



Date: May 19, 2023

Request for Proposal: UMMS System Intranet Selection

Table of Contents

1	General Overview.....	3
1.1	UMMS Corporate Overview.....	3
1.2	University of Maryland Marketing & Communications.....	3
2	High-Level Solution Requirements.....	3
2.1	Centralization.....	3
2.2	Interactivity.....	4
2.3	Ease of Use.....	4
2.4	Mobile Enabled.....	4
2.5	Content Management.....	4
2.6	Functionality.....	4
2.6.1	Ability to set reminders to review content on a per page/document basis.	4
2.6.2	A system calendar, customizable by entity/function/role.	4
2.6.3	Ability to embed YouTube and Vimeo videos.	4
3	Vendor Response.....	4
3.1	Confidentiality Statement.....	4
3.2	Guidelines & Contact Information.....	4
3.3	Submission Requirements.....	5
3.4	Part 1: Response to Requirements.....	5
3.4.1	Company Profile.....	5
3.4.2	Company Qualifications.....	5
3.4.3	Solution/Service Description.....	6
3.4.4	Implementation/Onboarding/Offboarding Plan.....	6
3.4.5	Customer Support model.....	7
3.4.6	Technology and Security.....	7
3.4.7	Agreements.....	8
3.4.8	Minority Participation.....	9
3.4.9	Assumptions.....	9
3.5	Part 2: Past Performances.....	9
3.6	Part 3: Price Proposal.....	9
4	Selection Process.....	10
4.1	Key Dates and Activities.....	10
	Appendix A: Past Performance Questionnaire.....	11
	Appendix B: Vendor Technology Intake Questionnaire.....	12
	Appendix C: UMMS Cloud-Based Questionnaire.....	14

Appendix D: About UMMS15

Appendix E: UMMS Business Associate Agreement 9/21/201716

1 General Overview

The University of Maryland Medical System (UMMS) is soliciting proposals for a modern employee intranet and mobile app.

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 11 hospitals across the state of Maryland. Please see [Appendix D](#) for more information about UMMS.

1.2 University of Maryland Marketing & Communications

The UMMS Marketing and Communications Department represents the “voice” of UMMS. We work to promote, strengthen and protect the reputation of our 11-hospital System through marketing to consumers and physicians, media relations, team member communications and engagement, web and social media management and much more.

We are a “shared service” that provides marketing and communications support for all UMMS member hospitals and affiliates. We are Maryland’s health care provider, and are working hard to ensure that citizens of Maryland understand what the University of Maryland Medical System is, what it represents and the tradition of innovative, cutting edge patient-centered and compassionate care we have been delivering for 200 years.

This project is a real opportunity for a vendor to partner with us to modernize and dramatically improve our ability to communicate with our 29,000+ team members and 4,500+ affiliated physicians. As we continue to focus on being a true medical system, this work is integral to helping us achieve our goals around shared culture, team member satisfaction, engagement, retention, recruitment and an overall understanding of what it means to be an UMMS team member, and the benefits therein.

2 High-Level Solution Requirements

University of Maryland Medical System (UMMS) brings academic medicine to communities across Maryland through our member organizations, which operate 11 hospitals, our network of UM Urgent Care locations and our skilled care teams who work hand in hand with the University of Maryland School of Medicine. UMMS is investigating intranet platforms to be used Systemwide to centralize internal communications at a System level. Our current state includes member organization distinctions and individually maintained intranet pages, and is not accessible via mobile devices and when team members are not in the office, unless they have VPN access. The intent for the future state is a centralized solution that team members can easily engage with wherever they are and get the information they want and need in real time including through personal, mobile devices. It should also allow us to communicate our culture and values and how we strive every day to provide a better state of care for our patients, team members and communities.

The section below is a narrative describing some high-level business objectives. A qualified response will address these in the format specified in [Section 3.4 Part 1: Response to Requirements](#).

2.1 Centralization

The goal of a new solution is to eliminate and replace all existing UMMS Insider intranets with a new, single, centralized portal that can efficiently meet the internal communications needs of the System and member organization. The preferred technology solution will be part of a more foundational shift in how the System communicates with team members, allowing for the prioritization of content most relevant to the largest number of team members and the de-prioritization of content infrequently accessed or used by small numbers of team members.

2.2 Interactivity

To achieve centralization, the platform must be user-oriented and should allow team members to customize landing pages based on individual needs and preferences while also establishing fixed information streams on landing pages that all users will encounter. The user experience is essential to effective communications and the solution and related processes will prioritize this perspective. The vendor should clearly indicate how the solution is able to customize landing pages and what customization entails.

2.3 Ease of Use

Team members must also be able to submit content and comment, like and share content, thus making them feel more connected to this content.

2.4 Mobile Enabled

In the interest of usability, the portal must be wholly or partially accessible on mobile devices either as a secure mobile-enabled web site or secure app. The ideal solution will have minimal steps to allow UMMS team member access while adhering to UMMS IT Security standards.

Mobile enablement should not require adding content twice. Content should only be added one time and pushed to both the intranet and the mobile solution.

2.5 Content Management

Centralizing as stated above will require a great deal of content analysis, migration and planning of best practices for the future.

2.6 Functionality

The solution should be able to provide/support:

- 2.6.1 Ability to set reminders to review content on a per page/document basis.
- 2.6.2 A system calendar, customizable by entity/function/role.
- 2.6.3 Ability to embed YouTube and Vimeo videos.

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, team members, care givers or other aspects of the business. Please note that UMMS 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.

Selected vendor will be required to sign a Business Associates Agreement, must be HIPAA compliant, maintain HIPAA compliance, and submit to an UMMS led Vendor Risk Assessment.

3.2 Guidelines & Contact Information

All questions regarding the RFP should be directed to Dustin.Meek@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 -team members, 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, vendors are required to prepare their proposals in accordance with the instructions outlined below. 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.

The University of Maryland Medical System (UMMS) is not responsible for any costs incurred due to response efforts.

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

Vendors are required to follow the outline below when preparing their proposals.

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
- 3.4.1.2 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.
- 3.4.1.3 Please 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.
- 3.4.1.4 Include examples of ROI and any comparisons to market competitors.
- 3.4.1.5 If you maintain any subcontracted agreements relative to the services included in your proposal, please describe those and include the qualifications of those subcontractors.
- 3.4.1.6 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 modern intranet solutions that is secure and accessible on both mobile and desktop devices. 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 creating effective employee apps and intranet solutions.
- 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 intranet solutions that are secure and accessible on both mobile and desktop devices to healthcare entities.
- 3.4.2.4 Provide additional relevant information to further demonstrate the firm's industry knowledge, credentials, certifications, etc., including other major health systems and hospitals you have as clients.
- 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 work in creating effective intranet solutions 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 this 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/Offboarding 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 What is your technical process for migrating current and legacy content into the future state solution?
- 3.4.4.4 What is your strategy on redirects from the current site to the new site?

3.4.4.5 Please describe your offboarding plan (i.e. How is the data provided back to the customer for import to another vendor? At a fee, etc.?)

3.4.5 Customer Support model

3.4.5.1 Describe your 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 include that in the cost proposal and indicate any upper limit of attendees for that training at the amount quoted.

3.4.5.4 Is a permanent Account Representative assigned to the customer account, who can be reached with questions, issues? Are periodic health checks performed and is the customer informed of these events?

3.4.5.5 Please provide what is included in the training (i.e., number of training hours, support model, on-site and/or remote, your plan to manage the transition of training, etc.) based on the terms of the contract.

3.4.5.6 Are there any partners UMMS will need to utilize in order to contract with you?

3.4.6 Technology and Security

3.4.6.1 Describe any UMMS provided hardware or infrastructure required to support your solution. Please provide any applicable hardware specifications. Specifically, outline number of servers required, CPU, RAM and total storage requirement of each. Is this fully a SaaS solution, or is on-premises infrastructure required? If so, please elaborate.

3.4.6.2 Is the solution compatible with mobile devices (iOS, Androids, etc.)?

3.4.6.3 Is compatible with multiple operating systems: Apple Mac OS X, Microsoft Windows?

3.4.6.4 Does the solution run any of the following: Java, SQL, Ruby, Flash?

3.4.6.5 Is the solution compatible with the following browsers: Microsoft Edge, Mozilla Firefox, Safari, Google Chrome?

- HTTPS is a requirement. Does your solution utilize any legacy HTTP?
- Where logins are used, does your solution leverage SAML for an SSO user experience?

3.4.6.6 Does the solution have the ability to integrate with the following applications: Microsoft 365 (principally Teams), ServiceNow, CloudSuite?

3.4.6.7 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.

3.4.6.8 Implementation with UMMS will require data extraction from the legacy system plus integration to receive data from other UMMS business systems.

- 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.
- Describe any API integrations applicable.
- Include any experience you have with integration with Electronic Health Records (EHR), scheduling and timekeeping applications such as Kronos, training and professional development applications and ERP and HR management tools like Infor.

- 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. Does your solution integrate with Citrix for relevant workflows?
- Please provide your vendor solution uptime SLA percentage.
- Describe your organization's business continuity and disaster recovery plans, to include any automated failover systems in place, in the event of a planned and unplanned downtime or outage. How do you communicate and what are your communication procedures during those events?

3.4.6.9 Where do you back up data? What are your data redundancy procedures?

3.4.6.10 How do you manage and communicate planned downtime and maintenance activities?

3.4.6.11 Has your firm experienced any security breaches? If so, please explain the scenario, implications, and remedies for future prevention.

3.4.6.12 Does your solution work well with Proofpoint browser isolation? Have any issues been reported related to this in the past?

3.4.6.13 Describe security and access control 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, Symantec VIP integration etc., as applicable to your services. To help facilitate our security review should you become a preferred vendor, we will ask that you provide:

- Documented 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.
- Documented 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.
- Description of any automated mechanisms within the application that support account management.
- Documented 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.
- Documentation indicating how audit records are prevented from being tampered with including what if any roles have access to the records, what the process is to access the records, and if the records are encrypted and with what cipher strength.

3.4.6.14 Describe your HIPAA compliance measures and any limitations this may present; Also 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. Let us know if your organization has and maintains any information security certifications; for example, ISO 270001 or HITRUST. Describe if any Payment Card Industry (PCI) channels are open & available for use on any sites you would potentially build & support for UMMS, and which payment channels (if any) would be used.

3.4.6.15 Complete the attached [Vendor Intake Questionnaire](#) in Appendix B and the [UMMS Cloud-Based Questionnaire](#) (if applicable) in Appendix C. Please provide your customer provided hardware specifications, as applicable. Specifically, outline number of servers required, CPU, RAM and total storage requirement of each.

3.4.7 Agreements

- 3.4.7.1 The awarded vendor will need to accept, without edit/change, and execute UMMS's [Business Associate 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.

3.4.8 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 RFP 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, among 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 performances be complex multi-hospital system clients. While not required, the Selection Committee would like to know if you have any references which either:

- a) include a large, academic medical center; and/or
- b) have implemented your solution after a large merger or integration of multiple entities (and their intranets).

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

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.

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
RFP Announcement	May 19, 2023
Questions to UMMS Due	May 30, 2023
RFP Responses Due to UMMS	June 05, 2023
Demonstration Presentations	Summer 2023
Selection and Notification	Winter/Spring 2023/24

Please note that the 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 Dustin.Meek@umm.edu by 5:00pm Eastern time on the date noted above. At that time, the RFP will be closed to responses. Respondents can expect an emailed acknowledgment of receipt within an hour of receipt (during business hours) on the due date. Please watch for this acknowledgment 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 <i>for which work was performed and location</i>		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 onboarded 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: Vendor Technology Intake Questionnaire

This document is intended to serve as a general guide to facilitate initial discussion(s) with the vendor that the client may be interested in with regards to a new Information Services related project request, to obtain details around 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 critical that the team understands as much about your needs as possible.	
Date:	
Project Name:	
Requestors Contact Information:	
Does the vendor agree to complete UMMS' vendor onboarding process including appropriate security and compliance assessments?	
Does the vendor possess any security and/or compliance certifications such as SOC 2 ISO 27001, or HITRUST? Is the vendor willing to share evidence of certifications?	
Does the vendor agree to remediate any lack or administrative or technical controls identified during the security/compliance assessment?	
What are the technical/system requirements? Provide architectural and design documentation and system requirements (Example: browser version, Java requirements, server and storage requirements, etc.)?	
What are the standard methods to contact support? List options such as email, website, portal, messaging, etc. Does the vendor provide end user support as well as application administrator or authorized user support? What are the hours of support operation (time zone)?	
What are the options for vendor support? Are there tiers of support that would require additional costs?	
Does the vendor require access to remotely operate, support, upgrade, or update any on-prem systems? What type of access is required? (Example: Is a VPN needed? Escorted access?)	
Can CrowdStrike be installed on any on-prem systems that are part of the solution?	
Are there any hardware/software needs outside of quote that the customer is responsible to purchase or implement?	
Is an interface required? If so, a high-level review and validation is required.	
How quickly could vendor implementation begin once a contract is signed?	
What is a general timeline for Implementation (from planning to Go-Live) from the vendor, and what is the general timeline based on?	
If a Request for Information (RFI) was done, has it been shared with a representative of the Project Management Office (PMO)?	
How will back-ups be performed? Who (University of Maryland Medical System [UMMS] or Vendor) is responsible for back-ups?	
How are patches, updates, and upgrades performed? (Example: Who is responsible, how are the patches applied, at what frequency)?	
How does the vendor send notifications to UMMS resources for planning purposes (e.g., change control notification, staffing)?	
If on-prem servers are required can they be virtualized using VMware?	

Is this application Active Directory integrated? Can the application be configured to use SSO? Is it SAML compliant?
Does the application provide or allow for Multi Factor Authentication?
Does the application integrate with SailPoint IDN?
Is high resolution rendering necessary for outputs of this application that would require an upgraded Graphics Processing Unit?
Can this application be virtualized in Citrix StoreFront?
Please attach any standard high availability/fault tolerant configurations supported by vendor: if required.
Please attach standard disaster recovery plans.
Other considerations:
If the vendor will be accessing a UMMS system which contains personal health information, does the vendor have a Business Agreement (BA) signed with UMMS? If not, a BA will need to be established. We are not to assume that even with an incumbent vendor, that the BA covers a new application, module or software installed.

Appendix C: UMMS Cloud-Based Questionnaire

1. What type of encryption is used at rest, in storage, and in transit? What data protection certifications do you currently hold?
2. Who keeps and manages the encryption keys?
3. Who has access to the encryption keys?
4. Do you offer periodic reports confirming compliance with security requirements and SLAs?
5. What security, privacy, or compliance certifications have you achieved? Do you follow a formal security framework for your infrastructure?
6. Are you audited by external parties, and do you publish a HIPAA, SSAE 16 Type II (aka SOC1), or SOC 2 Type II report?
7. Do you engage independent third parties to perform penetration tests at least annually?
8. Who can access, process, transmit or store UMMS information? How do you isolate and safeguard UMMS data from other clients?
9. 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?
10. What are your methods for backing up our data? What is the RPO and RTO for systems and data?
11. How many iterations of UMMS data are stored, and where are they stored?
12. Where is your data center(s), and what physical security measures are in place? Is any UMMS data maintained outside of the United States?
13. How do you screen your employees and contractors? Do you use third and fourth-party contractors?
14. What actions do you have in place to prevent unauthorized viewing of customer information? What controls are in place to audit access?
15. What actions do you take to destroy data after it is released by a customer?
16. What processes do you follow in the event UMMS data is misplaced or mishandled?
17. What processes do you follow in the event of data corruption?
18. How is an activity in the UMMS environment monitored and documented? What auditing capabilities are provided: Admin/MGMT, System Information, etc.?
19. Does your DR plan include data replication? What level of data durability do you provide?
20. Do you have an Incident Response Plan? If so, how often do you test the plan?
21. How much control does UMMS retain over data maintained by the vendor?
22. Do you offer SAML/SSO capabilities for authentication? What types of multifactor authentication is supported?
23. Can UMMS disable access immediately to our data in the event of a breach?
24. Can you continue to provide protection as UMMS workloads evolve? How scalable is the solution, including disaster recovery?
25. What certifications do you currently hold for your data centers?
26. Can you provide detailed SLA documents? What is your current uptime and SLA option? What if SLA is not met?
27. Do you alert your customers of significant changes like security practices and regulations or data center locations?
28. Will UMMS needs be served by dedicated instances/infrastructure or shared instances/infrastructure?
29. Provide a network schematic diagram of the solution.

Appendix D: 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 E: 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 expressed 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.