UNIVERSITY of MARYLAND
MEDICAL SYSTEM

April 3, 2024

Request for Proposal: Reverse Access Center Software Implementation

Version 1.0

Table of Contents

1 General Overview

The University of Maryland Medical System (UMMS) is soliciting proposals for a software platform that would be utilized by care managers to coordinate patient placement in acute care facilities post discharge.

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.

1.2 University of Maryland Access Center

We are expecting to create a more efficient patient placement experience by having the visibility of open beds at skilled nursing facilities (SNF), assisted living, hospice, and acute inpatient rehabilitation facilities (IRF). This would also provide an efficient coordination of care with home health care agencies. Care managers would be able to pair patients with Post-Acute Care (PAC) providers based on payer source and preferred location. The patient referral and response would be transmitted electronically eliminating the use of paper referrals and reducing time waiting on patient placement requests. The software platform would also allow for visibility of the patient’s condition to determine which site would be best suited for their clinical needs.

2 High Level Solution Requirements

This High-Level Solution Requirements section is a narrative describing some high-level business needs. Vendor responses should address these in the format specified in Section 3.4 Part 1: Response to Requirements.

2.1 Business Objective

Implement a tracking system that would facilitate PAC referrals to Skilled Nursing Facilities (SNF), Acute Inpatient Rehabilitation Facilities (IRF), Hospice, and Home Care by centralized care coordination. Establish a care management system that would reduce referred-to-accepted time. Create an increased percentage of UMMS patients in PAC services. Reduce overcrowding in emergency departments due to gridlocked acute critical care staffed beds. A reduction in insurance denials due to increased and unauthorized lengths of stay.

2.2 High Level Requirement #1

A software platform that would assist in the reduction of avoidable bed days and administrative days.

2.3 High Level Requirement #2

The software would provide placement options to ensure patient choice compliance.

2.4 High Level Requirement #3

Data reporting that would indicate the reduction in the average length of stay (ALOS) using an efficient PAC discharge process.

3 Vendor Response

3.1 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.

3.2 Guidelines & Contact Information

All questions regarding the RFP should be directed to Wendy.Kearson@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.

3.3 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) on 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, v**endors 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.

3.4 Part 1: Response to Requirements

3.4.1 Company Profile

3.4.1.1 Provide a general overview of company history, stability, capabilities, technical expertise and management structure. Please include the organization's DUNS number and any other information relevant to describing the organization's financial stability; to include long term growth strategy. Include artifacts such as your org chart with titles and names, listings of subcontractors or vendors routinely used to deploy services included in this RFP along with how long your firm has had a relationship with them and the services/work they provide. Though not required, including a few resumes of key members of your team would be helpful. Vendor should provide: 1) an annual report and/or financial documentation (audited income statements) for the last fiscal year; 2) description of your working capital/cash position and your ability to remain viable over the period of the contract; and 3) provide details of any material changes (ownership, structure, acquisitions) in the last financial year.

3.4.1.2 Include examples of ROI and comparisons to market competitors.

3.4.1.3 If you maintain any subcontracted agreements relative to the services included in your proposal, please describe those and include the qualifications of those subcontractors.

3.4.1.4 Do you work with Value Added Resellers and/or 3rd party implementors?

3.4.2 Company Qualifications

3.4.2.1 Provide a summary statement of your firm's qualifications and experience in providing a patient referral, insurance pre-certification, and software platform. Please emphasize the qualifications, experience of the firm, and employment qualifications of your firm. Please also provide Professional Bios of your firm’s leadership, their tenure with the firm, along with other documentation outlining expertise of other staff in this field. Detail your specific experience in post-acute length of stay management, pre-certification authorization, and patient choice compliance.

3.4.2.2 Describe all individual roles who will be allocated to the UMMS account, including the customer service representative(s). How many accounts is a customer service representative expected to manage? Do they specialize in certain industries? Detail the number of representatives with urgent care experience.

3.4.2.3 Indicate the number of years the firm has provided automated care management post-acute referral assistance to healthcare entities.

3.4.2.4 Provide additional relevant information to further demonstrate the firm’s industry knowledge, credentials, certifications, etc.

3.4.2.5 Provide additional relevant information to further demonstrate the firm’s scope and breadth of resources (internal and/or external), available to the vendor.

3.4.2.6 Provide additional relevant information to further demonstrate the firm’s established record of successful automated care management post-acute referral assistance for their clients. How does your organization define successful relationships with your clients?

3.4.3 Solution/Service Description

3.4.3.1 Provide a narrative description of the solution(s) offered. Describe the components that compose your product's architecture, and indicate how each component is packaged — software, appliance, virtual appliance, as a service, etc.

3.4.3.2 Along with the overview above, in detail please describe the performance metrics you routinely monitor to analyze the success for the solution and describe any remedies taken when performance metrics are not met.

3.4.3.3 Describe in detail how the solution is most often integrated into operational workflows.

3.4.3.4 Define scalability of the solution services. Please include descriptions of how your organization adapts to changes, either from your clients’ perspective or regulatory/industry changes. Please also describe procedures for staff augmentation when issues or workload from UMMS increases higher than the routine need. Included the length of notice needed for your firm to scale support in an urgent/high volume scenario.

3.4.3.5 Feel free to include information about services you think would be useful to UMMS. Include materials to supplement sections above such as marketing collateral, executive summary of function and features, white papers regarding product specifications, implementations, and use and comparisons to market competitors.

3.4.4 Implementation/Onboarding Plan

3.4.4.1 Provide a work plan describing typical/expected implementation/onboarding plan, including durations of activities and artifacts needed at key intervals. Identify the time frame from executed contract to go live implementation date.

3.4.4.2 Outline implementation roles and responsibilities of vendor, UMMS, and any third parties and/or subcontractors. Describe roles and expertise that UMMS must make available and when for successful and quick implementation.

3.4.4.3 Should your company be awarded a contract from UMMS, discuss the feasibility and plans you suggest to have UMMS on boarded and operational with your solution by early FY 2025 (July 1 – June 30). If you are unable to meet this timeframe, please provide detailed suggestions on how to onboard UMMS.

3.4.5 Customer Support model

3.4.5.1 Describe you customer engagement model, including after-hours support and escalation procedures.

3.4.5.2 Describe customer support plan for users including escalation paths to resolve problems. Include escalation path for your teams internally as well as the escalation path for your customers.

3.4.5.3 Describe any training provided for clients to get the most value out of your services. Should you have charges for that training, please be sure to included that in the cost proposal and indicate any upper limit of attendees for that training at the amount quoted.

3.4.5.4 Are there any partners UMMS will need to utilize in order to contract with you? For example, EHR or payer portal vendors, or external post-acute care providers.

3.4.6 Technology and Security

This section is intended to serve as a general guide to facilitate initial discussion with the vendor regarding new Information Services related project requests, to obtain details about the technology, and to aid in the development of project estimates. Please provide as much information as you can for each question listed below. It is important that UMMS understands as much about your needs as possible. Note that you may be requested to complete a formal security and compliance assessment in addition to answering the questions in this section. Please answer N/A for questions that do not apply to your solution.

3.4.6.1 Do you agree to complete UMMS' vendor onboarding process including appropriate security and compliance assessments?

- Identify any current security, compliance, or technical certifications such as ISO 27001, SOC 2, HITRUST, etc. Are you willing to share evidence of certifications?
- Do you agree to remediate any lack of administrative or technical controls identified during the security/compliance assessment?
- Do you offer periodic reports confirming ongoing compliance with security requirements and SLAs?
- Do you alert your customers of significant changes like security practices and regulations or data center locations?
- What is a general timeline for Implementation (from planning to Go-Live), and what is the general timeline based on?

3.4.6.2 Describe the technical design of your solution:

- Are you providing a hardware, software, SaaS, or services-based solution, or some combination?
- Can you provide detailed technical and logical diagrams, design documents, and workflows for your solution as it will be implemented at UMMS? Will your final deliverables include a formal Solution Design Document?
- What physical or virtual hardware or software must be provided by UMMS for your solution to be implemented? For example, does your solution require UMMS network infrastructure, physical or virtual servers, mobile devices, or software and applications to function?

- Provide any applicable specifications or requirements of UMMS provided technical resources. For example, outline the number of servers required, OS, CPU, RAM and total storage requirement of each.
- If the solution utilizes mobile devices (iOS, Androids, etc.) what are the types and versions of mobile devices supported?
- What operating systems are compatible with the solution, such as Apple Mac OS X, Microsoft Windows, Linux?
- What internet browsers are compatible with the solution, such as Internet Explorer, Microsoft Edge, Mozilla Firefox, Safari, Google Chrome?
- Can CrowdStrike be installed on any on-prem systems that are part of the solution? Does the application integrate with SailPoint IDN? Can this application be virtualized in Citrix StoreFront?
- Can the application be configured to use SSO? Is it SAML compliant? Does the application provide or allow for Multi Factor Authentication?

3.4.6.3 Describe network connectivity required by your solution.

- Does the solution connect to or is it installed on hardware that is connected to UMMS' networks?
- What network connectivity is required for the solution to operate? What ports and protocols are required to connect to what resources?
- Does the solution connect to the LAN, WAN, or public internet? Is a P2P or client VPN or other secure tunnel required? What traffic will be traversing the tunnel, if required?
- Do you require access to remotely operate, support, upgrade, or update any on-prem systems? What type of access is required? For example, constant access via a VPN or infrequent escorted access?
- Is monitoring or telemetry occurring over the connection?
- If remote access is required, how will you protect that access?

3.4.6.4 Describe all access, transmission, storage, and processing of UMMS data by your solution.

- Identify the UMMS systems that will transmit, receive or integrate with your solution.
- Identify all encryption methods and levels during access, transmission, storage, or processing. Is any UMMS data not encrypted in your solution?
- Will implementation or integration with UMMS require data extraction to replace legacy systems, or will it receive data from other UMMS business systems?
- Will data be kept only in the US?
- Describe how you expect to receive discreet data from UMMS and how you plan to return discrete data, if applicable. Please be as specific as you can. If this is customizable, please provide examples of your most common methods.
- Include any experience you have integrating with Electronic Health Records (EHR), or any clinical applications, software, systems, or tools.
- Describe any API integrations or system interfaces if applicable.
- Please describe how your firm addresses changes to system interfaces or APIs. For example, if UMMS were to change the EHR system during the course of a contract.

3.4.6.5 Describe your organization’s business continuity and disaster recovery plans in the event of a planned and unplanned downtime or outage.

- Can you provide business continuity and disaster recovery plans, including backup and redundancy capabilities, restore time and restore point objectives, and notification/communications procedure in case of an outage?
- Do you have an Incident Response Plan? If so, how often do you test the plan?
- How do you manage and communicate planned downtime and maintenance activities? How do you communicate and what are your communication procedures during those events?
- Has your firm experienced any service disruptions with any of your technology and software systems? If so, please explain the scenario, implications, and resolution of the disruption.
- What are your methods for backing up our data? What are your data redundancy procedures?
- How will back-ups be performed? Who (University of Maryland Medical System [UMMS] or Vendor) is responsible for back-ups? What is the RPO and RTO for systems and data?
- How are patches, updates, and upgrades performed? Who is responsible, how are the patches applied, and at what frequency?

3.4.6.6 Describe your security program for both the solution and your organization.

- What is your approach to assessing an organization's security needs? Can you describe your team's experience and expertise in cybersecurity?
- Describe your HIPAA Security measures and any security frameworks you follow such as NIST, CISA, etc.
- Where is your data center(s), and what physical security measures are in place? Is any UMMS data maintained outside of the United States?
- Has your firm experienced any security breaches? If so, please explain the scenario, implications, and remedies for future prevention?
- Can you disable access to UMMS data immediately in the event of a breach?
- Are your digital assets monitored on a 24/7 basis for security events?
- What controls are in place to audit access?
- Describe access controls levels and associated tools. Do you provide integration with Active Directory or other repositories for role and resource groupings?
- Include information such as your solution’s approach to Active Directory integration, Multi Factor Authentication, etc, as applicable to your services.
- Describe access control procedures for (a) defining and documenting system account types that support mission/business functions; and (b) defining conditions for group and role membership.
- Describe account management processes to include (a) authorization, group/role membership, and the access request approval and fulfillment process; and (b) monitoring user accounts and system accounts on a defined interval for compliance with account management requirements.
- Describe any accounts that need to be created for the solution including user accounts, service accounts, and the privileges required.
- Explain IT Security function audit-reporting procedures for the application; documented procedures for using automated IT Security function auditing features in the application, and alerts that can be configured to trigger if audit reporting fails.

- How is an activity in the UMMS environment monitored and documented? What auditing capabilities are provided: Admin/MGMT, System Information, etc.?
- Who accesses, processes, transmits or stores UMMS information? How do you isolate and safeguard UMMS data from other clients?
- Do you offer security training programs for employees to raise security awareness?
- How do you prevent tampering with audit records including what if any roles have access to the records, what the process is to access the records, and if the records are encrypted. Who keeps and manages the encryption keys?
- What actions do you take to destroy data after it is released by a customer?

3.4.6.7 Describe your compliance program for both the solution and the organization.

- Describe your HIPAA Privacy measures.
- How do you ensure the protection of sensitive data and privacy compliance?
- Describe any experience with managing HIPAA compliance when collaborating with 3rd party vendors.
- Please provide a data traffic and interface diagram showing types of data being stored, created, received, and/or transmitted by your systems.

3.4.7 Agreements

3.4.7.1 The awarded vendor will need to accept and execute UMMS's Business Associates Agreement. Language is included as an Appendix in this document.

3.4.7.2 Should your organization require any substantial deviations from the terms/language included here, please submit that need along with your response to this RFP.

3.4.7.3 The awarded vendor will comply with the requirements of the Vendor Data Security Addendum, Insurance Coverage Requirements, and Provider's Disclosure forms (as relevant) included as an Appendices in this document.

3.4.7.4 UMMS preferred contracting term is 3 years that may be extended pursuant to written amendment signed by both parties. Exceptions may be given on a case-by-case basis with approval from IST leadership.

3.4.7.5 The awarded vendor agrees to store all confidential information provided to Provider in connection with Software and/or Services in the U.S.A.

3.4.8 Minority Participation

UMMS is committed to the participation and development of minority and women-owned business enterprises. UMMS understands the importance of developing partnerships with minority and women-owned businesses. Our ability to identify, attract and maintain alliances with the right business partners is key.

Minority/Woman-owned Business Enterprises (MWBEs) are encouraged to participate in this vendor selection process. MWBEs with letters of certification from the State of Maryland's Office of Minority Affairs, the Maryland Department of Transportation, or the MD/DC Minority Supplier Development Council, the City of Baltimore, amongst others will be considered certified.

Please provide any qualifying information.

3.4.9 Assumptions

The vendor shall describe any assumptions upon which its proposal is based, such as:

- UMMS resources required, inclusive of UMMS provided computing equipment.
- UMMS responsibilities.
- Scope of Work requirements/limitations.
- Schedule.
- If the vendor makes no assumptions, please state that.

3.5 Part 2: Past Performances

The vendor shall complete ***Appendix A: Past Performance Questionnaire*** for at least 5 to 7 organizations for which it has completed work of similar size, scope and complexity as described herein. UMMS prefers that at least two (2) past performance be for clients with similar independent member organizations, care management structure, and inpatient volumes.

If the vendor intends to subcontract any part(s) of its performance of this contract, provide at least five Past Performance Questionnaires (PPQs) relevant to the tasks the subcontractor will perform for each individual subcontractor.

UMMS reserves the right to, and will, contact references listed in PPQs.

Each completed PPQ should be no longer than 3 pages, single-spaced, Calibri 11pt font, 1-inch margins, single-sided.

3.6 Part 3: Price Proposal

The vendor shall present the total price to perform all of the requirements of this RFP. This shall include an itemized list of ALL costs associated with ownership and/or operation of the proposed solution, to include:

- Onboarding Costs
- Annual/Ongoing Fees
- Training
- Professional Services
- Vendor Travel costs expected to be paid by UMMS
- Itemization of any 3rd party costs or a list of UMMS supplied components
- Any other miscellaneous costs
- Payment terms (remittance period, etc)

In the cost proposal, please assume a contract span of a year, with opportunities to extend the contract annually. Additionally, please also describe what your firm proposes as the minimum term for optimal pricing if it is greater than one year. Include a narrative about any penalties associated with early termination. UMMS contracting standard mandates termination without cause for either party with 90 days written notice. Exceptions must be approved by UMMS Information Services & Technology leadership.

The vendor shall present costs for any additional products or services proposed for the completion of the project that were not requested. Include a list of any hardware or other items that UMMS must supply and/or any required 3rd party purchases. UMMS reserves the right to review all aspects of the Price Proposal for reasonableness and to request clarification of any proposed cost where additional information is required or the cost component shows significant and unsupported deviation from industry standards.

4 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.

4.1 Key Dates and Activities

Activities	Dates
UMMS issues Request for Proposal	4/03/2024
Bidder notifies UMMS, via email, of intent to submit proposal	4/10/2024
Written questions from prospective Providers due	4/17/2024
UMMS responses to written questions	4/24/2024
Response to RFP due	5/01/2024
Prospective Providers are scheduled to present their product to the UMAC Steering Committee & Workgroup	5/02/2024 thru 5/09/2024
UMAC Steering Committee & Workgroup submits questions for Providers if needed	5/10/2024
Providers send responses to UMAC questions	5/15/2024
UMAC Committee selects Provider(s)	5/22/2024
Providers notified in writing of UMMS' selection	5/24/2024

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 Wendy.Kearson@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 five to seven (5-7) 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)**

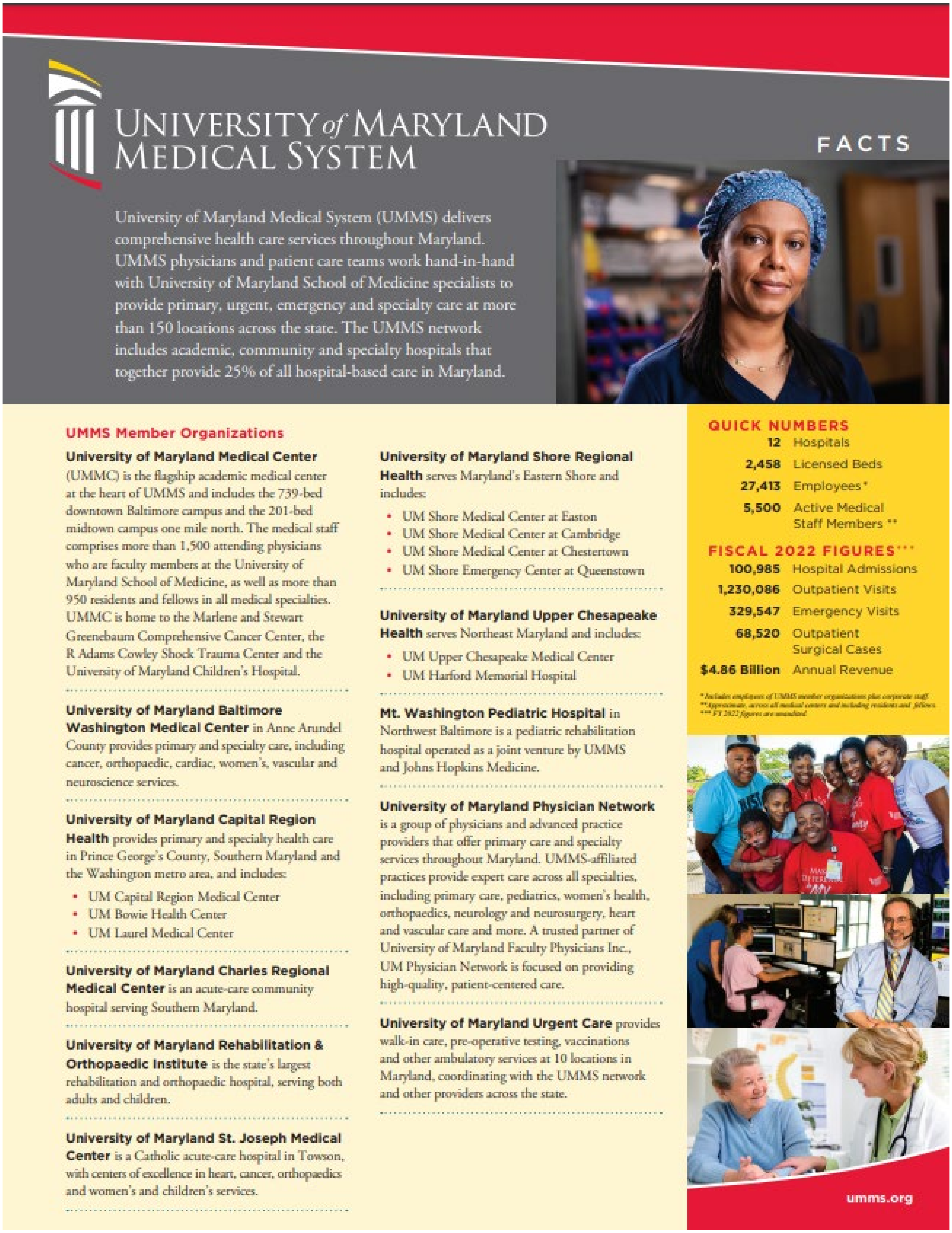
1. Description of Onboarding.

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 .

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: ______________________________________

Name: ___________________________________

Title: ____________________________________

Date: ____________________________________

By: ______________________________

Name: ____________________________

Title: _____________________________

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:

<u>Definitions</u>.

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:

<u>Affiliate</u>. "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.

<u>Business Associate</u>. "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.

<u>Covered Entity</u>. "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.

<u>Obligations of Business Associate</u>. 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.