Health Care

October 30, 2025

REQUEST FOR PROPOSAL 31203

Human Resources

Employee Health and EMR

for

The Curators of the University of Missouri
on behalf of University of Missouri Health Care

APPENDICES & ATTACHMENTS ONLY

- **Proposal Appendices – Informational Only** (do not submit with your proposal)
  - Appendix 1: "Instructions to Respondents Specific to this RFP"
  - Appendix 2" "Addendum to Agreement – Health IT"
  - Appendix 3: "Data Protection Addendum"

- **Proposal Attachments – Submission Required**

  Volume I (RFP Submittals – All but Financials) – MUST SUBMIT
  - Attachment A: "Specifications with Required Responses"
  - Attachment B" "Specs, IT and Tech, IT Security, HIPAA" (edit page 9)
  - Attachment C: "MBE/WBE/SDVE Participation Form"
  - Attachment D: "Physician Self-Referral Questionnaire"
  - Attachment E: "IT Security Questionnaire"
  - Attachment PA: "Proposal Agreement"

  Volume II (RFP Submittal – Financials) – MUST SUBMIT
  - Attachment FW: "Financial Worksheet"

Rick Hess / *Strategic Sourcing Specialist / Office: 573.882.1643 / RHess@Health.Missouri.edu*

APPENDIX 1
INSTRUCTIONS TO RESPONDENTS, SPECIFIC TO THIS RFP
RFP 31203 Employee Health and EMR

1.0 BACKGROUND AND NARRATIVE

1.1 University of Missouri / University of Missouri Health Care Background:

Please see RFP Section "2.0, Detailed Specifications", "2.3, Background" for the background and narrative for (1) The University of Missouri, (2) University of Missouri Health Care [MUHC], (3) MUHC Hospitals, and (4) MUHC Affiliations and IT Partnership.

1.2 Project/Solution Overview and Background:

MU Health Care is seeking information and/or proposals for an Employee Health and EMR Management Solution that provides a centralized, secure, and efficient system to manage the health and wellness of its workforce. The solution should support immunization tracking, medical surveillance, health assessments, compliance documentation, and reporting for a large, diverse employee population across multiple hospitals, clinics, and pharmacies.

The system should streamline workflows for Employee Health staff, enhance accessibility for employees through self-service capabilities, and ensure alignment with institutional policies, privacy standards, and regulatory compliance requirements.

Key Goals and Objectives:

- **Comprehensive Employee Health Record Management**
  Provide a centralized, longitudinal record of employee health data including immunizations, tests, exposures, and annual health screenings.
- **Immunization and Surveillance Tracking**
  Automate scheduling, reminders, and compliance monitoring for vaccines, TB testing, respiratory fit testing, and other required surveillance programs.
- **Employee Self-Service Portal**
  Allow employees to securely submit documentation, schedule appointments, and view health records online.
- **Reporting and Compliance Monitoring**
  Offer robust reporting tools for internal compliance, infection control, and regulatory audits.
- **Interoperability with Enterprise Systems**
  Integrate with HR, payroll, and enterprise EHR systems using standard data exchange protocols.
- **Data Security and Privacy**
  Ensure compliance with HIPAA and other relevant data protection regulations.
- **Scalability and Configurability**
  Support MU Health Care's enterprise scale with flexible configuration to adapt to evolving organizational requirements.
- **Operational Efficiency**
  Reduce manual data entry and improve coordination between Employee Health, HR, and clinical departments.

Operational Statistics: Hire types vetted include employees, credentialed practitioners, volunteers, contracted vendors, students, educators, travelers, observers, residents, and fellows. We close over 3000 new position requisitions annually and currently have over 10000 active charts.

2.0 REQUEST FOR PROPOSAL INSTRUCTIONS

Please also read RFP Section "1.0, General Information for Respondents". The following instructions are specific to this RFP.

Responses shall be in the same order and fashion of the "Mandatory" and "Desirable" specifications as outlined in "Attachment B / Specifications." To be fully credited in the evaluation, respondents shall describe their ability and methods for complying to each specification. If no response or insufficient response is provided to substantiate compliance, MUHC reserves the sole right to reject respondent's proposal from further consideration.

With responses to the specifications, reference any relevant supplemental documentation included with the proposal that would ensure the specifications are met.

2.1 Register as Participant with a "Letter of Intent"

To ensure inclusion of all RFP correspondences, Register as Participant by submitting a very brief "Letter of Intent" (LOI) via email to Rick Hess at RHess@Health.Missouri.edu, referencing "**RFP 31203, EE Health EMR**" in the subject and on the LOI email:

- An interest in submitting a proposal and receiving all RFP updates and modifications,
- The name, title, contact information, and role in the RFP process for the person who you wish to receive RFP updates and modifications (amendment),
- Stating the deadline for submitting questions (**Wed, November 12, 2025 @ 3:00 PM CT**), and
- The deadline for submitting proposals (**Wednesday, December 10, 2025 @ 3:00 PM CT**).

2.2 Preparation of Proposals

The respondent is expected to examine the specifications and all instructions. Failure to do so will be at the respondent's risk. The respondent shall furnish the information required by this Solicitation. Erasures or other changes must be initialized by the person authorized to sign the proposal.

2.3 Pre-Proposal Conference

There will not be a formal pre-proposal conference.

2.4 Questions/Explanations/Interpretations

Any prospective respondent desiring an explanation or interpretation of the solicitation, specifications, etc., must request it via email to:

- **Rick Hess at RHess@Health.Missouri.edu,** referencing "**RFP 31203, EE Health EMR**" in the subject.

NOTE: The deadline for submitting questions is **Wednesday, November 12, 2025 @ 3:00 PM CT.**

Oral explanations or instructions given before the award of the contract will not be binding. Any information given to a prospective respondent concerning this Solicitation will be furnished promptly

to all prospective respondents as an amendment if the information is necessary in submitting proposals or if the lack of it would be prejudicial to any other prospective respondents. The respondent *MUST BE REGISTERED TO RECEIVE AMENDMENT(S) VIA EMAIL*

2.5 Amendments to Solicitation

- If the Solicitation is amended, all terms and conditions which are not modified remain unchanged.
- Respondents shall acknowledge receipt of any amendment to this Solicitation by:
    - Identifying the amendment number and date in the space provided for this purpose on the "Proposal Agreement" form.

CONTINUED ON NEXT PAGE

2.6 Proposal Submission

PREFERRED METHOD (Electronic via Email)

To be eligible for consideration, an email with two attachments (either in Microsoft 365 or PDF format) must be submitted and received by **Wed, December 10, 2025 @ 3:00 PM CT** in the following format:

- **To (Rick Hess)**: RHess@Health.Missouri.edu
- **Subject (must be)**: RFP 31203, EE Health EMR, Due: 12/10/25 by 3:00 PM CT
- **Volume I (*Responses*) named**:
    - VI - EE Health EMR, Attach A-PA (Your Firm's Name) – YYMMDD
- **Volume II (*Financials*) named**:
    - VII - EE Health EMR, Attach FW (Your Firm's Name) – YYMMDD
- **Body:** Please do not include any of your "proposal" in the body of the email. Clearly include the name, email address and phone number of the person you wish to receive confirmation of receipt, and who Rick Hess may call with any questions or issues with the proposal (such as an attachment will not open properly).

Rick Hess will (1) open the email to reply with confirmation of receipt, (2) open the attachments only to ensure there is no issue with access, (3) close the attachments immediately without review, and (4) will not reopen the attachment prior to the submission deadline.

OPTIONAL METHOD (Hand or Carrier Delivered)

To be eligible for consideration, a sealed proposal packet [one (1) original, clearly identified as containing documents with original signatures and one (1) electronical copy of the entire submission on a flash drive], divided into two packets:

- **Volume I (*Responses*) named**:
    - VI - EE Health EMR, Attach A-PA (Your Firm's Name) – YYMMDD
- **Volume II (*Financials*) named**:
    - VII - EE Health EMR, Attach FW (Your Firm's Name) – YYMMDD

And must be submitted and received by **December 10, 2025 @ 3:00 PM CT** to the following address:

Rick Hess

Strategic Sourcing Specialist
MUHC Quarterdeck Building
2401 LeMone Industrial Blvd, Rm 171
Columbia, MO 65201

To ensure the proposal is routed properly and to prevent opening by unauthorized individuals, your proposal must be identified on the envelope or package as follows:

RFP 31203, EE Health EMR
Due: 12/03/25 by 3:00 PM CT

2.7 Handling of Proposals

- Proposals received prior to the closing date and time will remain unopened and secured until after the established proposal opening date and time.
- **A proposal will not be considered if it is received after the exact date and time specified for receipt**. Acceptable evidence to establish the time of receipt is the CT date/time of the email, or an MUHC stamped CT date/time on the proposal wrapper or other documentary evidence of receipt maintained by MUHC.

2.8 Proposal Modifications

- A modification resulting from MUHC's request for "best and final" proposal received after the time and date specified in the request will not be considered unless received before award and the late receipt is due solely to mishandling by MUHC after receipt at MUHC.
- Notwithstanding this provision, a late modification of an otherwise successful proposal that makes its term more favorable to the MUHC will be considered at any time it is received and may be accepted.

2.9 Proposal Withdrawal

- No proposal shall be withdrawn for a period of Ninety (90) days after the opening of the proposals without written consent of MUHC.

2.10 Evaluation of Proposals

- MUHC will strive to complete the proposal and presentation reviews and issue a "Notice of Award" by the end of day **Friday, January 30, 2026**.

2.11 OTHER APPENDICES - Informational Only (do not submit with your proposal):

- Please see Appendices 2 (Addendum to Agreement) and 3 (Data Protection Addendum). These documents are not required for submission with your proposal but will be incorporated as addenda to the agreement with the awarded firm.

APPENDIX 2

ADDENDUM TO AGREEMENT
THE CURATORS OF THE UNIVERSITY OF MISSOURI

Note: This appendix is not required for submission with your proposal. However, it will be incorporated as an addendum to the agreement with the awarded firm.

This Addendum to Agreement ("Addendum") is made and entered into and effective upon the signing of both Parties ("Effective Date") by and between The Curators of the University of Missouri, a Missouri public corporation ("University") and XXXXX ("Contractor"). This Addendum modifies and is incorporated by reference into the agreement entitled XXXXXX with effective date of XXXXX between University and Contractor ("Agreement"). Both University and Contractor are also referred to herein as "Party" or, collectively "Parties."

1. **Order of Precedence**: This Addendum modifies and supersedes anything contained in the Agreement or Contractor's forms, whether or not they are submitted before or after the signing of this Addendum. IN THE EVENT OF CONFLICT BETWEEN THE AGREEMENT AND THIS ADDENDUM, THIS ADDENDUM SHALL CONTROL AND CONTRACTOR WAIVES ANY CLAIM TO THE CONTRARY.

2. **Representations and Warranties by Contractor**: If Contractor is a corporation or a limited liability company, Contractor warrants, represents, covenants, and agrees that it is duly organized, validly existing and in good standing under the laws of the state of its incorporation or organization and is duly authorized and in good standing to conduct business in the State of Missouri, that it has all necessary power and has received all necessary approvals to execute and deliver the Agreement, and the individual executing the Agreement on behalf of Contractor has been duly authorized to act for and bind Contractor. Contractor represents and warrants that any software, deliverables, or data provided to University will (i) be free of viruses, malware and other malicious code; and (ii) will not infringe the intellectual property rights or misappropriate the trade secrets of any third party. Contractor will defend and indemnify University from and against any damages or third party claims arising out of a breach of these representations and warranties.

3. **Payment**: Payment by University for goods/services under the Agreement shall be made as follows: (a) payment shall be made no later than thirty (30) days following the later of (i) delivery of the goods or completion of the services and (ii) delivery of an invoice to University; and (b) any provisions in the Agreement obligating University to pay late fees or interest on past due payments are deleted in their entirety. If University disputes, reasonably and in good faith, the contents or validity of any item contained on a Contractor invoice to the University (the "Disputed Charge"), University may withhold payment of such portion that is the Disputed Charge provided that the University promptly gives Contractor written notice of, and the basis for, such Disputed Charge and the University pays timely all undisputed charges.

4. **Tax Exempt**: University is generally exempt from the payment of Missouri and federal income and/or sales taxes and will provide necessary documentation confirming its tax-exempt status upon written request. Any provisions in the Agreement requiring University to pay taxes, or allowing Contractor to withhold taxes, are deleted in their entirety.

5. **Charges, Fees, or Costs**: Any provisions in the Agreement obligating University to pay increases in pricing due to changes in tariffs, duties or similar governmental charges or costs of collection, court costs, and/or attorneys' fees are deleted in their entirety. The agreed-upon prices shall remain fixed and shall not be subject to adjustment based on any such external increased charges, fees, or costs.

6. **Third-Party Software**: If the Agreement contemplates or requires the use of third-party software, Contractor represents that none of the mandatory click-through, unsigned, or web-linked terms and conditions presented or required before using such third-party software conflict with any term of this Addendum or that it has authority to modify such third-party software's terms and conditions to be subordinate to this Addendum. Contractor shall indemnify and defend University against all claims resulting from an assertion that any such third-party terms and conditions are not in accord with, or subordinate to, this Addendum.

7. **Accessibility**: The University affords equal opportunity to individuals with disabilities in its employment, services, programs and activities in accordance with federal and state laws, including 28 C.F.R. Pt. 35, Section 508 of the Rehabilitation Act, and RSMo. 161.935. This includes effective communication and access to electronic and information communication technology resources, and the University expects that all products will, to the greatest extent possible, provide equivalent ease of use for individuals with disabilities as for non-disabled individuals. The University of Missouri has adopted the Web Content Accessibility Guidelines (WCAG) 2.2 and AA as the minimum standard.

   Contractor shall: (1) deliver all applicable services and products in reasonable compliance with University standards (Web Content Accessibility Guidelines 2.2, Level A and AA or above); (2) provide the University with an Accessibility Conformance Report detailing the product's current accessibility according to WCAG standards using the latest version of the Voluntary Product Accessibility Template (VPAT); (3) if accessibility issues exist, provide a "roadmap" plan for remedying those deficiencies on a reasonable timeline to be approved by the University; (4) within 15 days of notice respond to assist the University with resolving any accessibility complaints and requests for accommodation from users with disabilities resulting from Contractor's failure to meet WCAG 2.2 A and AA guidelines at no cost to the University; and (5) indemnify and hold the University harmless in the event of any claims arising from inaccessibility.

   When installation, configuration, integration, updates, or maintenance are provided, the Contractor must ensure these processes are completed in a way that does not reduce the original level of WCAG conformance. If at any point after procurement it is determined that accessibility improvements need to be made in order to comply with the WCAG 2.2 A and AA standards, the Contractor agrees to work with the University to remedy the non-compliance by submitting a roadmap detailing a plan for improvement on a reasonable timeline; provided, however, that any such improvements shall be implemented within 15 days of notice. Resolution of reported accessibility issue(s) that may arise should be addressed as high priority, and failure to make satisfactory progress towards compliance with WCAG, as agreed to in the roadmap, shall constitute a breach of contract and be grounds for termination or non-renewal of the agreement. The foregoing requirements are subject to the discretion of the University of Missouri System Director of Accessibility and ADA Coordinator.

8. **Governing Law, Jurisdiction, and Venue**: The Agreement and

all of the rights and obligations of the Parties hereto and all of the terms and conditions of the Agreement will be governed by the laws of the State of Missouri without giving effect to the conflict of laws principles. Any action to enforce the provisions of the Agreement shall be brought in a court of competent jurisdiction and proper venue in the State of Missouri. Any provisions to the contrary in the Agreement are deleted in their entirety.

9. **Termination Right**: University reserves the right to terminate this Agreement upon thirty (30) days' written notice to Contractor. If this right is exercised, University agrees to pay Contractor only for all undisputed services rendered or goods received before the termination's effective date. All provisions are deleted that seek to require University to (1) compensate Contractor, in whole or in part, for lost profit, (2) pay a termination fee, or (3) pay liquidated damages if the Agreement is terminated early.
10. **Use of Name**: Neither Party shall use the name or indicia of the other Party, nor of any of a Party's employees, in any manner of publicity, advertising, or news releases without prior written approval of the other Party.
11. **Confidentiality**: Any provisions in the Agreement requiring University or its employees to keep information confidential will not apply if disclosure is required by state or federal law, including Chapter 610 of the Revised Statutes of Missouri ("Missouri Sunshine Law") or by a valid court or administrative order.
12. **University's Indemnification of Contractor**: Any provisions in the Agreement requiring University to defend, indemnify or hold harmless Contractor or a third party are deleted in their entirety.
13. **Insurance**: Any provisions in the Agreement stating that University shall purchase or maintain liability insurance or name Contractor as an additional insured are deleted in their entirety.
14. **University Liability**: Any provisions in the Agreement stating that University agrees to be responsible for the acts or omissions of anyone other than its employees are deleted in their entirety. University will not be liable for any indirect or consequential damages including punitive damages and lost profits.
15. **Limitation of Actions**: Any provisions limiting the time in which University may bring suit against Contractor or any other third party are deleted in their entirety.
16. **Contractor Liability**: Any references to University limiting damages, remedies, or waiving any claim are deleted.
17. **Disputes**: Any provisions in the Agreement binding University to any arbitration or to the decision of any arbitration board, commission, panel, or other entity are deleted in their entirety. Any provision that University waive its rights to a jury trial is deleted in its entirety.
18. **Sovereign Immunity**: Neither the execution of the Agreement by University nor any other conduct, action, or inaction of any University representative relating to the Agreement is a waiver of sovereign immunity by University.
19. **No Boycott**: If the Agreement involves the acquisition or disposal of services, supplies, information technology, or construction and has a total potential value of $100,000 or more, and if Contractor is a company with ten (10) or more employees, then Contractor certifies that it, and any company affiliated with it, does not boycott Israel and will not boycott Israel during the term of the Agreement. In this Paragraph, the terms "company" and "boycott Israel" shall have the meanings described in Section 34.600 of the Missouri Revised Statutes.
20. **Non-Solicitation and Exclusivity**: Any non-solicitation and exclusivity provisions in the Agreement are deleted in their entirety.
21. **IT Manager**: If Contractor is providing University with software or other information technology solutions, Contractor acknowledges that University has transitioned and delegated some of its IT-related functions to Cerner Corporation and its personnel (the "IT Manager"), including, but not limited to, the monitoring, maintenance, and management of software and information technology solutions, in all cases solely for the University's business purposes and at the University's facilities (the "Transactions"). Contractor agrees that: (i) University may transition and delegate to the IT Manager the monitoring, maintenance, management, and incidental functions relating to Transactions, and (ii) University may permit the IT Manager or other contractor performing similar functions to access and use the software in furtherance of the foregoing, in each case in connection with the Transactions; provided, that the IT Manager or such other contractor shall be subject to and comply with all confidentiality and other license restrictions applicable to the University and the software under the Agreement in accordance with its terms.
22. **IT Applications**: All information technology (IT) applications and systems used by the University must be developed, implemented, and maintained in a secure manner in accordance with either established University policy or, in the absence of a specific University policy, in accordance with industry-standard best practices. In addition, the University requires compliance with the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI) specifications, and all other applicable state, local, and federal laws and regulations. Contractor certifies that it has read and will comply with the University's guidelines for application development (https://www.umsystem.edu /ums/is/infosec/sections-sysapp) and all applicable elements of the University of Missouri Information Security Program (https://www.umsystem.edu/ums/is/infosec). Contractor agrees to protect the privacy and security of University data at all times and further agrees not to use or disclose such data other than to accomplish the objectives of this Agreement. Contractor will comply with University's Data Protection Addendum ("DPA") which is located at https://www.umsystem.edu/sites/default/files/media/fa/procurement/Data%20Protection%20Addendum.pdf and is incorporated herein by reference.
23. **Insurance**: Contractor agrees to maintain Data Breach coverage to cover claims arising out of the negligent acts, errors, or omissions of Contractor, its subcontractors, or anyone directly or indirectly employed by them. The coverage provided shall not be less than $2,000,000 per occurrence, $5,000,000 aggregate. Prior to the commencement of work under the Agreement, Contractor shall provide a certificate of insurance evidencing such insurance, shall name the officers, employees, and agents of the University as Additional Insured with respect to the order to which these insurance requirements pertain. Neither the requirement for Additional Insured status nor any of the Contractor's actions in compliance with such requirement, either direct or indirect, is intended to be and neither shall be construed as a waiver of any sovereign immunity, governmental immunity, or any other type of immunity enjoyed by University, the Board of Curators of the University of Missouri, or any of its officers, employees, or agents. Contractor shall provide for notification to University within at least thirty (30) days prior to expiration or cancellation of such

insurance. The Contractor agrees to defend, indemnify, and hold harmless University, its officers, agents, employees, and volunteers, from and against all loss or expense from any cause of action arising from the Contractor's operations. The Contractor agrees to investigate, handle, respond to and provide defense for and defend against any such liability, claims, and demands at the sole expense of the Contractor or at the option of the University, and agrees to pay or reimburse the University for the defense costs incurred by the University in connection with any such liability claims, or demands. Failure to maintain the required insurance in force may be cause for contract termination. In the event the Contractor fails to maintain and keep in force the required insurance or to obtain coverage from its subcontractors, the University shall have the right to cancel and terminate the Agreement upon written notice.

24. **Exclusion and Debarment**: Contractor represents and warrants that neither it nor any of its owner, officers, directors, managers, or employees providing services under this Agreement are excluded from participation in any federal health care programs, as defined under 42 U.S.C. 1320a-7b(f), or any form of state Medicaid program. Contractor further represents and warrants that neither it nor any of its owners, officers, directors, managers, or employees providing services under this Agreement have been debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal or state department or agency. Contractor agrees to notify University of the commencement of any such proceeding to exclude, debar, suspend, or declare ineligible Contractor or any of its owners, officers, managers, or employees providing services under this Agreement within seven (7) business days of learning of it.

25. **HIPAA**: The parties understand and agree that this Agreement may be subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the administrative regulations and/or guidance which have issued or may in the future be issued pursuant to HIPAA, including, but not limited to, the Department of Health and Human Services regulations on privacy and security, and Missouri state laws pertaining to medical privacy (collectively, "Privacy Laws"). Contractor agrees to comply with all Privacy Laws that are applicable to this Agreement and to negotiate in good faith to execute any amendment to this Agreement that is required for the terms of this Agreement to comply with applicable Privacy Laws. In the event the Parties are unable to agree on the terms of an amendment pursuant to this paragraph within thirty (30) days of the date the amendment request is delivered by a Party to the other, this Agreement may be terminated by either Party upon written notice to the other Party.

26. **Access to Books and Records**: If either Party should be deemed a subcontractor of the other Party subject to the disclosure requirements of 42 U.S.C. § 1395x(v)(1), that Party shall, until the expiration of four years after the furnishing of services pursuant to this Agreement, make available upon request to the Secretary, U.S. Department of Health and Human Services, and the U.S. Comptroller General, or any of their duly authorized representatives, a copy of the Agreement and the books, documents and records of services that are necessary to certify the nature and extent of the costs incurred under this Agreement by that party. If services or any duties of this Agreement are through a subcontractor with a value or cost of $10,000 or more over a 12-month period with a third party, such subcontract shall contain a clause to the effect that should the third party be deemed a related organization, until the expiration of four years after the furnishing of services pursuant to such subcontract, the third party shall make available upon request to the Secretary, U.S. Department of Health and Human Services, and the U.S. Comptroller General, or any of their duly authorized representatives, a copy of the subcontract and the books, documents and records of such third party that are necessary to verify the nature and extent of the costs incurred under this Agreement by that Party. No attorney-client, accountant-client or other legal privilege will be deemed to have been waived by either Party as a result of this Agreement.

27. **Change in Law**: In the event that legislation is enacted or regulations are promulgated or a decision of a court or administrative tribunal is rendered which affects or may affect, in the opinion of legal counsel of University, the legality of this Agreement or adversely affect the ability of either Party to perform its obligations or receive the benefits intended hereunder, then, within fifteen (15) days following notice, each Party will negotiate in good faith an amendment to this Agreement which will carry out the original intention of the Parties to the extent possible in light of such legislation, regulation, or decision, and each Party will execute such amendment. In the event that the Parties cannot reach agreement on the terms and provisions of any such amendment within sixty (60) days following the notice provided in this paragraph, this Agreement may be terminated upon not less than thirty (30) days' prior written notice of termination.

28. **Compliance with Policies**: Contractor shall comply with all of University's policies for contractors and vendors.

29. **Amendment**: The Parties agree that all amendments, modifications, alterations or changes to the Agreement shall be by mutual agreement, in writing, and signed by both Parties. Any provisions to the contrary in the Agreement are deleted in their entirety.

30. **Miscellaneous**: In the event that any provision of the Agreement or this Addendum or portion thereof is determined to be invalid, unlawful, void, or unenforceable, such portion shall be deemed to be amended and removed, with all remaining portions of the Agreement as amended by this Addendum to remain in force and unaffected thereby. All capitalized terms used but not defined herein shall be as defined in the Agreement. Except as and to the extent modified by this Addendum, all provisions of the Agreement shall remain in full force and effect in accordance with its terms. This Addendum shall be manually or electronically signed and may be delivered by facsimile or other electronic transmission, which shall constitute an original. The Agreement as amended by this Addendum constitutes the entire agreement between the Parties with respect to the subject matter herein and therein.

Contractor:

By:_____

Name:_____

University:

By:_____

Name:_____

Title:_____

Date:_____

Title:_____

Date:_____

APPENDIX 3
DATA PROTECTION ADDENDUM
(Rev. July 2025)

Note: This appendix is not required for submission with your proposal. However, it will be incorporated as an addendum to the agreement with the awarded firm.

This Data Protection Addendum supplements the University of Missouri Standard Procurement Terms and Conditions found at PO Terms & Conditions ("Terms and Conditions"). The Curators of the University of Missouri ("University") requires that their service providers, suppliers, distributors and other business partners and their employees (collectively "Contractor") comply with the requirements in this Data Protection Agreement ("DPA") with respect to any information that University, University employees, representatives, customers, or other business partners make available to Contractor in the context of Contractor's business relationship with University (collectively "University Data"). Contractor is a Processor that provides certain services ("Services") to University pursuant to an agreement or agreements with University (the "Underlying Agreement(s)") and Processes, on University's behalf, Personal Information that is necessary to perform the Services under the Underlying Agreement(s).

NOTE REGARDING PATIENT INFORMATION: If Contractor, through work with one of the University's designated "health care components", will receive, create, or come into non-incidental contact with individually identifiable health information of University patients -- "Protected Health Information" as that term is defined in regulations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), at 45 C.F.R. Part 160.103 -- the University's Business Associate Addendum applies in addition to this Data Protection Addendum. Where noted herein, certain sections of the Business Associate Addendum replace sections of this Data Protection Addendum as regards to Protected Health Information (PHI).

1. Definitions

Any capitalized term used but not defined herein shall have the meaning ascribed to it in the applicable Data Protection Laws.

The definitions enumerated below (including all conjugations, forms, and tenses thereof) apply to this DPA:

a. "Data Breach " means Contractor's negligence or a breach of Contractor's security measures leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information.

b. "Data Protection Laws" means, as applicable: (a) the Family Educational Rights and Privacy Act (FERPA); (b) the Health Insurance Portability and Accountability Act (HIPAA); (c) the Gramm-Leach-Bliley Act (GLBA); (d) the Payment Card Industry Data Security Standards (PCI-DSS); (e) the Federal Export Administration Regulations, Federal Acquisitions Regulations, Defense Federal Acquisitions Regulations and Department of

Education guidance; and (f) any other laws, rules, regulations, self-regulatory guidelines, implementing legislation, or third party terms relating to privacy, security, breach notification, data protection, or confidentiality and applicable to processing of Personal Information.

c. "Data Subject" means any person, household, or device that becomes subject in any manner to the services performed for University by Contractor.

d. "Personal Information" (i) means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Data Subject that may be (a) disclosed or otherwise made accessible to Contractor by University in anticipation of, in connection with, or incidental to the performance of Services for or on behalf of University; (b) Processed at any time by Contractor in connection with or incidental to the performance of this DPA or the Underlying Agreement(s); or (c) derived by Contractor from the information described in a) or b) above; and (ii) supplements the foregoing definition enumerated in (i) by also incorporating the definition of "Personal Information," "Personal Data," and "Non-Public Personal Information under Data Protection Laws. Personal Information includes without limitation behavioral characteristics and profiles. Personal Information includes Protected Health Information as defined under HIPAA.

e. "Processing" means performing any operation (whether automated or manual, or through some combination) relative to Personal Information, including, without limitation, accessing, collecting, organizing, retaining, using, disclosing, storing, manipulating, adapting, analyzing, aggregating, categorizing, transmitting, destroying, and deriving or creating information from, Personal Information.

f. “Securely Destroy” means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-88, REV 1 guidelines relevant to data categorized as high security.

2. Processing Restrictions and Obligations

Contractor may Process Personal Information only as strictly necessary to deliver the Services pursuant to the Underlying Agreement(s). Without limiting the foregoing and to avoid any doubt, Contractor represents, warrants, and covenants as follows:

a. Contractor is acting solely as a Processor with respect to Personal Information, and University has the exclusive authority to determine the purposes for and means of Processing the Personal Information.

b. Contractor will Process Personal Information only (i) for a business purpose and (ii) on behalf of University, for the sole purpose of performing the Services specified in the

Underlying Agreement(s), and Contractor will not collect, retain, use, disclose or otherwise Process Personal Information for any other purpose.

c. Contractor will not sell Personal Information or use or otherwise Process Personal Information for monetary or other valuable consideration.

d. Contractor will not retain, use, disclose or otherwise Process Personal Information outside of the direct business relationship between Contractor and University.

e. Contractor may not derive information from Personal Information for any purpose other than to perform Services under the Underlying Agreement(s).

f. Contractor may not engage or communicate with a Data Subject in any way, whether directly or indirectly (including, without limitation, via interest-based advertising, mobile messaging, contextual online experiences, online ad-serving, email, telephone, social media, and location-aware technologies) except under written agreement between Contractor and University that specifies the means and methodology of, and limitations on, the media or communication channel in question

g. Contractor will immediately inform University in writing of any requests with respect to Personal Information received from University's customers, consumers, employees or others. Contractor will cooperate with University as needed by University regarding Data Subject rights, including enabling (i) access to a Data Subject's Personal Information, (ii) delivering information about the categories of sources from which the Personal Information is collected, (iii) delivering information about the category of Processor that Contractor is, or (iii) providing information about the categories or specific pieces of a Data Subject's Personal Information that Contractor Processes on University's behalf, including by providing the requested information in a portable and, to the extent technically feasible, readily useable format that allows a Data Subject to transmit the information to another entity without hindrance.

h. Upon University's request, Contractor will immediately Securely Destroy a particular Data Subject's Personal Information from Contractor's records and direct any relevant contractors or agents to also Securely Destroy such Personal Information from their records. If Contractor is unable to Securely Destroy the Personal Information for reasons permitted under applicable Data Protection Laws, Contractor will (i) promptly inform University of the reason(s) for Contractor's refusal of the destruction request, (ii) ensure the privacy, confidentiality, and security of such Personal Information, and (iii) Securely Destroy the Personal Information promptly after the reason for Contractor's refusal has expired.

i. Contractor may only Process Personal Information for as long as the applicable Underlying Agreement(s), relationship, or arrangement between Contractor and University authorizes it, and only to benefit University (and not Contractor or any of Contractor's other clients or customers). In the event of any conflict with this DPA Data Protection

Addendum and any Business Associate Agreement ("BAA") between University and Contractor, the BAA will control.

j. Where Contractor provides a third-party access to Personal Information, or contract any of Contractor's rights or obligations concerning Personal Information to a third party, Contractor will enter into a written agreement with each such third party that imposes obligations on the third party that are at least equivalent to those imposed on Contractor under this DPA. By written agreement and through technical, organizational, and physical measures, Contractor must (i) limit such third party's access to and Processing of Personal Information to that which is solely necessary to deliver the Services under the Underlying Agreement(s) and (ii) prohibit such third party from selling Personal Information. Contractor shall conduct ongoing reviews, at least annually, of such third-party agreements to ensure ongoing compliance with the requirements of this DPA or those that are least equivalent.

k. Contractor will maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, University Data), pursuant to applicable Data Protection Laws, and keep University Data confidential. Contractor will ensure that such persons with access to University Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

l. Contractor will make its applicable employees familiar with the relevant provisions of the Data Protection Laws and shall provide adequate training. Contractor will supervise compliance of such employees with applicable Data Protection Laws.

m. University has the right in its sole discretion to perform audits of Contractor at the University's expense to ensure compliance with the Data Protection Laws, the Underlying Agreement(s) and this DPA (including the technical and organizational measures). Contractor shall reasonably cooperate in the performance of such audits. This provisions applies to all agreements under which Contractor must create, obtain, transmit, use, maintain, process, or dispose of University Data. If Contractor must under this DPA create, access, obtain, transmit, use, maintain, process, or dispose of University Data, Contractor will, at its expense, conduct or have conducted, at least annually, a (1) security audit by a third-party with audit scope and objectives deemed sufficient by the University, which attests the Contractor's security policies, procedures, and controls; (2) vulnerability scan performed by a third-party using industry standard and up-to-date scanning technology of Contractor's electronic systems and facilities that are used in any way to deliver electronic services under this agreement; and (3) formal penetration test by a third-party using industry-standard and up-to-date scanning technology, of Contractor's electronic systems and facilities that are used in any way to deliver electronic services under this DPA.

n. Additionally, no more than once per year, Contractor shall make available to University, information reasonably necessary to confirm compliance with this DPA. Upon request, Contractor will provide the University with its current industry standard independent third-party certification/attestation such as Service Organization Control (SOC) 2 Type II audit report, ISO27001/2 or equivalent, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this DPA. Contractor agrees to be held legally accountable for the accuracy of any self-attestations provided by the Contractor in regard to the submitted certifications/attestations. The University shall have sole discretion to determine whether the audit report/certification/attestation provided is sufficient to satisfy the requirements of this paragraph. The University may require, at University expense, the Contractor to perform additional audits and tests, the results of which will be provided promptly to the University.

o. In accordance with the Data Protection Laws and other industry standards, Contractor has appropriate policies and procedures in place to manage a Data Breach.

p. In accordance with the Data Protection Laws, Contractor shall notify University without undue delay, but in no event later than 36 hours after discovery, in the event of a Data Breach relating to University Data, of which Contractor reasonably suspects or knows to have occurred. Contractor shall provide commercially reasonable cooperation and assistance in identifying the cause of the Data Breach and take all commercially reasonable steps to remediate the Data Breach to the extent within Contractor's control.

q. Contractor will not process Personal Information outside of the United States without the prior written consent of University, which may be granted or denied by University in its sole discretion.

r. Contractor will maintain a list of subcontractors and update such list prior to any engagement of any subcontractor and give University an opportunity to object to that subcontractor. If University objects to the subcontractor, Contractor will work with University in good faith to arrange for the performance of the Services without the use of such subcontractor and University may terminate this Agreement without penalty. Such engagement must be pursuant to a written contract that requires the subcontractor to also meet the obligations set forth in this Section for the Contractor

s. With respect to any Data Breach due to Contractor or any subcontractor's action or inaction, notwithstanding anything to the contrary in the Underlying Agreement(s), and without regard to any limitations of liability contained in the Underlying Agreement(s), Processor shall indemnify University for the cost of a cyber forensic investigation, any required consumer regulator notices and related attorney fees and any other costs, fines, damages, and penalties incurred under Applicable Data Protection Laws.

t. In addition to any other insurance coverage required by another contract/agreement with the University, the Contractor will for the duration of the term of the Underlying Agreement(s), maintain data breach coverage to cover claims arising out of the negligent

acts, errors or omissions of Contractor, its subcontractors or anyone directly or indirectly employed by them. The coverage provided shall not be less than $2,000,000 per occurrence, $5,000,000 aggregate. Prior to the commencement of work under the Underlying Agreement(s), Contractor shall provide a certificate of insurance evidencing such insurance, shall name the officers, employees, and agents of The Curators of the University of Missouri as Additional Insured with respect to the order to which these insurance requirements pertain. Neither the requirement for Additional Insured status nor any of the Contractor's action in compliance with such requirement, either direct or indirect, is intended to be and neither shall be construed as a waiver of any sovereign immunity, governmental immunity or any other type of immunity enjoyed by University, the Board of Curators of the University of Missouri, or any of its officers, employees or agents. Contractor shall provide for notification to University within at least thirty (30) days prior to expiration or cancellation of such insurance. In the event the Contractor fails to maintain and keep in force the required insurance or to obtain coverage from its subcontractors, the University shall have the right to cancel and terminate the Underlying Agreement(s) upon written notice.

3. Compliance with Data Protection Laws

a. Contractor and University acknowledge and agree that University does not sell Personal Information to Contractor in connection with any Agreement between Contractor and University. Contractor acknowledges and confirms that Contractor does not Process Personal Information from University in exchange for monetary or other valuable consideration, and that Contractor may not have, derive, or exercise any rights or benefits regarding Personal Information, except to Process the Personal Information as necessary to deliver Services to University pursuant to the Underlying Agreements.

b. Upon the reasonable request of University, Contractor shall make available all information in its possession necessary to demonstrate compliance with any applicable Data Protection Law.

c. Contractor will promptly notify University if Contractor determines that Contractor can no longer meet its obligations under this Section or any applicable Data Protection Law.

d. The Parties acknowledge and agree that University has no knowledge or reason to believe that Contractor is unable to comply with the provisions of this DPA or any applicable provisions of the Data Protection Laws.

e. Contractor certifies that Contractor understands and will comply with the requirements and restrictions set forth in this DPA, and with all applicable provisions of the Data Protection Laws.

f. The following provision applies only if Contractor will have access to the University's education records as defined under FERPA: The Contractor acknowledges that for the purposes of this DPA it will be designated as a "school official" with "legitimate

educational interests" in the University education records, as those terms have been defined under FERPA and its implementing regulations, and the Contractor agrees to abide by the limitations and requirements imposed on school officials. Contractor will use the education records only for the purpose of fulfilling its duties under the Underlying Agreement(s) and will not share such data with or disclose it to any third party except as provided for in this DPA, required by law, or authorized in writing by the University.

g. If the Payment Card Industry Data Security Standard (PCI-DSS) is applicable to the Contractor service provided to the University, the Contractor agrees to:

   i. Store, transmit, and process University Data in scope of the PCI DSS in compliance with the PCI DSS; and

   ii. Attest that any third-party providing services in scope of PCI DSS under the Underlying Agreement(s) will store, transmit, and process University Data in scope of the PCI DSS in compliance with the PCI DSS; and

   iii. Provide either proof of PCI DSS compliance or a certification (from a recognized third-party security auditing firm), within 10 business days of the request, verifying Firm/Vendor and any third party who stores, transmits, or processes University Data in scope of PCI DSS as part of the services provided under the Underlying Agreement(s) maintains ongoing compliance under PCI DSS as it changes over time; and

   iv. Store, transmit, and process any University Data in scope of the PCI DSS in a manner that does not bring the University's network into PCI DSS scope; and

   v. Attest that any third-party providing services in scope of PCI DSS under the Underlying Agreement(s) will store, transmit, and process University Data in scope of the PCI DSS in a manner that does not bring the University's network into PCI DSS scope.

h. Digital Accessibility. The University affords equal opportunity to individuals with disabilities in its employment, services, programs and activities in accordance with federal and state laws, including 28 C.F.R. Pt. 35, Section 508 of the Rehabilitation Act, and RSMo. 161.935. This includes effective communication and access to electronic and information communication technology resources, and the University expects that all products will, to the greatest extent possible, provide equivalent ease of use for individuals with disabilities as for non-disabled individuals. The University of Missouri has adopted the Web Content Accessibility Guidelines (WCAG) 2.2 A and AA as the minimum standard.

   Contractor shall: (1) deliver all applicable services and products in reasonable compliance with University standards (Web Content Accessibility Guidelines 2.2, Level A and AA or above); (2) provide the University with an Accessibility Conformance Report detailing the

product's current accessibility according to WCAG standards using the latest version of the Voluntary Product Accessibility Template (VPAT); (3) if accessibility issues exist, provide a "roadmap" plan for remedying those deficiencies on a reasonable timeline to be approved by the University; (4) within 15 days of notice respond to assist the University with resolving any accessibility complaints and requests for accommodation from users with disabilities resulting from Contractor's failure to meet WCAG 2.2 A and AA guidelines at no cost to the University; and (5) indemnify and hold the University harmless in the event of any claims arising from inaccessibility. If Contractor does not currently comply with WCAG 2.2 A and AA, they must provide confirmation that they have a roadmap in place to comply.

When installation, configuration, integration, updates, or maintenance are provided, the Contractor must ensure these processes are completed in a way that does not reduce the original level of WCAG conformance. If, at any point after procurement, it is determined that accessibility improvements need to be made in order to comply with the WCAG 2.2 A and AA standards, the Contractor agrees to work with the University to remedy the non-compliance by submitting a roadmap detailing a plan for improvement on a reasonable timeline; provided, however, that any such improvements shall be implemented within 15 days of notice. Resolution of reported accessibility issue(s) that may arise should be addressed as high priority, and failure to make satisfactory progress towards compliance with WCAG, as agreed to in the roadmap, shall constitute a breach of contract and be grounds for termination or non-renewal of the agreement. The foregoing requirements are subject to the discretion of the University of Missouri System Director of Accessibility and ADA Coordinator.

4. Response to Legal Orders, Demands or Requests for Data

a. Except as otherwise expressly prohibited by law, Contractor will:

i. immediately notify the University of Contractor's receipt of any subpoenas, warrants, or other legal orders, demands or requests seeking University Data;

ii. consult with the University regarding its response;

iii. cooperate with the University's reasonable requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request; and

iv. provide the University with a copy of its response.

b. If the University receives a subpoena, warrant, or other legal order, demand or request (including request pursuant to the Missouri Sunshine Law) seeking University Data maintained by Contractor, the University will provide a copy to Contractor. Contractor will promptly supply the University with copies of data required for the University to

respond in a timely manner and will cooperate with the University's reasonable requests in connection with its response.

5. Data Transfer Upon Termination or Expiration

a. Upon termination or expiration of the Underlying Agreement, Contractor will ensure that all University Data are Securely Destroyed or returned as directed by the University in its sole discretion. Transfer to the University or a third party designated by the University shall occur within a reasonable period of time, and without significant interruption in service. Contractor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to University Data during the transition.

b. Upon termination or expiration of the Underlying Agreement, and after any requested transfer of data, Contractor must Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which Contractor might have transferred University Data. Contractor agrees to provide documentation of data destruction to the University.

c. Contractor will notify the University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and University Data and providing the University access to Contractor's facilities to remove and destroy University- Data. Contractor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. Contractor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the University. Contractor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.

6. Integration

This DPA applies in addition to, not in lieu of, any other terms and conditions agreed to between Contractor and University, including the Underlying Agreement(s), except as specifically and expressly agreed in writing with explicit reference to these Standards. This DPA governs in the case of any direct conflict with existing terms and conditions in the Underlying Agreement. Any limitations of liability or damages in the Underlying Agreement(s) will not apply to a breach by Contractor of this DPA.

7. Survival

Contractor's obligations under Section 5 shall survive termination of this DPA until all University Data has been returned or Securely Destroyed.

RFP 31203

Employee Health and EMR

Request for Proposals

VOLUME I

Required Submittals

(All but Financials)

Attachment A: "Specifications with Required Responses"

Attachment B: "Specs - IT and Tech, IT Security, HIPAA"

Attachment C: "MBE-WBE-SDVE Participation Form"

Attachment D: "Physician Self-Referral Questionnaire"

Attachment E: "IT Security Questionnaire"

Attachment PA: "Proposal Agreement"

ATTACHMENT A
SPECIFICATIONS WITH REQUIRED RESPONSES
RFP 31203 Employee Health and EMR

1.1 Objective:

To enter a long-term partnership with a professional team of experts in the support and maintenance of all phases and applications of a comprehensive Employee Health and EMR program.

1.2 Proposal Submission

See **Appendix 1**: Instructions to Respondents, Specific to this RFP, Section 2.6.

1.3 Proposal Requirements

A proposal must be submitted as prescribed by MUHC in this Request for Proposal (RFP).

Respondent shall provide thorough responses to all "specifications" below.

Failure to include any of the required information may result in rejection of the proposal.

- **Provide a Cover Letter** on your company's letterhead, signed by an authorized representative with the ability to commit to the performance of services outlined in the proposal. The letter should also identify all materials and enclosures submitted in response to this RFP.
- **Qualifications**
    - **Company Overview and Organizational Information:**
        - Provide a detailed description of your organizational structure, including parent company, subsidiaries, years in business, headquarters location, and the approximate percentage of your operations dedicated to this solution.
        - Introduce your company by summarizing its history, ownership structure, business activities, corporate direction, qualifications, certifications, and development history related to this solution. Include an overview of your broader product and service offerings.
        - Provide profiles of the principals and key staff who play a role in delivering this solution, highlighting relevant expertise and responsibilities.
        - State your credit rating from **Moody's Investor Services** and/or **Standard & Poor's.** If your company is not rated, provide alternative evidence of financial stability and strength.
    - **Experience, Expertise, and Client Success:**
        - Provide a comprehensive overview of your team's experience and expertise with Employee Health and EMR, including success stories and supporting statistics.
        - Describe your customer support approach, specifically in the areas of training, program assistance, system issue resolution, and ongoing application maintenance.
        - Confirm whether you maintain a documented **Business Continuity Plan** and **Disaster Recovery Plan** (if separate) and indicate whether these plans are tested annually.
        - Indicate the total number of clients currently utilizing this program. Of these, specify how many of these are healthcare organizations of at least 2,500 employees with multiple hospitals and healthcare clinics, supported with relevant statistics.
        - Provide details on at least three (3) current healthcare applications of your Occupational Medicine and EMR program that meet the following criteria: organizations of at least 2,500 employees with multiple hospitals and healthcare clinics, successfully deployed, fully functional, and in service for a minimum of two (2) years. Include the institution

names (contacts not required) and discuss both the successes and challenges associated with these implementations.

- **Unique Experience and Expertise:**
  - Describe the tools, methodologies, or strategies your company has developed that differentiate you from competitors.
  - Provide examples of specialized knowledge or experience within the healthcare industry, with emphasis on academic institutions and medical centers.
  - Share specific examples of how you support clients across hospitals, clinics, and practitioner environments.
  - Outline any partnerships with resellers, implementers, or other application providers, and explain how these collaborations enhance your ability to deliver these services.
- **Price Structure:**
  - **As costs are not considered in the initial evaluations, complete and submit "Attachment FW – Financial Worksheet" separately as "Volume II."**
  - You may modify or submit an alternate Pricing Worksheet, but either way this must be comprehensive and inclusive of all expenses over the anticipated term of this contract; The initial contract term shall be five (5) years. Beginning with year three (3), the contract shall continue to automatically renew on an annual basis unless either party provides written notice of non-renewal in accordance with the requirements set forth in the executed agreement.
- **References:**
  - If selected as a finalist in this RFP process, your firm may be asked to provide the facility name, contact name, and contact information for at least three (3) healthcare clients currently using your Employee Health and EMR program. Each reference must represent a deployment that is fully implemented, operational for a minimum of two (2) years, and within an organization of at least 2,500 employees with multiple hospitals and healthcare clinics, aligning closely with the scope of this RFP.
- **Attachments (must provide the following with the proposal):**

  Be certain to thoroughly complete, identify, and submit "Volumes" **separately**.

  - **Volume I** – Attachments A (this document), plus

    B, C, D, E, F and PA: Proposal Agreement
  - **Volume II** – Attachment FW: Financial Worksheet

1.4 SPECIFICATIONS

For evaluation purposes, please support your 'Yes' or 'No' selection with enough detail to demonstrate understanding, methodology, and value as applicable.

CRITICAL: A "**No**" to a "**MANDATORY**" item may eliminate the Respondent from further consideration! Please ensure that you thoroughly justify a "No" in your response so that we may consider the reason you are not able to provide the mandatory item, e.g., *"We are developing this and expect to have it by…"*

Criterion 1: IT and Technical, IT Security, HIPAA (Attachment B)
Criterion 2: System Functionality and Workflow Integration
Criterion 3: Compliance, Reporting, and Analytics
Criterion 4: Data Integration and Migration
Criterion 5: User Access, Communication, and Support
Criterion 6: Implementation, Scalability, and Enterprise Risk Management (ERM)
Criterion 7: Strategic Roadmap – Upcoming Initiatives

Criterion 1: IT and Technical, IT Security, HIPAA

This criterion is "**Attachment B**" that **must be completed and submitted** with the proposal as an extension of these specifications.

Criterion 2: System Functionality and Workflow Integration

(Covers registration, documentation, usability, and core employee health operations)

MANDATORY

1. System supports comprehensive employee health management, including immunizations, compliance management, communication, surveillance programming, fit testing, and exposure tracking.

   Provided? Yes ☐ No ☐

   Response:

2. Registration and record maintenance for multiple populations with single and concurrent appointments.

   Provided? Yes ☐ No ☐

   Response:

3. Customizable forms, surveys, and/or templates for documentation of clinical encounters, tests, and surveillance events. **Provided? Yes ☐ No ☐**

   Response:

4. Scalable design to support multi-facility and multi-campus operations under MU Health Care.

   Provided? Yes ☐ No ☐

   Response:

5. Integration with university HR systems. **Provided? Yes ☐ No ☐**

Response:

6. Staff self-service for access of information and submission of clinical documentation.

   Provided? Yes ☐ No ☐

   Response:

7. Ongoing support maintenance for new or modified tests/results with interface mapping and workflow.

   Provided? Yes ☐ No ☐

   Response:

DESIRABLE

1. Scheduling tools for immunizations, fit tests, and appointments. **Provided? Yes ☐ No ☐**

   Response:

2. Electronic signature support for consent and acknowledgment forms. **Provided? Yes ☐ No ☐**

   Response:

3. Occupational medicine module for injury tracking and work-related visits. **Provided? Yes ☐ No ☐**

   Response:

4. Configurable role-based workflows tailored to academic and clinical departments. **Provided? Yes ☐ No ☐**

   Response:

ADDITIONAL INFORMATION

1. How would you generate custom surveys to meet facility policy standards and expectations?

   Response:

Criterion 3: Compliance, Reporting, and Analytics

(Addresses regulatory compliance, auditability, and decision support)

MANDATORY

1. Secure audit logs capturing all record changes. **Provided? Yes ☐ No ☐**

   Response:

2. Standardized reports suitable for internal, university, and state audits. **Provided? Yes ☐ No ☐**

   Response:

3. Ability to export or summarize compliance data for The Curators of the University of Missouri and public reporting obligations. **Provided? Yes ☐ No ☐**

   Response:

4. Role-based dashboards available for staff, managers, and administrators. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Real-time dashboards displaying compliance by department, campus, or population.

   Provided? Yes ☐ No ☐

   Response:

2. Automated alerts for upcoming expirations or missed compliance items. **Provided? Yes ☐ No ☐**

   Response:

3. Predictive analytics for risk identification (e.g., outbreak or exposure clustering). **Provided? Yes ☐ No ☐**

   Response:

4. Integration with HR absence/leave systems for return-to-work monitoring. **Provided? Yes ☐ No ☐**

   Response:

Criterion 4: Data Integration and Migration

(Covers interoperability, data transfer, and governance alignment)

MANDATORY

1. Secure migration of existing employee health data, including medical records and uploaded documents.

   Provided? Yes ☐ No ☐

   Response:

2. Standards-based interoperability (HL7, FHIR, API, CSV) with Oracle Millenium. **Provided? Yes ☐ No ☐**

   Response:

3. Interface with laboratory system for ordering and results. **Provided? Yes ☐ No ☐**

   Response:

4. Integration with Missouri state immunization registries. **Provided? Yes ☐ No ☐**

   Response:

5. Alignment with MU and State of Missouri data governance and retention policies. **Provided? Yes ☐ No ☐**

   Response:

6. Encryption of all data in transit and at rest in accordance with HIPAA and university IT policies. **Provided? Yes ☐ No ☐**

   Response:

7. LDAP/Active Directory synchronization for provisioning and deactivation. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Bi-directional data exchange between systems in real time. **Provided? Yes ☐ No ☐**

   Response:

2. Integration with occupational exposure and incident management tools. **Provided? Yes ☐ No ☐**

   Response:

3. Archival access for historical records and reporting. **Provided? Yes ☐ No ☐**

   Response:

4. Data segmentation enabling secure sharing among HR, Employee Health, and academic programs.

   Provided? Yes ☐ No ☐

   Response:

5. Interface with radiology and ePrescribe for ordering. **Provided? Yes ☐ No ☐**

   Response:

Criterion 5: User Access, Communication, and Support

(Covers access control, SSO, communication, and vendor support)

MANDATORY

1. Single Sign-On (SSO) integration with MU Health Care and University of Missouri identity systems.
   Provided? Yes ☐ No ☐
   Response:

2. Secure internal messaging between Employee Health staff and employees. **Provided? Yes ☐ No ☐**
   Response:

3. Web-based employee portal accessible across devices and facilities. **Provided? Yes ☐ No ☐**
   Response:

4. Vendor-provided implementation support, training materials, and "train-the-trainer" sessions.
   Provided? Yes ☐ No ☐
   Response:

5. Defined Service Level Agreement (SLA) with escalation paths and response metrics.
   Provided? Yes ☐ No ☐
   Response:

DESIRABLE

1. Tiered support model with dedicated account management. **Provided? Yes ☐ No ☐**
   Response:

2. Online knowledge base, e-learning modules, and user community access. **Provided? Yes ☐ No ☐**
   Response:

3. Configurable broadcast communications for enterprise-wide health notices. **Provided? Yes ☐ No ☐**
   Response:

4. Change-management plan with communication templates and adoption metrics. **Provided? Yes ☐ No ☐**
   Response:

5. Regular account reviews and quarterly performance reporting. **Provided? Yes ☐ No ☐**
   Response:

Criterion 6: Implementation, Scalability, and Enterprise Risk Management (ERM)

(Addresses deployment, sustainability, and alignment with MU's enterprise risk program)

MANDATORY

1. Documented, comprehensive, and time-tested implementation methodology (see Additional Information below for providing detailed information).

   Provided? Yes ☐ No ☐

   Response:

2. Defined risk-identification, mitigation, and monitoring processes during rollout and ongoing operations.

   Provided? Yes ☐ No ☐

   Response:

3. Scalability to support multi-entity use under The Curators of the University of Missouri.

   Provided? Yes ☐ No ☐

   Response:

4. Compliance with state procurement, contracting, and funding policies for public institutions.

   Provided? Yes ☐ No ☐

   Response:

5. Sandbox/test environment for configuration validation. **Provided? Yes ☐ No ☐**

   Response:

6. Integration with enterprise reporting tools (e.g., Power BI) for governance dashboards.

   Provided? Yes ☐ No ☐

   Response:

DESIRABLE

1. Phased rollout plan aligned with ERM risk thresholds. **Provided? Yes ☐ No ☐**

   Response:

2. Post-implementation performance metrics and lessons-learned documentation. **Provided? Yes ☐ No ☐**

   Response:

ADDITIONAL INFORMATION

1. Provide a comprehensive implementation plan detailing project scope, timeline, resource requirements, training approach, system integrations, testing protocols, go-live methodology, and post-go-live support structure.

   Response:

Criterion 8: Strategic Roadmap – Upcoming Initiatives

(*Evaluates planned initiatives and innovations and alignment with the organization's long-term goals*)

Please provide a roadmap for the next three to five years, outlining planned product and/or service enhancements, key milestones, anticipated release timelines, and a description of how these initiatives will support long-term alignment, innovation, and the sustained success of this engagement.

Response:

ATTACHMENT B
SPECIFICATIONS WITH REQUIRED RESPONSES
IT and Technical, IT Security, HIPAA

RFP 31203 Employee Health and EMR

1.1 SPECIFICATIONS

Most of these specifications will only require a 'Yes' or 'No' selection; however, when applicable, responses should include sufficient detail to demonstrate understanding and methodology.

CRITICAL: A "**No**" to a "**MANDATORY**" item may eliminate the Respondent from further consideration! Please ensure that you thoroughly justify a "No" in your response so that we may consider the reason you are not able to provide the mandatory item, e.g., *"We are developing this and expect to have it by…"*

- **Criterion 1**: Application Specifications (if a "BAA" is required)
- **Criterion 2**: Application Specifications (Security Related)
- **Criterion 3**: Application Specifications (Non-Security Related)
- **Criterion 4**: Documentation That Will Be Requested for Security Review

Criterion 1: **Application Specifications (if a "Business Associate Agreement" [BAA] is required)**

- Will this solution include any exposure to Protected Health Information (PHI), thus require a "Business Associate" relationship? *(See 'i' on the first from last page for PHI indicators)*

  Yes ☐ No ☐ / If "No" select "**N/A**" for numbers **1.** through **5.** and reply to number **6.**

MANDATORY

1. ***Solutions that require a BAA*** / Agree to enter a BAA provided by or agreed to by MU Health Care.

   Will Comply: Yes ☐ No ☐ N/A ☐

   Response:

2. ***Solutions that require a BAA*** / Will confirm that any subcontractors who have access to Protected Health Information (PHI) have signed a BAA with the vendor.

   Will Comply: Yes ☐ No ☐ N/A ☐

   Response:

3. ***Solutions that require a BAA*** / "Role-Based Access Controls" (RBAC) must support minimum necessary standard.

   Will Comply: Yes ☐ No ☐ N/A ☐

   Response:

4. ***Solutions that require a BAA*** / The solution meets "User Access Log Requirements" (see "ii" on last page)

   Will Comply: Yes ☐ No ☐ N/A ☐

   Response:

5. ***Solutions that require a BAA*** / Business Associate shall not disclose PHI to a subcontractor not within the borders and jurisdiction of the United States of America without the prior written consent of Covered Entity which may be withheld in its sole discretion.

   Will Comply: Yes ☐ No ☐ N/A ☐

   Response:

6. ***Solutions that DO NOT require a BAA*** / The solution logs access, modification, deletion, and export of data.

   Will Comply: Yes ☐ No ☐ N/A ☐

   Response:

Criterion 2: **Application Specifications (Security Related)**

MANDATORY

1. ***Any Solution*** / Provides evidence of secure coding practices, including framework adoption.

   Will Comply: Yes ☐ No ☐

   Response:

2. ***Any Solution*** / User accounts can be disabled or deactivated rather than deleted and disabled accounts are not subject to licensing.

   Will Comply: Yes ☐ No ☐

   Response:

3. ***Any Solution*** / Meets "Authentication Requirements" (see "iii" on last page)

   Will Comply: Yes ☐ No ☐

   Response:

4. ***Any Solution*** / Solution supports Microsoft Azure's Single-Sign-On through UM System's Azure instance or LDAP.

   Will Comply: Yes ☐ No ☐

   Response:

5. ***Any Solution*** / Solution supports unique user identification requirement.

   Will Comply: Yes ☐ No ☐

   Response:

6. ***Any Solution*** / Vendor utilizes zero trust methodology.

   On-prem Servers, Appliances, and Devices (if applicable) must:

   - Support residing in an isolated VLAN where inbound and outbound traffic must be allow-listed.
   - Support MUHC endpoint detection and response (malware protection).
   - Support operating systems that are not end of life support.

   Will Comply: Yes ☐ No ☐

   Response:

7. ***Any Solution*** / Solution supports Role-Based Access Controls (RBAC).

   Will Comply: Yes ☐ No ☐

   Response:

- *Select "**N/A**" for any of the following that this solution will not utilize, and no response would then be required:*

8. ***Solutions that need to send email where the "from" email address is from a UM domain*** (e.g., @health.missouri.edu, @umsystem.edu, @missouri.edu), the solution must support subdomains (e.g., @vendorsolution.health.missouri.edu).

   Will Comply: Yes ☐ No ☐ N/A ☐

   Response:

9. ***Solutions that are fully or partially hosted by the vendor, or where the vendor stores, processes, creates, receives, or transmits MUHC PHI*** / All PHI on vendor's systems and subsystems will be encrypted with industry approved encryption technology.

   Will Comply: Yes ☐ No ☐ N/A ☐

   Response:

10. ***Solutions that are fully or partially hosted by the vendor, or where the vendor stores, processes, creates, receives, or transmits MUHC data***. / Vendor will provide evidence of independent audit (SOC 2 Type 2, HITRUST, ISO 27001) where the scope of the audit covers the vendor's operational practices and technical controls **or** complete a HECVAT FULL (most recent version). **NOTE**: Independent audit is desired over HECVAT.

    Will Comply: Yes ☐ No ☐ N/A ☐

    Response:

11. ***Solutions that involve medical devices.*** / A "Manufacturer Disclosure Statement for Medical Device Security" (MDS2) is required.

    Will Comply: Yes ☐ No ☐ N/A ☐

    Response:

12. ***Solutions that involve a mobile app used by MUHC workforce.*** / Mobile apps must be capable of running under MUHC's Mobile Device Management solutions.

    Will Comply: Yes ☐ No ☐ N/A ☐

    Response:

13. ***Solutions that involve cloud-based, web-based, or API components.*** / Must provide complete vulnerability scan and penetration testing reports conducted within the past 12 months. **NOTE**: Independent vulnerability scan and penetration test is desired over internal.

    Will Comply: Yes ☐ No ☐ N/A ☐

    Response:

DESIRABLE

1. ***Solutions that involve cloud-based, web-based, or API components.*** / Supports Allow-Listing of University IP address.

    Provided: Yes ☐ No ☐ N/A ☐

    Response:

2. ***Solutions that involve desktop application.*** / Desktop application will not require admin privileges to be used by the end user of the application.

    Will Comply: Yes ☐ No ☐ N/A ☐

    Response:

Criterion 3: **Application Specifications (Non-Security Related)**

MANDATORY

1. ***Solutions requiring integration with MUHC EMR.*** / Solution supports integration to Oracle Electronic Medical Record (EMR) system.

    Will Comply: Yes ☐ No ☐ N/A ☐

    Response:

2. ***Solutions requiring the application of "Web Content Accessibility Guidelines" (WCAG)*** / Shall: (1) deliver all applicable services and products in reasonable compliance with University standards WCA Guidelines 2.1, Level AA or above; (2) provide the University with an Accessibility Conformance Report detailing the product's current accessibility according to WCAG standards using the latest version of the Voluntary Product Accessibility Template (VPAT); (3) if accessibility issues exist, provide a "roadmap" plan for remedying those deficiencies on a reasonable timeline to be approved by the University; (4) promptly respond to assist the University with resolving any accessibility complaints and requests for accommodation from users with disabilities resulting from Contractor's failure to meet WCAG 2.1 AA guidelines at no cost

to the University; and (5) indemnify and hold the University harmless in the event of any claims arising from inaccessibility.

Will Comply: Yes ☐ No ☐ N/A ☐

Response:

<u>Criterion 4</u>: Documentation That Will Be Requested for Security Review

1. ***Any Solution*** / Provide a general description of how the solution will be used.
   - For clinical use, describe what clinical procedures or type of patients.
   - For operational use, describe workflows, business processes, or analytic capabilities the solution provides.

   Will Provide if Awarded: Yes ☐ No ☐

   Response:

2. ***Any Solution*** / Where multiple subscriptions and options exist, provide a list specific subscription and options are included in RFP (or reference which document has information).

   Will Provide if Awarded: Yes ☐ No ☐

   Response:

3. ***Any Solution*** / List of all user-facing access points to the solution, such as web portals, mobile applications, or other interfaces. This does not require detailing every individual screen or page. The goal is to provide a clear understanding of each unique method by which users, whether patients, providers, or administrators, can access the system.

   Will Provide if Awarded: Yes ☐ No ☐

   Response:

4. ***Any Solution*** / Network requirements, including, but not limited to firewall rules.

   Will Provide if Awarded: Yes ☐ No ☐

   Response:

5. ***Any Solution*** / Describe solution's backup methodology.

   Will Provide if Awarded: Yes ☐ No ☐

   Response:

- *Select "**N/A**" for any of the following that this solution will not utilize, and no response would then be required:*

6. ***Solution will be fully or partially hosted by the vendor, or where the vendor stores, processes, creates, receives, or transmits MUHC data.*** / Recovery Time Objective (RTO) - Specify the maximum acceptable amount of time the solution may be unavailable during a disruption before normal operations are restored in alignment with the RTO.

   Will Provide if Awarded: Yes ☐ No ☐ N/A ☐

   Response:

7. ***Solution will be fully or partially hosted by the vendor, or where the vendor stores, processes, creates, receives, or transmits MUHC data.*** / Recovery Time Objective (RTO) - Documentation on how the vendor intends to meet and how they have tested the RTO.

   Will Provide if Awarded: Yes ☐ No ☐ N/A ☐

   Response:

8. ***Solution will be fully or partially hosted by the vendor, or where the vendor stores, processes, creates, receives, or transmits MUHC data.*** / Recovery Point Objective (RPO) – Specify the maximum acceptable amount of data loss measured in time (i.e., the point in time to which data must be restored following a disruption) in accordance with the solution's RPO.

   Will Provide if Awarded: Yes ☐ No ☐ N/A ☐

   Response:

9. ***Solution will be fully or partially hosted by the vendor, or where the vendor stores, processes, creates, receives, or transmits MUHC data.*** / Must provide complete vulnerability scan and penetration testing reports conducted within the past 12 months. **NOTE:** Independent vulnerability scan and penetration test is desired over internal.

   Will Provide if Awarded: Yes ☐ No ☐ N/A ☐

   Response:

10. ***Solutions where remote access is needed by the vendor to access servers or devices on MUHC's network.*** / Requirements and options for remote access.

    Will Provide if Awarded: Yes ☐ No ☐ N/A ☐

    Response:

11. ***Solutions requiring Application Registrations or service accounts.*** / Documentation of Azure Application Registrations or service accounts, including permissions that are needed.

    Will Provide if Awarded: Yes ☐ No ☐ N/A ☐

    Response:

12. ***Solutions that require desktop software to be installed.*** / Inventory of desktop-based software, modules, or add-ons, with documentation on what permissions are needed to install or run the application.

    Will Provide if Awarded: Yes ☐ No ☐ N/A ☐

Response:

13. ***Where the vendor intends to de-identify and use MUHC's data.*** / Documentation of intended use of MUHC's de-identified data. Include detailed description of how the data will be de-identified and if the vendor will be maintaining a mapping table (to re-identify a record) to the de-identified dataset.

    Will Provide if Awarded: Yes ☐ No ☐ N/A ☐

    Response:

[i] **Business Associate Agreement** (PHI Indicators)

If the services requested by MUHC via this RFP require the respondents to use and/or disclose protected health information (PHI), a "Business Associate" relationship exists. The following 19 identifiers, together or individually, may constitute PHI:

1. Names,
2. All geographic subdivisions smaller than a state
    - (e.g. street address, city, county, precinct, zip code),
3. All dates related to the individual
    - (e.g. date of birth, admission date, discharge date, date of death),
4. Telephone number,
5. Fax number,
6. Electronic mail addresses,
7. Social Security Number {SSN),
8. Medical record number,
9. Health plan numbers,
10. Account numbers,
11. Certificate or license numbers,
12. Vehicle identification/serial numbers, including license plate numbers,
13. Device identification/serial numbers,
14. Universal resource locators (URL's),
15. Internet protocol (IP) addresses,
16. Biometric identifiers,
17. Full face photographs and comparable images,
18. Genetic information, or
19. Any other unique identifying number, characteristic or code.

[ii] User Access Log Requirements

Record Access – when a user views the single record or partial record of an individual within the solution.
List Access – when a user views PHI presented in a list view (i.e., list of patients scheduled that day, list of patients based on search).

- The solution creates audit logs on the following:
  - When a user authenticates (login) to the solution.
  - When a user creates, modifies, or deletes a user of the solution.
  - When a user accesses, creates, modifies, or deletes PHI of an individual (**Record Access**).
  - When a user views PHI of individuals (List Access).
  - When a user exports PHI (e.g., creates a report, exports data to Excel or CSV).
- Logs contain the following information:
  - User identifier such as username.
  - Description of action.
  - Date and time of action.
  - Description of data accessed or reference window name (e.g., demographics, lab results, clinical note).
  - Identifier of patient(s) (e.g., name, patient ID number, or medical record number).
    - For **List Access,** having the ability to determine which patients were displayed when the user accessed the list would be an acceptable compensating control with confirmation from the vendor that the report was thorough and accurate.
- Access to Audit Logs: Customer can access the above-mentioned audit logs via the application.
- Log Retention: The above-mentioned audit logs are available for no less than 12 months.
- Log Integrity: Vendor implements protections to ensure that audit logs cannot be modified by the customer or vendor.

[iii] Authentication Requirements

The solution must support one of the following authentication methods:

- Single Sign-On (SSO) via the UM System's Microsoft Azure instance
- Integration with the UM' Systems LDAP directory
- Application-based authentication that meets the criteria outlined below

If using application-based authentication, the solution must:

- Support multi-factor authentication (MFA) using an authenticator app
- Alternatively, support email or SMS-based MFA combined with IP allow-listing

If the application is internet-accessible and hosted by the vendor:

The vendor must confirm that login activity logs are actively monitored for suspicious access attempts.

ATTACHMENT C
MBE/WBE/SDVE PARTICIPATION FORM

Evaluation of Supplier's MBE/WBE/SDVE Participation: If a Respondent is proposing participation by a Minority Business Enterprise (MBE), Women Business Enterprise (WBE), or Service-Disabled Veteran Enterprise (SDVE), in order to receive evaluation consideration for participation by the MBE/WBE/SDVE, the Respondent must provide the required information with the proposal. Information not included with the proposal will not be considered in scoring.

MBE/WBE Evaluation: The Respondent's proposed MBE/WBE participation will be considered in the evaluation process as follows:

a. If Participation Meets or Exceeds Target: Respondents proposing MBE and/or WBE participation percentages that meet or exceed the target participation percentage of 10% for MBE and 5% for WBE shall be assigned the maximum stated MBE/WBE Participation evaluation points.
b. If Participation Below Target: Respondents proposing MBE and/or WBE participation percentages that are lower than the target participation percentages of 10% for MBE and 5% for WBE shall be assigned a proportionately lower number of the MBE/WBE Participation evaluation points than the maximum MBE/WBE Participation evaluation points.
c. If No Participation: Respondents failing to propose any commercially useful MBE/WBE participation shall be assigned a score of 0 in this evaluation category.

SDVE Evaluation: The respondent must either be a SDVE or must be proposing to utilize a SDVE as a subcontractor and/or supplier that provides at least three percent (3%) of the total contract value. If the Respondent proposing a SDVE participation percentage meets or exceeds three percent (3%) of the total contract value and provides the required documentation identified herein, then the Supplier shall be assigned the three (3) bonus points.

MBE/WBE/SDVE Commitment: If the Respondent is awarded a contract and the Respondent received points for the MBE/WBE/SDVE participation in the evaluation, the percentage level of MBE/WBE/SDVE participation committed to by the Respondent shall be a contractual requirement.

Spending with MBE/WBE/SDVE Companies: If you are a certified MBE, WBE, SDVE, as defined in the Instructions to Respondents, section #9, please check the appropriate selection below and provide evidence of certification.

Minority Business Enterprise _____
Women Business Enterprise _____
Service-Disabled Veteran Business _____
None of the Above _____

MBE/WBE/SDVE Certified in Missouri: Are you a MBE/WBE/SDVE certified by the State of Missouri, Office of Administration? YES _____ or NO _____

If YES was checked above as being a certified MBE/WBE by the State of Missouri, Office of Administration, provide the name of the MBE/WBE the certificate is under and the certification number. _____

If YES was checked above as being a certified SDVE by the State of Missouri, Office of Administration, provide the name of the SDVE your certificate is under. _____

If you are not a certified MBE/WBE/SDVE, are you willing to commit to using one or more certified MBE/WBE/SDVE companies in the performance of this contract if awarded? If yes, please explain the nature of the participation by each MBE/WBE/SDVE and provide the percentage of the contract value that will be attributable to such MBE/WBE/SDVE and evidence of certification.

- Yes: ____ Nature of Participation: _____ Percentage: ____

----------THIS FORM MUST BE SUBMITTED WITH THE RESPONSE----------

ATTACHMENT D
PHYSICIAN SELF-REFERRAL QUESTIONNAIRE

Section I – Company Ownership

1. Is your company a publicly traded stock company with more than $75 million in stockholder equity? NO: _____ YES: _____
2. Is your company a public agency? NO: _____ YES: _____

Section II – Physician Relationship

For purpose of answering these questions, the term "immediate family member" means the following individuals: husband or wife; natural or adoptive parent, child or sibling, stepparent, stepchild, stepbrother or stepsister, father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, or sister-in-law, grandparent or grandchild, and spouse of a grandparent or grandchild.

1. Is your company owned or governed in whole or part by a physician (or an immediate family member of a physician) who may refer patients or treat patients at a MU Health Care facility? NO: ___ YES: ___
2. Is your company owned or governed in whole or part by any person (other than a physician or immediate family member of a physician) who may refer patients to a MU Health Care facility? NO: _____ YES: _____
3. Does your company employ or contract with a physician (or an immediate family member of a physician) who may refer patients or treat patients at a MU Health Care facility? NO: _____ YES: _____
4. Does your company have compensation arrangements with a physician (or an immediate family member of a physician) that vary with or take into account the volume or value of referrals or other business generated by the physician for a MU Health care facility? NO: _____ YES: _____

If you answered "Yes" to any of the questions 1-4 of Section II, please provide the applicable physician's name(s), the person(s) who refers patients to the health care facilities, the name(s) of the health care facilities, and if applicable, the name(s) of the immediate family members of the physicians or other person.

_____

_____

_____

I represent the answers provided herein are truthful and accurate as of the date of my signature below. I agree to immediately notify the Director of MUHC Supply Chain Operations at 2910 LeMone Industrial Blvd., Columbia, MO 65201 of any changes in the above disclosed information.

_____
Company Name

_____
Signature Date

_____
Print Name Title

University of Missouri
Information Security Requirements

Vendors must demonstrate compliance with the security criteria listed below by responding in writing to every statement and question in the identified categories. Validation of the answers provided by the vendor may be conducted during the review/audit process. Any erroneous information could limit the vendor's ability to finalize implementation of a new solution or place a hold on continued use of a current solution. Vendors are expected to maintain an awareness of the laws and regulations applicable to the use of the solution in a University environment.

Data Classification

LINKS: https://www.umsystem.edu/ums/is/infosec/classification https://www.umsystem.edu/ums/is/infosec/classification-definitions

The University uses a "Data Classification System" (DCS) to assign "Data Classification Levels" (DCL) for all University owned or hosted IT-based systems. This system will have a DCS Level of 4 . Security requirements for the DCS can be found at: https://www.umsystem.edu/ums/is/infosec/classification & .../classification-definitions (links above). The University of Missouri reserves the right to periodically audit any or all hardware and/or software infrastructure provided by the vendor to ensure compliance with industry standards and best practices as well as the requirements of the University's DCS. When applicable, the University of Missouri requires compliance with the Health Insurance Portability and Accountability Act (HIPAA), FERPA, GLBA, PCI specifications, and all other applicable state, local and federal laws and regulations.

The University considers security to be an ongoing responsibility and as a result, these information security criteria are subject to additions and changes without warning. When appropriate, the vendor will be expected to work in good faith with the University to maintain compliance with new laws and regulations and/or to improve the security of the solution.

Compensating Controls and Descriptions

All statements and questions below are mandatory unless they are not applicable. The vendor must clearly explain why a given question is not applicable. For all other questions, if a requirement cannot be met, the vendor still has an opportunity to meet the requirement by the use of compensating controls. Compensating controls must be described in full in the appropriate column, including a full explanation of the compensating control detailing how the control meets the intent of the original question. In some instances, the University has requested that the vendor provide a description to accompany their response to a particular statement or question below. Descriptions are requested when a "Meets or Exceeds" answer alone could be deceptive without further detail.

When more room is needed to fully explain the compensating control or provide further detail, attachments can be included so long as such attachments are labeled and cross-referenced in the "Comments or Explanations of compensating controls" column. The University has the sole right to determine if a proposed compensating control is acceptable and if the details provided describe a solution that truly meets or exceeds the University's needs.

Vendor/Product Information (MUST BE COMPLETED)

Vendor Name and Contact Information _____

Product Name and Brief Description _____

_____

Does this solution store and/or transmit any of the following types of restricted and/or highly restricted data? Check all that apply.

___ Protected Health Information (PHI); ___ Payment Card Industry (PCI); ___ Gramm-Leach-Bliley Act (GLBA); ___ Social Security Numbers (SSN); ___ Federal Educational Rights & Privacy Act (FERPA)

___ Biometric Data (fingerprints, handprints, etc.); ___ Personally Identitiable Information (PII); ___ Intellectual Property; ___ Confidential Research

Vendor represents and warrants that their responses to the above questions are accurate and that the system configuration will continue to conform to these answers unless mutually agreed upon by the University and the Vendor. Vendor further agrees to work with the University in good faith to maintain compliance with new laws and regulations and/or to improve the security of the system.

Agreed this _____ day of _____, 20__

_____
Company Name

_____
Signer's Name and Title

_____
Signature

University of Missouri
Information Security Requirements

Requirements	This is DSC Level 4	Meets "X"	Does Not Meet "X"	Comments/Compensating Control
1. The vendor must acknowledge and agree to allow the University, at its discretion, to inspect/assess all or portions of the proposed solution prior to placing the system into production. The University does not need the vendors "code" to perform such assessments, however, the University will use web application (IBM AppScan, HP WebInspect) and network vulnerability tools (Nessus) in coordination with the vendor's technical team when appropriate. The results of the assessment(s) will be provided to the University customer (i.e., the department) and to the vendor.	All			
1.a The vendor must agree to remediate high risk security vulnerabilities that are identified by such assessments within a reasonable time frame and at no cost to the University. Medium and low risk vulnerabilities should also be remediated but will be scheduled for remediation based on a mutually agreeable timeframe. (This applies to generally accepted security vulnerabilities within the industry, NOT changes or modifications that would be considered customer-requested improvements or functionality enhancements.)	All			
2. Upon request, details of any third party reviews related to industry or regulatory compliance must be made available for University review. Vendor MUST include third party web application and server vulnerability and/or penetration tests if available. Redacted reports are acceptable. Please check all that are available: **___ SOC2 Report; ___ HiTrust Certification; ___ Other;** **___ None available**	DCL3 and DCL4			
3. Vendor must comply with applicable industry standards and best practices for system administration and application development (i.e. OWASP). Indicate which industry standards are utilized by the vendor.	All			
4. If applicable, Payment Card Industry - Data Security Standard (PCI-DSS) or Payment Data Security Standard (PA DSS) compliance is required. The vendor can comply with this item if it has attained PCI certification for the overall set of products/services being proposed or by having one or more system implementations that are currently PCI certified. Provide evidence of such certification attached to the response. If available, the vendor must provide a guide for PCI-compliant implementation of their product.	DCL4			

University of Missouri
Information Security Requirements

Requirements	This is DSC Level 4	Meets "X"	Does Not Meet "X"	Comments/Compensating Control
Authentication, Authorization and Password Security				
1. The University requires that the vendor allow authentication to their system through existing University authentication methods. For on-campus systems, Shibboleth/SAML2.0 (preferred) or Microsoft Active Directory (AD) is required. For vendor-hosted systems, Shibboleth/SAML 2.0 (SP initiated) is required. Vendor must provide their Shibboleth/SAML 2.0 integration documentation. Please check all that are supported: **___ Windows AD; ___ LDAP; ___ Shibboleth/SAML 2.0; ___ Other**	DCL2, DCL3 and DCL4			
2. For vendor-hosted systems that are unable to implement or are not required to use Shibboleth/SAML 2.0 (SP initiated) at the University's discretion, the vendor must meet the following University Password Standards: • Passwords requirements must be enforced and meet the University Password Standard https://www.umsystem.edu/ums/is/infosec/standards-password. • Passwords must be stored in a manner such that they are not decryptable. (This usually means a one-way hash and salt). • Password recovery mechanisms must be in place for users who forget their password. • The authentication session must be encrypted. (HTTPS for web applications). • Support for SSL v2/v3 and TLS 1.0 must be disabled. Only TLS 1.2 should be supported, 1.1 if necessary.	DCL2, DCL3 and DCL4			
Application Security				
1. The database must be segregated from front-end systems (i.e web and application servers.) Please describe how this is accomplished.	DCL3 and DCL4			
Cryptography/Encryption				
1. Except for the viewing of static Web pages, the vendor must ensure that all other transmissions to and from the system, including file transfers, data in process, authentication mechanisms, end-user and administrator access, etc. are handled via encrypted protocols.	All			
2. Any data stored at rest on a hard drive, on a file server and/or in a database MUST be encrypted or granted an exception by the appropriate Information Security Officer at https://www.umsystem.edu/ums/is/infosec/admin/	DCL4			

University of Missouri
Information Security Requirements

Requirements	This is DSC Level 4	Meets "X"	Does Not Meet "X"	Comments/Compensating Control
Answer These Additional Questions If The Proposed Solution Will Be Vendor Hosted				
1. The vendor must immediately disable all or part of the system functionality should a security issue be identified.	All			
2. The University requires notification of actual or suspected security incidents/breaches within **24** hours of the vendor's first knowledge of such an event.	All			
3. The proposed solution must be behind a firewall to protect and limit access to the system.	DCL3 and DCL4			
4. The vendor must ensure that University of Missouri owned or provided data is segregated and protected from other customers. Please describe how this is accomplished.	All			
5. The vendor must always change vendor-supplied defaults before installing a system on the network.	All			
6. The vendor must remove or disable unnecessary default accounts before installing a system on the network.	All			
7. The vendor must prohibit group, shared, or generic accounts, passwords, or other authentication methods as follows: • Generic user IDs and accounts are disabled or removed; • Shared user IDs for system administration activities and other critical functions do not exist; and • Shared and generic user IDs are not used to administer any system component.	All			
8. The vendor must configure user password parameters to require passwords meet the following: • Minimum password length of 8 characters • Contain both alphabetic and numeric characters	All			
9. The application/system/environment must be monitored consistently (24x7) for integrity and availability. Data center is hosted by: ___ **Vendor**; ___ **Third party** (please specify)	All			
10. The system must provide user access logs: • Will you provide on-line access to query the logs?; • If not, can you SFTP the log to our Splunk instance?; • If not, can you provide a report on a schedule or on demand?; • What security events are logged?; • How long are access and security logs retained?; • Describe backup recovery and resiliency of information system; and • Do logs contain ePHI? If yes, which identifiers are collected?	DCL3 and DCL4			

ATTACHMENT PA
PROPOSAL AGREEMENT

RFP 31203 Employee Health and EMR

By signing below:

- We have thoroughly examined the Scope of Work, and being familiar with the requirements, hereby agree to furnish all labor, supplies, licenses, and fees to offer the services as stipulated and set forth herein.
- We agree that this Proposal may not be withdrawn for a period of ninety (90) calendar days after the scheduled closing time for the receipt of Proposals.

By signing below, the representatives of this firm hereby certify that:

- The Proposal is genuine and is not made in the interest of or on behalf of any undisclosed person, firm or corporation, and is not submitted in conformity with any agreement or rules of any group, association or corporation.
- We have not directly or indirectly induced or solicited any other firm to put in a false or sham proposal.
- We have not solicited or induced any person, firm, or corporation to refrain from proposing.
- We have not sought by collusion or otherwise to obtain for themselves any advantage over any other firm or over MUHC.
- To the best of our knowledge and belief, we or our principals are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency in accordance with Executive Order 12549 (2/18/86).
- In connection with the furnishing of equipment, supplies, and/or services under the contract, the supplier and all subcontractors shall not discriminate against any recipients of services, or employees or applicants for employment on the basis of race, color, national origin, ancestry, religion, sex, pregnancy, age, disability, protected veteran status, or any other status protected by applicable state or federal law.

By signing below, the representatives of this firm declare that:

- We have received amendment(s) **0** through **0** .
- We had an opportunity to inquire about any uncertainties and have a general understanding of the requirements of this project.
- We have carefully prepared this Proposal, and the cost of the services required is accurate.
- All information submitted in this Proposal is correct and it contains no falsified records.

Respectfully submitted by:

Authorized Signature Date

Printed Name Title

Company Name:	
Mailing Address:	
City, State, Zip:	
Phone Number:	**Fed Employer ID No**:
Fax Number:	**E-Mail Address**:
Number of calendar days delivery after receipt of order: _____	Payment Terms: _____ Net 30 is default. Early pay discounts encouraged.
Select Payment Method: SUA ACH Check	
Type of Business: Individual Partnership Corporation Other: __	
If a corporation, incorporated under the laws of the State of:	
Licensed to do business in the State of Missouri: ☐ Yes ☐ No	
Business headquarters located in Missouri: ☐ Yes ☐ No	
Maintains a regular place of business in the State of Missouri: ☐ Yes ☐ No	

RFP 31203

Employee Health and EMR

Request for Proposals

VOLUME II

Required Submittal

(Financials**)**

Attachment FW: "Financial Worksheet"

ATTACHMENT FW
FINANCIAL WORKSHEET

RFP 31203 Employee Health and EMR

Important: This is a sample Pricing Worksheet. You may modify this or submit an alternate worksheet, but either way this must be comprehensive and inclusive of all expenses over the anticipated term of this contract.

NOTE: The initial contract term shall be five (5) years. Beginning with year three (3), the contract shall continue to automatically renew on an annual basis unless either party provides written notice of non-renewal in accordance with the requirements set forth in the executed agreement.

Please provide pricing details for each of the following items:

a. Total Year 1 Total Estimated Cost $_____

Year 1 Itemization

i. _____ $_____

ii. _____ $_____

iii. _____ $_____

iv. _____ $_____

v. _____ $_____

vi. _____ $_____

vii. _____ $_____

viii. _____ $_____

ix. _____ $_____

b. Maintenance & Support Year 2 $_____

c. Maintenance & Support Year 3 $_____

d. Maintenance & Support Year 4 $_____

e. Maintenance & Support Year 5 $_____