Health Care

August 18, 2025

REQUEST FOR PROPOSAL 31200

Surgical Services and Sterile Processing

Procurement and Payment Bill-Only

for

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

(Hereafter referred to as **University**, **MUHC**, or **MU Health Care**)

CONTACT & SUBMITTALS

Rick Hess

Strategic Sourcing Specialist
Office: 573.882.1643
RJH2c4@Health.Missouri.edu

MUHC Quarterdeck Building
2401 LeMone Industrial Blvd, Ste 171
Columbia, MO 65201

Deadline for Questions/Explanations/Interpretations

August 27, 2025 @ 5:00 PM Central Time

Sealed or Emailed Proposals Accepted Until

September 12, 2025 @ 3:00 PM Central Time

ATTACHMENT A
INSTRUCTIONS TO RESPONDENTS, SPECIFIC TO THIS RFP
RFP 31200 Procurement and Payment Bill Only

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 & B1 / 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.

1.1 Introduction / Background / Insight:

A baseline assessment data analysis was completed that assessed University of Missouri Health Care's (MUHC) existing process and Electronic Health Records (EHR) and Enterprise Resource Planning (ERP) documentation accuracy. Most of the procedural spend data provided was missing crucial data elements needed for analysis. The spend data that was capable of analysis ($17M/$30+M) identified massive opportunities for:

Improving Item Master Integrity – (31% of spend associated with non-built items)

- EHR & ERP Documentation Accuracy – (69% of PO's missing surgical date, 31% of PO spend items were description only, >8% EHR Misdocumentation rate)
- Process Improvement – (18-day process variability from procedure to PO)

Since the data needed for an analysis was so incomplete, an estimated assessment of opportunity was provided using aggregated vendor provided customer data & MUHC's estimated bill-only spend volumes.

So…

We are seeking proposals in search of a solution that aligns clinical and financial data to ensure revenue data EHR always matches expense data ERP, giving greater line-of-sight visibility into procedural spending. MUHC wishes to accomplish the following through the implementation of a desired solution:

- Productivity: Reduce manual intervention and touchpoints by 80% (for OR teams, Supply Chain, and billing), and remove of all labor associated with automation of Purchase Order submissions (~50% of customer's bill-onlys).
    - 99% EHR documentation and bill price accuracy, 0 FTE touchpoints.
- Cost Avoidance: Target between 10-30% for Non-Contract Savings plus reduction of overspend and vendor fees
- Predictability & Profitability: ~10% of bill-only spend is mis-documented in patient record.

Misdocumentation = missed charges = missed revenue = understated costs = acting on erroneous information. (Impacts revenue, margins, analytics, etc.)

1.2 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 **RJH2c4@Health.Missouri.edu**, referencing "**RFP 31200, Procure & Pymt BO**" 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 (Wednesday, August 27, 2025 @ 5:00 PM CDT), and the deadline for submitting proposals (Friday, September 12, 2025 @ 3:00 PM CDT).

1.3 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.

1.4 Pre-Proposal Conference

There will not be a formal pre-proposal conference.

1.5 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 RJH2c4@Health.Missouri.edu,** referencing "**RFP 31200, Procure & Pymt BO**" in the subject.

NOTE: The deadline for submitting questions is **Wednesday, August 27, 2025 @ 5:00 PM CDT**.

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*

1.6 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.

1.7 Proposal Submission

OPTION 1 (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 **Friday, September 12, 2025 @ 3:00 PM CDT** in the following format:

- **To (Rick Hess)**: RJH2c4@Health.Missouri.edu
- **Subject (must be)**: **RFP 31200, Procure & Pymt BO, Due: 09/12/2025 by 3:00 PM CDT**
- **Volume I attached and named**:
  - VI - RFP 31200, Procure & Pymt BO, Attach B-PA (YYMMDD) – Your Firm's Name
- **Volume II attached and named**:
  - VII - RFP 31200, Procure & Pymt BO, Financials (YYMMDD) – Your Firm's Name
- **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.

OPTION 2 (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 attached and named**:
  - VI - RFP 31200, Procure & Pymt BO, Attach B-PA (YYMMDD) – Your Firm's Name
- **Volume II attached and named**:
  - VII - RFP 31200, Procure & Pymt BO, Financials (YYMMDD) – Your Firm's Name

And must be submitted and received by **Friday, September 12, 2025 @ 3:00 PM CDT** 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 31200, Procure & Pymt BO
Due: 09/12/2025 by 3:00 PM CDT

1.8 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 CDT date/time of the email, or an MUHC stamped CDT date/time on the proposal wrapper or other documentary evidence of receipt maintained by MUHC.

1.9 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.

1.10 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.

1.11 Evaluation of Proposals

MUHC will strive to complete the proposal and presentation reviews and issue a "Notice of Award" by the end of day **Wednesday, October 22, 2025**.

RFP 31200

Procurement and Payment Bill-Only

Request for Proposals

VOLUME I

Required Submittals

(All but Financials)

Attachment B: "Specifications with Required Responses"

Attachment B1: "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 F: "Data Protection Addendum"

Attachment G: "IdP Integration Questionnaire"

Attachment PA: "Proposal Agreement"

ATTACHMENT B
SPECIFICATIONS WITH REQUIRED RESPONSES

RFP 31200 Procurement and Payment Bill-Only

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 Procurement and Payment Bill-Only program.

1.2 Proposal Submission

See **Attachment A**: Instructions to Respondents, Specific to this RFP, Section 1.7.

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.

- **Proposal Cover Letter**: Provided on your letterhead and signed by a person who is authorized to commit to your company's performance of the services included in the proposal while identifying all materials and enclosures being forwarded in response to this RFP.
- **Qualifications**
    - **Organizational Structure and Profile of Principals and Key Staff:**
        - Provide a detailed description of the organizational structure… parent company and subsidiaries, number of years in business and headquarters location, and approximately what percentage of your operation focuses on this solution?
        - Introduce your company, its history, ownership interests, active business venues, corporate direction, qualifications and certifications, development history as pertaining to this solution, and an overview of your product offerings.
        - Provide your credit rating by "Moody's Investor Services" (and/or) "Standard & Poor's." If not rated by these agencies, provide evidence of your institution's financial strength.
        - Provide profiles of the Principals and Key Staff in the hierarchy in the delivery of this solution.
    - **General Experience and Expertise:**
        - Comprehensively discuss your team's experience and expertise with this Payment and Procurement Bill-Only solution including success stories and statistics to support achievements.
        - Describe your customer approach as it pertains to training, program assistance, system issues, and general maintenance of the application.
        - How many clients are currently utilizing these services? How many of these are in the healthcare field with a relative size operation? Support this with statistics.
        - Provide details of at least three (3) current applications of this Payment and Procurement Bill-Only solution in healthcare with a relative size operation, successfully deployed, fully functional, in service for at least two (2) full years, and most pertinent to the scope of this RFP. Provide the names of the institutions, although contacts are not required. Discuss successes as well as challenges of these applications.

- **Unique Experience and Expertise:**
    - Discuss any tools and strategies your company has developed that you feel separate you from the competition. Include any other details that you feel further supports your company's experience and expertise with this application.
    - Provide examples of special knowledge or understanding of the healthcare industry, especially academic and medical centers. Please describe any special knowledge in this realm.
    - Give specific examples of how you support your clients, especially in the hospital, clinic, and practitioner arenas.
    - Describe partnerships you have with resellers, implementers, or other application suppliers. Give details of any external partnerships that improve your ability to provide these services.
- **Implementation:**
    - Provide a comprehensive outline of an implementation typical to ours, estimated durations (days, weeks, months). Provide any scenarios that may impair your company's ability to proceed expeditiously with this plan and schedule.
- **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 presented with a Notice of Award, we may request the facility name, contact name, and contact information of at least three (3) separate clients who are currently utilizing your Payment and Procurement Bill-Only solution that is successfully deployed, fully functional, and has been in service for at least two (2) full years. References would be required to be in healthcare with a relative size operation, and most pertinent to 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 B (this document), plus

      B1, C, D, E, F, G and PA: Proposal Agreement
    - **Volume II** – Attachment FW: Financial Worksheet

1.4 SPECIFICATIONS

Proposal evaluations will heavily consider the "**Response:**", so please refrain from only selecting Yes or No.

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
Criterion 2: Integration with EHR and ERP
Criterion 3: Automation Capabilities
Criterion 4: Data Cleanliness
Criterion 5: Vendor Compliance Support
Criterion 6: Reporting
Criterion 7: Procurement-to-Payment Case Management
Criterion 8: Strategic Roadmap – Upcoming Initiatives

Criterion 1: IT and Technical, IT Security, HIPAA

This criterion is "**Attachment B1**" that **must be completed and submitted** with the proposal as an extension of these specifications!

Criterion 2: Integration with EHR and ERP

MANDATORY

1. Ability to read surgical case schedule in Oracle Cerner to create a matching case. **Provided? Yes ☐ No ☐**

   Response:

2. Ability to validate device documentation against GUDID. Important for upcoming compliance with UDI documentation in claims data.

   Provided? Yes ☐ No ☐

   Response:

3. Ability to trigger PO dispatch in Peoplesoft. **Provided? Yes ☐ No ☐**

   Response:

4. Ability to reconcile bills against Oracle Cerner patient record data, Peoplesoft Item Master pricing data, and Peoplesoft vendor contract data.

   Provided? Yes ☐ No ☐

   Response:

DESIRABLE

1. Ability to create automated (touchless) Purchase Orders. **Provided? Yes ☐ No ☐**

Response:

2. Ability to interface with TrackCore. **Provided? Yes ☐ No ☐**

   Response:

3. Utilizes Case Card Coordinators/Integrated Picklists. **Provided? Yes ☐ No ☐**

   Response:

ADDITIONAL INFORMATION

1. Explain integration methods utilized and required data points for all solutions in scope.

   Response:

2. Describe capabilities / segment compatibility to integrate with the Oracle (Cerner) Health item master?

   Response:

3. Provide entity names of healthcare clients (preferably 3 or more) that are utilizing the Oracle (Cerner) EMR and/or Peoplesoft with comparable scope and size of our operations including for each:

   Response:

   - What limitations or difficulties did they encounter during implementation and post-implementation?

     Response:

4. Provide entity names of healthcare clients (preferably 3 or more) that are utilizing Case Card Coordinators / Integrated Picklists with this system with comparable scope and size of our operations.

   Response:

Criterion 3: Automation Capabilities

MANDATORY

1. Can handle a complete surgical case from procurement to payment without human touchpoints.

   Provided? Yes ☐ No ☐

   Response:

2. Automated vendor management: vendor support outreach and confirmation, vendor bill submission / receipt, PO dispatch, vendor process updates

Provided? Yes ☐ No ☐

Response:

3. Automated bill reconciliation process to confirm item prices and quantities with Oracle Cerner, Peoplesoft Item Master, and vendor contract data to ensure data accuracy across systems.

Provided? Yes ☐ No ☐

Response:

4. Automated bill approval process to approve error-free bills through the bill review process.

Provided? Yes ☐ No ☐

Response:

5. Automated PO dispatch triggered directly in Peoplesoft. **Provided? Yes ☐ No ☐**

Response:

6. Configurable automation acceptance criteria based on case templates for procurement and vendor management; and based on cost thresholds for bill review and PO automation.

Provided? Yes ☐ No ☐

Response:

DESIRABLE

1. Automated GUDID data population. **Provided? Yes ☐ No ☐**

Response:

2. Provides sterile tray tracking. **Provided? Yes ☐ No ☐**

Response:

3. Connects to the Case Number. **Provided? Yes ☐ No ☐**

Response:

Criterion 4: Data Cleanliness

MANDATORY

1. History of achieving an EHR documentation accuracy rate of >99%. **Provided? Yes ☐ No ☐**

Response:

2. GUDID data documentation for items used in surgery. **Provided? Yes ☐ No ☐**

   Response:

3. Reconciliation with patient record, item master, vendor contract, and bill details. **Provided? Yes ☐ No ☐**

   Response:

4. Log cases and bills to serve as a back-up resource of financial and clinical data. **Provided? Yes ☐ No ☐**

   Response:

5. Ability to view data and reports on-demand. **Provided? Yes ☐ No ☐**

   Response:

6. Ability to download case data including bill, item, financial, and clinical information on-demand.

   Provided? Yes ☐ No ☐

   Response:

7. Identifies wasted items within the bill including the reason for the waste. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Captures serial, lot number, expiration numbers and dates. **Provided? Yes ☐ No ☐**

   Response:

2. Tracks duplicate items on the billing. **Provided? Yes ☐ No ☐**

   Response:

Criterion 5: Vendor Compliance Support

MANDATORY

1. History of 97% compliance by vendor reps with perioperative protocols. **Provided? Yes ☐ No ☐**

   Response:

2. Provides 24/7 support and dedicated account management. **Provided? Yes ☐ No ☐**

   Response:

3. Vendor-facing app in the iOS and Android app stores for vendor access. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Provides automated recall alerting. **Provided? Yes ☐ No ☐**

   Response:

Criterion 6: Reporting

MANDATORY

1. Ability to view data and reports on-demand. **Provided? Yes ☐ No ☐**

   Response:

2. Ability to download case data including bill, item, financial, and clinical information on-demand.

   Provided? Yes ☐ No ☐

   Response:

3. Ability to view a case in its entirety, from creation to close. Including files, items and pricing, case event logs, and associated users.

   Provided? Yes ☐ No ☐

   Response:

4. Includes a "variance" report for omitted/missing documentation and/or information that delays billing. This shall include missing or incorrect clinical documentation and/or missing or incorrect vendor information.

   Provided? Yes ☐ No ☐

   Response:

DESIRABLE

1. Includes an EDW (PowerBi) data integration for custom reporting. **Provided? Yes ☐ No ☐**

   Response:

2. Will align with MU Health Care's chargemaster and alert to items inactive or not present in the chargemaster.

   Provided? Yes ☐ No ☐

   Response:

Criterion 7: Procurement-to-Payment Case Management

MANDATORY

1. Ability to view a case in its entirety, from creation to close. Including files, items and pricing, case event logs, and associated users.

   Provided? Yes ☐ No ☐

   Response:

2. Ability to message with vendor reps directly through the platform. **Provided? Yes ☐ No ☐**

   Response:

3. Ability for reps to scan item codes to capture UDI information for compliance. **Provided? Yes ☐ No ☐**

   Response:

4. Notifications to reps regarding unread messages or support requests. **Provided? Yes ☐ No ☐**

   Response:

5. Ability for users to leave comments on cases to elaborate on unique situations. **Provided? Yes ☐ No ☐**

   Response:

DESIRABLE

1. Includes built in dispute resolution. **Provided? Yes ☐ No ☐**

   Response:

ADDITIONAL INFORMATION

1. Describe your method(s) for ensuring accurate tray content.

Criterion 8: Strategic Roadmap – Upcoming Initiatives

Please provide a current and forward-looking roadmap outlining your planned product and/or service enhancements over the next 1–3 years. Include major milestones, anticipated release timelines, and how these developments will improve and support the long-term success of this engagement.

Response:

ATTACHMENT B1
SPECIFICATIONS WITH REQUIRED RESPONSES
IT and Technical, IT Security, HIPAA

RFP 31200 Procurement and Payment Bill-Only

1.1 SPECIFICATIONS

Proposal evaluations will heavily consider the "**Response:**" for comparisons, so please refrain from only selecting Yes or No (unless the Criterion is not applicable to this solution).

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)?

  Yes ☐ No ☐ / If "No" select "**N/A**" for all the following and no response would then be required:

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 "i" 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:

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*** / If the solution needs 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 ☐

   Response:

3. ***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:

4. ***Any Solution*** / Meets "Authentication Requirements" (see "ii" on last page)

   Will Comply: Yes ☐ No ☐

   Response:

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

   Will Comply: Yes ☐ No ☐

   Response:

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

   Will Comply: Yes ☐ No ☐

   Response:

7. ***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:

8. ***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:*

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] 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.

[ii] 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 F
DATA PROTECTION ADDENDUM
(approved as of July 2025)

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.

Contractor Acceptance

Contractor Name

Contractor Representative Signature & Printed Name

Date of Signature

ATTACHMENT G

UM System IdP (ID Providers) Integration Questionnaire

			YES	NO
Requestor Contact Information (the University/department contact)				
	Requestor Name:	The Curators of the University of Missouri on behalf of University of Missouri Health Care		
	Requestor Email Address:	rjh2c4@health.missouri.edu		
	Requestor Phone Number:	(573) 882-1643		
	Requesting Department Name:	Supply Chain / Strategic Sourcing Specialist		
	Requesting Business Unit:	Hospital (HOSPT)		
External/Third Party Contact Information				
	Sales Contact Name:			
	Technical Contact Name:			
	Company:			
	Email address:			
Service Provider (SP) Information				
1	Name of application/service:			
2	Application URL:			
3	Description of application/service:			
4	Service Provider Solution (i.e. Shibboleth, OpenSAML 2 or other product):			
5	Is your entire site protected using SSL?			
	If no, will you use SSL to protect the authentication session?			
	If no, explain why:			

ATTACHMENT G

UM System IdP (ID Providers) Integration Questionnaire

		YES	NO
6	Will you be expecting attributes to be passed for authorization purposes?		
	If so, list and describe attributes:		
7	How will attributes be used in the application/service?:		
	- (i.e., given to third parties, used for reports, etc.)		
8	Will attributes be used for any other purpose?		
	If yes, how will attributes be stored and for how long?:		
9	Will attributes be stored?		
	If yes, how will attributes be stored and for how long?		
10	Do you support SP initiated SSO?		
11	Can you consume a metadata file?		
12	Does your SP support XML signature/encryption?		
13	Does your SP support signed/encrypted assertions?		
14	Will your SP metadata be emailed directly to us?		
15	Does your SP metadata file contain, at a minimum, the following components?		
	a <md:EntityDescriptor>		
	b <md:SPSSODescriptor>		
	- (must include the proper protocolSupportEnumeration)		
	c <md:KeyDescriptor>		
	d <md:SingleLogoutService> (if any)		
	e <md:NameIDFormat> (if any)		

If this is an RFP requirement, please submit with the RFP Proposal

IF REQUESTED FOR OTHER PURPOSES…

Please send completed questionnaire to:	umdoitsasupport@umsystem.edu

ATTACHMENT PA

PROPOSAL AGREEMENT

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).
- We will not discriminate against any employee or applicant for employment because of race, color, national origin, ancestry, sex, religion, disability/handicap, marital status, sexual orientation, or age.

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

- We have received amendment ___ through ___.
- 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 No:	**Fed Employer ID No**:
Fax No:	**E-Mail Address**:
Number of calendar days delivery after receipt of order: _____	Payment Terms: _____ Note: 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	
Maintain a regular place of business in the State of Missouri? _____Yes _____No	

RFP 31200

Procurement and Payment Bill-Only

Request for Proposals

VOLUME II

Required Submittal

(Financials**)**

Attachment FW: "Financial Worksheet"

ATTACHMENT FW
FINANCIAL WORKSHEET

RFP 31200 Procurement and Payment Bill-Only

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 $_____