreement with limits of \$5,000,000 per occurrence and \$5,000,000 annual aggregate. Coverage shall include, but not be limited to, the following: Internet and network liability (providing protection against liability for system attacks; denial or loss of service; introduction, implantation, or spread of malicious software code; and unauthorized access and use), infringement of privacy or intellectual property rights (excepting patent infringement), internet advertising and content offenses, defamation, errors or omissions in software and/or systems development, implementation and maintenance, and privacy liability (providing protection against liability for the failure to protect, or wrongful disclosure of, private or confidential information).

Purchaser as Insured. Purchaser shall be named as an additional insured on each of said policies, and a certificate of such insurance shall be issued to Purchaser with a thirty (30) day cancellation notice.

Certificate. The insurance requirements contained herein are not subject to changes in, or modifications of, coverage, forms and/or limits without written prior approval by Purchaser. Provider shall provide Purchaser with certification, by a properly qualified representative of the insurer that Provider's insurance complies with the requirements of this Section. The certificate evidencing the amount and type of insurance shall be sent to Purchaser upon request.

Insurer Requirements. All required insurance policies shall be issued by companies who hold a current policyholder's alphabet and financial size category rating of not less than an A - (X) according to Best's insurance reports. Insurance shall be at the sole expense of the Provider.

Provider's Failure to Obtain Required Insurance. Should Provider fail to adhere to the requirements of this Section, Purchaser may order any such insurance and charge the cost thereof to Provider, which amount shall be due and payable by Provider upon demand.

Survival. The insurance requirements shall survive the expiration of termination of this Agreement.

Appendix E: Provider's Disclosure

Date: _____

Company Name: _____

Contact Person (printed): _____

Initiative (Type of Product/Service): _____

UMMS System Contracting Contact: Name: _____

Email: _____

Consistent with Provider's obligations under Section 22.12 of the Agreement, please disclose any prior, existing or planned:

arrangements, interest or financial stake in Provider's business, that you are aware of, by any UMMS or Affiliate board member, officer, employee, member of the medical staff, contracted staff or family members of such individuals ("Covered Party").

gifts, trips, or other items of value with a total accrued value of more than \$250 provided by Provider to a Covered Party.

This disclosure shall include the nature, type, and equivalent amount of any remuneration provided to or any financial interests held by any Covered Party.

Please submit this completed attachment to Purchaser as soon as possible, but in no event later than execution of the Agreement. The initial Disclosure Form will be included as part of the Agreement. IF THERE IS NOTHING TO DISCLOSE, THEN STATE "THERE IS NOTHING TO DISCLOSE" ON THIS FORM.

Signed by: _____

Title: _____

Submit additional response, if necessary.

Appendix F: UMMS Business Associate Agreement 9/21/2017

This Business Associate Agreement (this “Agreement”), effective as of the day and year of the last signature set forth on the signature page (“Effective Date”) is entered into by and between **University of Maryland Medical System Corporation** (“UMMS”) on its own behalf and on behalf of its Affiliates, including, but not limited to, the Affiliates identified on Attachment 1 hereto (UMMS and the Affiliates are collectively and individually referred to herein as “Covered Entity”) and _____ **[Insert Name of Business Associate]** _____ (“Business Associate”) and supplements and is made a part of all agreements entered between the parties (collectively and individually referred to herein as the “Underlying Agreement”) pursuant to which Business Associate will create, receive, transmit or maintain Protected Health Information on behalf of Covered Entity (“PHI”) as that term is defined under the Health Insurance Portability and Accountability Act of 1996 including all pertinent regulations, including without limitation the Privacy, Security, Breach Notification, and Enforcement Rules, codified at 45 C.F.R. Parts 160 and 164, as amended by the Health Information Technology for Economic and Clinical Health Act, and as may be further amended in the future (“HIPAA”); and

WHEREAS, in consideration of the covenants herein, the Covered Entity and Business Associate desire to enter into this Agreement for the purpose of ensuring compliance with HIPAA.

NOW THEREFORE, in consideration of the mutual promises set forth herein, and other good and valuable consideration, the receipt, adequacy, and sufficiency of which are hereby acknowledged, the parties agree as follows:

Definitions.

The following terms used in this Agreement shall have the same meaning as those terms in HIPAA: Breach, Data Aggregation, Designated Record Set, Disclosure, Electronic PHI, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information/PHI, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. Specific definitions include:

Affiliate. “Affiliate” shall mean, when used in connection with a particular entity, any corporation, partnership, trust, joint venture, professional association or other entity, directly or indirectly controlling, controlled by, or under common control with such entity. “Control,” including “controlling,” “controlled by,” and “under common control with,” shall mean the power to direct or cause the direction of the management and policies through ownership of voting securities, by contract or otherwise of a corporation, partnership, trust, joint venture, or other entity.

Business Associate. “Business Associate” shall mean the party named above as “Business Associate” and will generally have the same meaning as the term “Business Associate” at 45 C.F.R. § 160.103.

Covered Entity. “Covered Entity” shall mean the University of Maryland Medical System Corporation and its applicable Affiliates and will generally have the same meaning as the term “Covered Entity” at 45 C.F.R. § 160.103.

Protected Health Information/PHI and Electronic Protected Health Information or Electronic PHI shall generally have the same meaning as the terms are defined at 45 C.F.R. § 160.103, but for purpose of this Agreement will be limited to the PHI created, received, transmitted or maintained by Business Associate on Covered Entity's behalf.

Scope of Use and Disclosure by Business Associate of PHI.

Business Associate may access, Use and Disclose PHI that the Covered Entity Discloses to Business Associate as necessary to perform Business Associate's obligations under the Underlying Agreement, provided:

Business Associate's Disclosure is to only its employees, Subcontractors and/or agents in accordance with this Agreement, the Underlying Agreement, and state and federal privacy and security laws;

Business Associate's access, Use or Disclosure of PHI would not violate HIPAA or if carrying out an obligation on Covered Entity's behalf, would not violate HIPAA if done by Covered Entity;

Business Associate's Use or Disclosure for any fundraising purpose must be permitted by the Underlying Agreement and HIPAA;

Business Associate will not access, Use or Disclose PHI for marketing purposes or directly or indirectly receive remuneration in exchange for PHI, except with Covered Entity's prior written consent and only as permitted by the Underlying Agreement and HIPAA; and

Business Associate makes all reasonable efforts not to access, Use, or Disclose more than the Minimum Necessary amount of PHI to accomplish the purpose of the access, Use or Disclosure.

Unless otherwise limited by this Agreement, Underlying Agreement, or HIPAA, Business Associate may:

Access and/or Use the PHI in its possession for its proper management and administration and to fulfill any legal responsibilities of Business Associate;

Disclose the PHI in its possession to a third party for the purpose of Business Associate's proper management and administration or to fulfill any legal responsibilities of Business Associate, provided, however, that the Disclosures are Required by Law or Business Associate has received from the third party written assurances that:

the PHI will be held confidentially, as required under 45 C.F.R. § 164.504(e)(4) and 164.314, and accessed, Used or further Disclosed only as Required by Law or for the purposes for which it was Disclosed to the third party;

the third party will notify Business Associate of any instances of which it becomes aware in which the confidentiality of the PHI has been Breached; and

the third party's access, Use and Disclosure of PHI are overall compliant with HIPAA.

Upon Covered Entity's request, Business Associate shall provide Covered Entity with a copy of the third party's written assurances;

Business Associate will notify Covered Entity within five (5) days of becoming aware of any instances covered under Section II.B.2(b);

Business Associate may provide Data Aggregation services if related to Covered Entity's Health Care Operations and only to the extent specifically required in the Underlying Agreement and may not Disclose Covered Entity's aggregated data in a manner that identifies Covered Entity without Covered Entity's prior written consent; and

To the extent permitted by HIPAA, Business Associate may de-identify PHI for Covered Entity but only to the extent specifically required in the Underlying Agreement and in accordance with HIPAA. Business Associate will not Disclose Covered Entity's de-identified PHI in a manner that identifies Covered Entity without Covered Entity's prior written consent.

Confidentiality Obligations. In the course of performing under the Underlying Agreement and this Agreement, each party may receive, be exposed to or acquire Confidential Information including but not limited to, all information, data, reports, records, summaries, tables and studies, whether written or oral, fixed in hard copy or contained in any computer data base or computer readable form, as well as any information identified as confidential ("Confidential Information") of the other party. For purposes of this Agreement, "Confidential Information" shall not include PHI, the security of which is the subject of this Agreement and is provided for elsewhere. The parties including their employees, agents or representatives (i) shall not disclose to any third party the Confidential Information of the other party except as otherwise permitted by the Underlying Agreement and this Agreement, (ii) only permit use of such Confidential Information by employees, agents and representatives having a need to know in connection with performance under the Underlying Agreement and this Agreement, and (iii) advise each of their employees, agents, and representatives of their obligations to keep such Confidential Information confidential. Notwithstanding anything to the contrary herein, each party shall be free to use, for its own business purposes, any ideas, suggestions, concepts, know-how or techniques contained in information received from each other that directly relates to the performance under this Agreement. This provision shall not apply to Confidential Information: (a) after it becomes publicly available through no fault of either party; (b) which is later publicly released by either party in writing; (c) which is lawfully obtained from third parties without restriction; or (d) which can be shown to be previously known or developed by either party independently of the other party.

Obligations of Business Associate. In connection with its access, Use and Disclosure of PHI, Business Associate agrees that it shall:

Access, Use or further Disclose PHI only as permitted or required by this Agreement or as Required by Law;

Use and maintain reasonable and appropriate safeguards and comply with the applicable requirements of Part C of 45 C.F.R. Part 164 and any guidance issued by the Secretary of Health and Human Services with respect to Electronic PHI, to prevent access, Use or Disclosure of PHI other than as provided for by this Agreement;

Report to the Covered Entity within five (5) business days of becoming aware of or discovering any Security Incident, Breach, and/or impermissible access, Use or Disclosure of PHI not permitted pursuant to this Agreement, the Underlying Agreement or applicable state and federal law. The content of such report shall include those elements requested by the Covered Entity, including, without limitation, (a) a brief description of the occurrence, including the date of incident, (b) a description of the type of PHI that was involved, and (c) contact information (name, phone number, email address) for a person that can assist with the Covered Entity's assessment of the incident. Business Associate shall cooperate and work with the Covered Entity as necessary to assess the incident and make timely notifications, as applicable;

Implement and follow commercially reasonable administrative, physical, and technical safeguards and security procedures to protect the confidentiality, integrity, and availability of Electronic PHI as required by the Security Rule;

To the extent practicable, mitigate any harmful effect that is known to Business Associate of an access, Use or Disclosure of PHI by Business Associate or its Subcontractors in violation of this Agreement and cooperate with Covered Entity in any mitigation or Breach reporting effort;

Ensure that any Subcontractors that create, receive, maintain, or transmit PHI, in electronic or other form, on behalf of Business Associate agree to the same restrictions, and requirements that apply to Business Associate under this Agreement and enter a contract or other arrangement that meets the requirements of 45 C.F.R. § 164.308(b)(2) and 45 C.F.R. § 164.502(e)(2), provided that this provision will not be deemed to provide Business Associate with a right to assign or subcontract its responsibilities except as provided in the Underlying Agreement;

Make available to the Secretary of Health and Human Services or to the Covered Entity on request, Business Associate's internal practices, books and records relating to the access, Use and Disclosure of PHI for purposes of determining compliance with the Privacy Rule, subject to any applicable legal privileges;

Within five (5) days of receiving a request from the Covered Entity or an Individual, Business Associate will, in the form and format requested:

Make available the PHI necessary for the Covered Entity to make an accounting of Disclosures of the Individual's PHI to the Individual, as provided under 45 C.F.R. § 164.528;

Make available PHI necessary for the Covered Entity to respond to Individuals' requests for access to PHI in a Designated Record Set that is not in the possession of the Covered Entity, if applicable;

Incorporate any amendments or corrections to the PHI in a Designated Record Set that is not in the possession of the Covered Entity, if applicable, in accordance with 45 C.F.R. § 164.526; and

Make available PHI in a Designated Record Set, if applicable, to Covered Entity, in accordance with 45 C.F.R. § 164.524.

To the extent the Business Associate is to carry out one or more of Covered Entity's obligations under HIPAA, comply with the applicable requirements under HIPAA;

Cooperate with the Covered Entity to facilitate the Covered Entity's compliance with HIPAA; and

Not send any notice or communication regarding any unauthorized access, Use or Disclosure of PHI to an Individual, the federal or any state government, or the media without prior written consent from the Covered Entity unless Required by Law.

Term and Termination.

Term. The Term of this Agreement shall commence on the Effective Date, and shall remain in effect unless termination by either party is requested and received in writing.

Termination for Breach. The Covered Entity may terminate the Underlying Agreement and this Agreement at any time if the Covered Entity determines that Business Associate has breached a material term of this Agreement. Alternately, the Covered Entity may choose to provide Business Associate with notice of the existence of a breach of a material term of this Agreement and afford Business Associate an opportunity to cure the material breach. In the event Business Associate fails to cure the breach to the satisfaction of the Covered Entity, the Covered Entity may immediately thereafter terminate the Underlying Agreement and this Agreement.

Effect of Termination. Upon termination of the Underlying Agreement or Agreement, Business Associate will return (or if agreed to by Covered Entity, destroy) all PHI created, received, maintained or transmitted by Business Associate on behalf of the Covered Entity in any form and retain no copies of such PHI.

Notwithstanding the foregoing, if such return or destruction is not feasible, Business Associate will notify Covered Entity in writing. Said notification shall include: (i) a statement that Business Associate has determined that it is not feasible to return or destroy the PHI in its possession, and (ii) the specific reasons for such determination. Upon mutual agreement of the parties that return or destruction of PHI is infeasible, Business Associate may maintain PHI after termination, provided that Business Associate will extend the protections of this Agreement and applicable law to the PHI, including those specific to Electronic PHI, and limit further access, Uses and Disclosures to those purposes that make the return or destruction of the PHI infeasible.

If it is infeasible for Business Associate to obtain, from a Subcontractor or agent, any PHI in the possession of the Subcontractor or agent, Business Associate must provide a written explanation to Covered Entity detailing the type of PHI in the Subcontractor or agent's possession and the reasons it is not feasible to return or destroy such PHI and require the Subcontractors and agents to agree to extend any and all protections, limitations and restrictions contained in this Agreement and applicable law to the Subcontractors' and/or agents' Use and/or Disclosure of any PHI retained after the termination of this Agreement, and to limit any further Uses and/or Disclosures to the purposes that make the return or destruction of the PHI infeasible.

This Section IV.C shall survive termination or expiration of this Agreement and the Underlying Agreement until such time as all PHI has been returned or otherwise properly destroyed.

Insurance, Indemnification and Limitation of Liability.

Insurance. Business Associate will procure and maintain in effect during the term of this Agreement: (1) general liability insurance coverage with minimum limits of \$1 million per event and \$3 million annual aggregate; (2) as applicable, professional liability insurance coverage and/or professional errors and omissions, within minimum limits of \$1 million per event and \$3 million annual aggregate; (3) workers' compensation insurance coverage within statutory limits of state law in which Business Associate is located; (4) Network security, cyber liability, and privacy breach coverage with minimum limits of \$2,000,000 per event and \$5,000,000 aggregate; and (5) umbrella liability coverage over all of the above listed policies, excluding workers compensation, with limits of \$5 million per occurrence and \$5 million annual aggregate.

Tail. If a policy listed above is claims made and is terminated for any reason, an extended reporting endorsement (commonly referred to as "tail coverage") will be procured by Business Associate to respond to any events that occurred while the policy was active but reported after the policy ended.

Survival. The insurance obligations in this Section V shall survive the expiration or termination of this Agreement for any reason.

Indemnification. Business Associate agrees to indemnify, defend and hold harmless Covered Entity and Covered Entity's Affiliates, employees, directors, officers, Subcontractors, agents or other members of its workforce from any costs, damages, expenses, judgments, losses, and attorney's fees arising from any breach of this Agreement

by Business Associate, its employees, Subcontractors and/or agents or arising from any negligent or wrongful acts or omissions of Business Associate, its employees, Subcontractors and/or agents, including failure to perform its obligations under HIPAA. Business Associate's indemnification obligation shall survive the expiration or termination of this Agreement for any reason.

Limitation of Liability.

Covered Entity shall not be liable to Business Associate for any incidental, consequential, special, or punitive damages of any kind or nature, whether such liability is asserted on the basis of contract, tort (including negligence or strict liability), or otherwise, even if Business Associate has been advised of the possibility of such loss or damages.

To the extent that Business Associate has limited its liability under the terms of the Underlying Agreement, whether with a maximum recovery for direct damages or a disclaimer against any incidental, consequential, special, or punitive damages, or other such limitations, all limitations shall exclude any damages to Covered Entity arising from Business Associate's, its employees', Subcontractors' or agents' breach of its obligations relating to the access, Use and Disclosure of PHI.

Amendment. Business Associate and the Covered Entity agree to take such action as is necessary to amend this Agreement from time to time as necessary for Business Associate and Covered Entity to comply with the requirements of HIPAA and guidance from the Secretary as they may be issued or amended from time to time.

Changes in Law. The parties recognize that this Agreement is at all times subject to applicable state, local, and federal laws. The parties further recognize that this Agreement may become subject to amendments in such laws and regulations and to new legislation, regulatory guidance and instructions and decisional law ("Change in Law"). Any provisions of law that invalidate, or are otherwise inconsistent with, the material terms and conditions of this Agreement, or that would cause one or both of the parties hereto to be in violation of law, shall be deemed to have superseded the terms of this Agreement. In such event, the parties agree to utilize their best efforts to modify the terms and conditions of this Agreement to be consistent with the requirements of such law(s) in order to effectuate the purposes and intent of this Agreement. Within thirty (30) days of a Change in Law, either party may submit to the other party proposed modifications to the terms and conditions of this Agreement in light of the Change in Law. If the parties fail to agree upon proposed modifications to the terms and conditions of this Agreement by executing a written amendment within an additional thirty (30) days, either party may, by giving the other party an additional sixty (60) days written notice, terminate this Agreement, unless it would terminate earlier by its terms. In the event a Change in Law precludes or substantially precludes a contractual relationship between the parties similar to that expressed in this Agreement, then, under such circumstances, where renegotiation of the applicable terms of this Agreement would be futile, either party may, upon at least sixty (60) days advance written notice, terminate this Agreement, unless it would terminate earlier by its terms. Upon termination of this Agreement as hereinabove provided, neither party shall have any further obligation hereunder except for (i) obligations occurring prior to the date of termination, and (ii) obligations, promises or covenants contained herein which are expressly made and intended to extend beyond the term of this Agreement.

Data Ownership. Business Associate acknowledges that it has no ownership rights with respect to PHI.

Construction of Terms. The terms of this Agreement shall be construed in light of any applicable interpretation or guidance on HIPAA and/or the Privacy Rule issued by the United States Department of Health and Human Services or the federal Office for Civil Rights from time to time.

Inconsistent Provisions. To the extent that the Underlying Agreement has any provisions inconsistent with this Agreement, the provisions in this Agreement shall prevail.

No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

Applicable Law. This Agreement shall be governed by the laws of the State of Maryland and applicable federal law.

Attorney's Fees. If any legal action or other proceeding of any kind is brought for the enforcement of this Agreement, or because of any alleged breach, default, or any other dispute in connection with any provision of this Agreement, the successful or prevailing party shall be entitled to recover all reasonable attorney's fees and other costs incurred in any such action or proceedings, in addition to any relief to which it may be entitled.

Entire Agreement. This Agreement constitutes the entire agreement between the Covered Entity and Business Associate. This Agreement supersedes all prior and contemporaneous business associate agreements or agreements between the parties.

Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed to be an original, but all of which together shall constitute one and the same instrument.

Notice. Unless otherwise directed in writing, all notices given hereunder shall be sent to the applicable addressee at the applicable address set forth beneath the signatures of the parties below.