Health Care

December 4, 2025

REQUEST FOR PROPOSAL 31201

Health Information Management's

Clinical AI Analyzer

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"

- **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"
  - 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 31201 Clinical AI Analyzer

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 Clinical AI Analyzer Overview and Background:

Enterprise Clinical Data Intelligence and Documentation Integrity Solution Description:

MU Health Care seeks to identify and implement a comprehensive technology solution designed to identify documentation opportunities and completeness in an automated fashion to improve efficiency of clinical documentation across the health system.

The platform should leverage advanced analytics, artificial intelligence, and interoperability with existing EHR and financial systems to identify documentation gaps, optimize coding integrity, and generate actionable insights that drive clinical and operational improvement.

The selected solution should provide intuitive dashboards, workflow automation, and evidence-based analytics to support clinicians, coders, and clinical documentation improvement teams. It must align with MU Health Care's mission to deliver high-quality, patient-centered care while maintaining compliance with regulatory documentation and coding standards.

Background Information:

Seeking technology to provide a second level clinical documentation review prior to discharge of coded visits to identify possible missed revenue and quality opportunities occurring after the first human level review. This tool will reduce possible revenue cycle leakage through human error.

Key Goals and Objectives:

1. **Clinical Documentation Integrity and Quality Improvement**
   a. Perform comprehensive analysis of 100% of patient charts (not limited to samples) to identify incomplete, inconsistent, or inaccurate documentation.
   b. Leverage AI and NLP to extract structured and unstructured data (e.g., labs, vitals, clinical notes, orders) to ensure complete and accurate clinical representation.
   c. Improve diagnostic accuracy, case mix index (CMI), and risk adjustment accuracy.
   d. Provide clinicians and CDI staff with actionable insights to support accurate and timely documentation at the point of care.
2. **Revenue Integrity and Financial Optimization**
   a. Identify missed or under-documented clinical conditions that affect coding and reimbursement in order to minimize revenue leakage across service lines.
   b. Support recovery of appropriate revenue through improved documentation and coding accuracy.
3. **Denial Management and Appeals Automation**
   a. Utilize AI-driven analytics to assist in identifying root causes of payer denials.

b. Generate evidence-based appeal letters and supporting documentation to streamline the appeals process.
c. Reduce manual effort, accelerate turnaround time, and increase overturn success rates for clinical denials.

4. **Enterprise Integration and Scalability**
   a. Integrate securely with MU Health Care's existing EHR, coding, and revenue cycle systems.
   b. Provide scalable architecture capable of handling enterprise-level data volumes across multiple hospitals and clinics.
   c. Ensure compliance with all relevant data security and privacy regulations (HIPAA, HITECH, etc.).
5. **Clinical Usability and Operational Efficiency**
   a. Deliver intuitive, clinician-friendly interfaces for CDI specialists, coders, and physicians.
   b. Offer configurable reporting and analytics dashboards for performance tracking and improvement monitoring.
   c. Support both retrospective and concurrent (real-time) documentation analysis workflows.

Operational Statistics:

Estimating 15,000 inpatient encounters for FY26 (July 1, 2025 – June 30, 2026)

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 "Attachments A and 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 RFP correspondences Register as Participant by submitting a very brief "Letter of Intent" (LOI) to Rick Hess at **RHess@Health.Missouri.edu**, referencing "**RFP 31201, Clinical AI Analyzer**" 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 (**Monday, December 15, 2025 @ 3:00 PM CT**), and the deadline for submitting proposals (**Wednesday, January 14, 2026 @ 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 31201, Clinical AI Analyzer**" in the subject.

NOTE: The deadline for submitting questions is **Monday, December 15, 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, January 14, 2026 @ 3:00 PM CT** in the following format:

- **To (Rick Hess)**: RHess@Health.Missouri.edu
- **Subject (must be)**: RFP 31201, Clinical AI Analyzer, Due: 01/14/26 @ 3:00 PM CT
- **Volume I (*Responses*) named**:
    - VI - Clinical AI Analyzer, Attach A-PA (Your Firm's Name) – YYMMDD *(date of submission)*
- **Volume II (*Financials*) named**:
    - VII - Clinical AI Analyzer, Attach FW (Your Firm's Name) – YYMMDD *(date of submission)*
- **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 - Clinical AI Analyzer, Attach A-PA (Your Firm's Name) – YYMMDD *(date of submission)*
- **Volume II (*Financials*) named**:
    - VII - Clinical AI Analyzer, Attach FW (Your Firm's Name) – YYMMDD *(date of submission)*

And must be submitted and received by **Wed, January 14, 2026 @ 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 31201, Clinical AI Analyzer
Due: 01/14/26 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, February 27, 2026.

RFP 31201

Clinical AI Analyzer

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 31201 Clinical AI Analyzer

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 **Clinical AI Analyzer**.

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 the Clinical AI Analyzer solution, 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 10,000 annual inpatients, supported with relevant statistics.
        - Provide details on at least three (3) current healthcare applications of the Clinical AI Analyzer solution that meet the following criteria: organizations of at least 10,000 annual inpatients, 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 Financial Worksheet, but either way this must be comprehensive and inclusive of all expenses over the anticipated term of this contract; This shall be a five 5-year contract: 3-year fixed term with years 4 and 5 one-year optional extensions that may be terminated for convenience with written notice as 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 Clinical AI Analyzer solution. Each reference must represent a deployment that is fully implemented, operational for a minimum of two (2) years, and with at least 10,000 annual inpatients, 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 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: Functional and Technical Capabilities
Criterion 3: Integration and Interoperability
Criterion 4: Revenue Improvement Outcomes/Ongoing return on investment
Criterion 5: Clinical Quality Opportunities
Criterion 6: Data Analytics and Artificial Intelligence Features
Criterion 7: User Experience and Workflow Optimization
Criterion 8: Reporting, Quality Metrics, and Performance Monitoring
Criterion 9: Implementation, Support, Training, and Maintenance
Criterion 10: Roadmap

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: Functional and Technical Capabilities

The solution should provide comprehensive features that support clinical documentation accuracy, coding integrity, and operational efficiency across multiple care settings.

MANDATORY

1. Provide end-to-end functionality that supports clinical documentation improvement (CDI), coding review, and physician query management. **Provided? Yes ☐ No ☐**

   Response:

2. Support concurrent and retrospective documentation review workflows. **Provided? Yes ☐ No ☐**

   Response:

3. Allow role-based access for clinical, coding, compliance, and administrative users. **Provided? Yes ☐ No ☐**

   Response:

4. Offer configurable workflows and templates tailored to different service lines and specialties.

   Provided? Yes ☐ No ☐

   Response:

5. Support deployment in on-premises, cloud, or hybrid environments. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Enable dynamic rule creation and modification by authorized administrators without vendor intervention.

   Provided? Yes ☐ No ☐

   Response:

2. Offer mobile accessibility for clinicians and reviewers. **Provided? Yes ☐ No ☐**

   Response:

3. Provide real-time alerts or notifications for documentation gaps or quality indicators.

   Provided? Yes ☐ No ☐

   Response:

Criterion 3: Integration and Interoperability

The solution must integrate with MU Health Care's enterprise EHR, coding, and analytics systems while maintaining data integrity and real-time synchronization.

MANDATORY

1. Demonstrate interoperability with MU Health Care's EHR and associated data systems via standard APIs (FHIR, HL7, etc.). **Provided? Yes ☐ No ☐**

   Response:

2. Support bidirectional data exchange between clinical and financial systems. **Provided? Yes ☐ No ☐**

   Response:

3. Maintain compliance with ONC and interoperability standards. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Provide connectors or interfaces for additional data sources (e.g., pharmacy, lab, and radiology systems).

   Provided? Yes ☐ No ☐

   Response:

2. Enable configurable data mapping and normalization without custom coding. **Provided? Yes ☐ No ☐**

   Response:

3. Offer integration documentation and certification history. **Provided? Yes ☐ No ☐**

   Response:

ADDITIONAL INFORMATION

1. Provide a detailed list of existing EHR and third-party integrations currently supported.

   Response:

2. Describe the typical implementation timeline and resources required for system integration.

   Response:

Criterion 4: Revenue Improvement Outcomes/Ongoing return on investment

The solution should apply advanced analytics, AI, or natural language processing (NLP) to identify documentation opportunities and drive actionable insights.

MANDATORY

1. Provide real-time dashboards and KPIs for DRG impact, acceptance rates, quality indicators.

   Provided? Yes ☐ No ☐

   Response:

2. Provide data visualization tools or dashboards for performance monitoring. **Provided? Yes ☐ No ☐**

   Response:

3. Ensure transparency of algorithms used for documentation recommendations. **Provided? Yes ☐ No ☐**

   Response:

4. Share before/after baselines and trend lines across 2–3 quarters, highlighting sustained improvements and any payer-specific nuances. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Provide real-time dashboards and KPIs for DRG impact, acceptance rates, quality indicators.

   Provided? Yes ☐ No ☐

Response:

2. Provide current customer results (acceptance rates, DRG accuracy lift, realized revenue corroborated to 835) at comparable health systems to include scope, elapsed time and governance approach.

   Provided? Yes ☐ No ☐

   Response:

Criterion 5: Clinical Quality Opportunities

The solution should apply advanced analytics, AI, or natural language processing (NLP) to identify documentation opportunities and drive actionable insights.

MANDATORY

1. Provide real-time dashboards and KPIs for DRG impact, acceptance rates, quality indicators.

   Provided? Yes ☐ No ☐

   Response:

2. Provide data visualization tools or dashboards for performance monitoring. **Provided? Yes ☐ No ☐**

   Response:

3. Ensure transparency of algorithms used for documentation recommendations. **Provided? Yes ☐ No ☐**

   Response:

4. Share before/after baselines and trend lines across 2–3 quarters, highlighting sustained improvements and any payer-specific nuances. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Clinical criteria and coding guidelines configured and used to per facility specific policies, payer specific logic and thresholds. **Provided? Yes ☐ No ☐**

   Response:

Criterion 6: Data Analytics and Artificial Intelligence Features

The solution should apply advanced analytics, AI, or natural language processing (NLP) to identify documentation opportunities and drive actionable insights.

MANDATORY

1. Use AI/NLP to detect potential documentation or coding discrepancies. **Provided? Yes ☐ No ☐**

Response:

2. Provide data visualization tools or dashboards for performance monitoring. **Provided? Yes ☐ No ☐**

   Response:

3. Ensure transparency of algorithms used for documentation recommendations. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Enable predictive analytics for case prioritization or quality improvement initiatives.

   Provided? Yes ☐ No ☐

   Response:

2. Offer clinician-facing feedback loops for continuous learning. **Provided? Yes ☐ No ☐**

   Response:

3. Provide configurable AI model parameters or explainable AI capabilities. **Provided? Yes ☐ No ☐**

   Response:

Criterion 7: User Experience and Workflow Optimization

The system should enhance user productivity and minimize administrative burden through intuitive, efficient interfaces.

MANDATORY

1. Provide a user-friendly interface accessible via modern web browsers. **Provided? Yes ☐ No ☐**

   Response:

2. Support customizable dashboards and task prioritization. **Provided? Yes ☐ No ☐**

   Response:

3. Ensure low system latency and minimal clicks for core workflows. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Include in-application collaboration tools or annotation features. **Provided? Yes ☐ No ☐**

Response:

2. Offer personalization settings (e.g., saved views, favorites, or filters). **Provided? Yes ☐ No ☐**

   Response:

3. Allow integration with single sign-on (SSO) and MU Health Care's identity management systems.

   Provided? Yes ☐ No ☐

   Response:

Criterion 8: Reporting, Quality Metrics, and Performance Monitoring

The solution should support standardized and ad hoc reporting to track CDI effectiveness, productivity, and compliance outcomes

MANDATORY

1. Provide out-of-the-box reports for documentation quality, coding accuracy, and financial impact.

   Provided? Yes ☐ No ☐

   Response:

2. Allow users to design and save custom reports without vendor assistance. **Provided? Yes ☐ No ☐**

   Response:

3. Offer real-time dashboards and exportable data in standard formats (CSV, Excel, PDF).

   Provided? Yes ☐ No ☐

   Response:

DESIRABLE

1. Provide benchmarking capabilities across departments or facilities. **Provided? Yes ☐ No ☐**

   Response:

2. Support scheduled report distribution and automated notifications. **Provided? Yes ☐ No ☐**

   Response:

Criterion 9: Implementation, Support, Training, and Maintenance

The vendor must demonstrate a structured and collaborative implementation process with strong post-deployment support and user education.

MANDATORY

1. Assign a dedicated project manager and technical lead for the duration of implementation.

Provided? Yes ☐ No ☐

Response:

2. Offer 24/7 technical support with defined response and resolution times. **Provided? Yes ☐ No ☐**

Response:

3. Provide initial and ongoing training for system administrators, clinicians, and end-users.

Provided? Yes ☐ No ☐

Response:

4. Include software updates, patches, and maintenance services as part of the agreement.

Provided? Yes ☐ No ☐

Response:

DESIRABLE

1. Offer self-service training materials (videos, guides, simulations). **Provided? Yes ☐ No ☐**

Response:

2. Provide periodic optimization reviews post-implementation. **Provided? Yes ☐ No ☐**

Response:

ADDITIONAL INFORMATION

1. Provide a comprehensive implementation plan with milestones, deliverables, risk mitigation strategies, project governance, data migration, testing, validation, and change management approach.

Response:

2. Describe your support escalation model and service level agreement (SLA) structure

Response:

Criterion 10: 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 31201 Clinical AI Analyzer

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 31201 Clinical AI Analyzer

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 31201

Clinical AI Analyzer

Request for Proposals

VOLUME II

Required Submittal

(Financials**)**

Attachment FW: "Financial Worksheet"

ATTACHMENT FW
FINANCIAL WORKSHEET

RFP 31201 Clinical AI Analyzer

Important: This is a sample Financial 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: This shall be a five 5-year contract: 3-year fixed term with years 4 and 5 one-year optional extensions that may be terminated for convenience with written notice as 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 $_____