

REQUEST FOR PROPOSAL
RFP#916278

University Health and Wellness EHR

RFP Timeline	
RFP Issue Date:	January 30, 2026
Deadline for Respondent Questions to MSU:	February 9, 2026
RFP Response Due Date:	March 2, 2026, 3:00 pm Eastern
Demonstrations (virtual)	April 6-17, 2026

RFP Contact	
Name:	Lisa True
Unit:	MSU Procurement
Email:	truelisa@msu.edu

DESCRIPTION: Michigan State University (the “**University**” or “**MSU**”) is soliciting proposals through this Request for Proposal (“**RFP**”) for the purpose of an EHR system for University Health and Wellbeing. The requested services are more thoroughly described under the Scope of Work Section of this RFP. Firms intending to respond to this RFP are referred to herein as a “**Respondent**” or “**Supplier**.”

PROPOSAL INSTRUCTIONS

- PROPOSAL PREPARATION.** The University recommends reading all RFP materials prior to preparing a proposal, particularly these Proposal Instructions. Respondents must follow these Proposal Instructions and provide a complete response to the items indicated in the table below. References and links to websites or external sources may not be used in lieu of providing the information requested in the RFP within the proposal. Include the Respondent's company name in the header of all documents submitted with your proposal.

Document	Description	Response Instructions
Cover Page	Provides RFP title and number, important dates, and contact information for MSU	Informational
Proposal Instructions	Provides RFP instructions to Respondents	Informational
Respondent Information Sheet	Company and Contact Information, and Experience	Respondent must complete and submit by proposal deadline
Scope of Work	Describes the intended scope of work for the RFP	Respondent must complete and submit by proposal deadline
Pricing	Pricing for goods and services sought by the University through this RFP	Respondent must complete and submit by proposal deadline
Master Service Agreement	Provides legal terms for a contract awarded through this RFP	Deemed accepted by Respondent unless information required in Section 9, Master Service Agreement is submitted by proposal deadline

- EXPECTED RFP TIMELINE.**

Activity	Date
RFP Issue Date:	January 30, 2026
Deadline for Respondent Questions to MSU:	February 9, 2026
RFP Response Due Date:	March 2, 2026, 3:00 pm Eastern
Demonstrations (virtual)	April 6-17, 2026

- CONTACT INFORMATION FOR THE UNIVERSITY.** The sole point of contact for the University concerning this RFP is listed on the Cover Page. Contacting any other University personnel, agent, consultant, or representative about this RFP may result in Respondent disqualification.
- QUESTIONS.** Respondent questions about this RFP must be submitted electronically by email to the contact listed on the cover page of this RFP. In the interest of transparency, only written questions are accepted. Answers to all questions will be sent to Respondents via email. Submit questions by

referencing the following: (i) Question Number, (ii) Document Name, (iii) Page Number, and (iv) Respondent Question. Please refer to **Section 2** above for the deadline to submit questions.

5. **MODIFICATIONS.** The University may modify this RFP at any time. Modifications will be sent via email. This is the only method by which the RFP may be modified.
6. **DELIVERY OF PROPOSAL.** The Respondent must submit its proposal, all attachments, and any modifications or withdrawals electronically via email to the contact listed on the cover page of this RFP. **The price proposal should be saved separately from all other proposal documents and should be sent as a separate attachment from the other proposal documents.** The Respondent should submit all documents in a modifiable (native) format (examples include but are not limited to: Microsoft Word or Excel and Google Docs or Sheets). In addition to submitting documents in a modifiable format, the Respondent may also submit copies of documents in PDF. Respondent's failure to submit a proposal as required may result in disqualification. The proposal and attachments must be fully uploaded and submitted prior to the proposal deadline. **Do not wait until the last minute to submit a proposal.** The University **may not** allow a proposal to be submitted after the proposal deadline identified in the Cover Page, even if a portion of the proposal was already submitted.
7. **MANDATORY MINIMUM REQUIREMENTS.** The RFP may contain minimum qualifications, which will be identified as "**Mandatory Minimum Requirements**" in the Scope of Work Section of this RFP. If the RFP does contain mandatory minimum requirements, any proposal not meeting these minimum requirements **will be deemed non-qualified and will not be considered.** All proposals meeting these mandatory minimum requirements will proceed for review and evaluation consistent with **Section 8, Evaluation Process.**
8. **EVALUATION PROCESS.** The University will convene a team of individuals from various Departments within MSU to evaluate each proposal based on each Respondent's ability to provide the required services, taking into consideration the overall cost to the University. The University may require an oral presentation of the Respondent's proposal; conduct interviews, research, reference checks, and background checks; and request additional price concessions at any point during the evaluation process. The following criteria will be used to evaluate each proposal:

Criteria	Weight
Proposed solution meets desired requirements	[40]%
proposed solution appears to meet MSU technical and system interface needs	[25]%
Overall value and cost to the University	[30]%
Responsiveness to MSU terms and conditions and completion of SPSA.	[5]%
	100%

The evaluation process may consist of two phases. If a second phase of evaluation is needed, the **top candidate(s)** will be asked to demonstrate their product using a scripted scenario that will be provided by the University. The following criteria will be used for evaluation:

Criteria	Weight
Solution is accessible, Intuitive, and easy to use	[40]%
Suitability of the interface for each identified stakeholder	[40]%
Ease of accessing data for both operational and strategic reporting	[20]%

MICHIGAN STATE UNIVERSITY

	100%

The scores from both phases will be combined to determine the contract award.

9. **MASTER SERVICE AGREEMENT.** The University strongly encourages strict adherence to the terms and conditions set forth in the Master Service Agreement. The University reserves the right to deem a proposal non-responsive for failure to accept the Master Service Agreement. Nevertheless, the Respondent may submit proposed changes to the Master Service Agreement in track changes (i.e., visible edits) with an explanation of the Respondent's need for each proposed change. Failure to include track changes with an explanation of the Respondent's need for the proposed change constitutes the Respondent's acceptance of the Master Service Agreement. General statements, such as "the Respondent reserves the right to negotiate the terms and conditions," may be considered non-responsive.

10. **CLARIFICATION REQUEST.** The University reserves the right to issue a Clarification Request to a Respondent to clarify its proposal if the University determines the proposal is not clear. Failure to respond to a Clarification Request timely may be cause for disqualification.

11. **RESERVATIONS.** The University reserves the right to:
 - a. Disqualify a Respondent for failure to follow these instructions.
 - b. Discontinue the RFP process at any time for any or no reason. The issuance of an RFP, your preparation and submission of a proposal, and the University's subsequent receipt and evaluation of your proposal does not commit the University to award a contract to you or anyone, even if all the requirements in the RFP are met.
 - c. Consider late proposals if: (i) no other proposals are received; (ii) no complete proposals are received; (iii) the University received complete proposals, but the proposals did not meet mandatory minimum requirements or technical criteria; or (iv) the award process fails to result in an award.
 - d. Consider an otherwise disqualified proposal, if no other proposals are received.
 - e. Disqualify a proposal based on: (i) information provided by the Respondent in response to this RFP; or (ii) if it is determined that a Respondent purposely or willfully submitted false or misleading information in response to the RFP.
 - f. Consider prior performance with the University in making its award decision.
 - g. Consider total-cost-of-ownership factors (e.g., transition and training costs) when evaluating proposal pricing and in the final award.
 - h. Refuse to award a contract to any Respondent that has outstanding debt with the University or has a legal dispute with the University.
 - i. Require all Respondents to participate in a Best and Final Offer round of the RFP.
 - j. Enter into negotiations with one or more Respondents on price, terms, technical requirements, or other deliverables.
 - k. Award multiple, optional-use contracts, or award by type of service or good.
 - l. Evaluate the proposal outside the scope identified in **Section 8, Evaluation Process**, if the University receives only one proposal.
 - m. Obtain and consider information from other sources concerning a Respondent, such as the Respondent's capability and performance under other contracts, the qualifications of any subcontractor identified in the Proposal, the Respondent's financial stability, past or pending litigation, and other publicly available information.
 - n. Utilize third parties to assist in the evaluation process, provided such parties are subject to confidentiality requirements.

- 12. AWARD RECOMMENDATION.** The contract will be awarded to the responsive and responsible Respondent who offers the best value to the University, as determined by the University. Best value will be determined by the Respondent meeting any mandatory minimum requirements and offering the best combination of the factors in **Section 8, Evaluation Process**, and price, as demonstrated by the proposal. The University will email a **Notice of Award** to all Respondents. A Notice of Award does not constitute a contract, as the parties must reach final agreement on a signed contract before any services can be provided. The awarded Respondent is prohibited from partnering with losing bidders unless the RFP specifically allows for such arrangement, and any violation of this prohibition may result in disqualification of the awarded Respondent.
- 13. GENERAL CONDITIONS.** The University will not be liable for any costs, expenses, or damages incurred by a Respondent participating in this solicitation. The Respondent agrees that its proposal will be considered an offer to do business with the University in accordance with its proposal, including the Master Service Agreement, and that its proposal will be irrevocable and binding for a period of 180 calendar days from date of submission. If a contract is awarded to the Respondent, the University may, at its option, incorporate any part of the Respondent's proposal into the contract. This RFP is not an offer to enter into a contract. This RFP may not provide a complete statement of the University's needs, or contain all matters upon which agreement must be reached. Proposals submitted via email are the University's property.
- 14. FREEDOM OF INFORMATION ACT.** Respondent acknowledges that any responses, materials, correspondence or documents provided to the University may be subject to the State of Michigan Freedom of Information Act ("FOIA"), Michigan Compiled Law 15.231 *et seq.*, and may be released to third parties in compliance with FOIA or any other law. Questions about the Respondent's own performance can be directed to the RFP Contact indicated on page 1 of this document. Questions about the overall evaluation and any other post-award inquiries must be submitted via a formal FOIA request to the [Michigan State University FOIA office](#).

RESPONDENT INFORMATION SHEET

Please complete the following Information Sheet in the space provided:

Information Sought	Response
Contact Information	
Respondent's sole contact person during the RFP process. Include name, title, address, email, and phone number.	
Person authorized to receive and sign a resulting contract. Include name, title, address, email, and phone number.	
Respondent Background Information	
Legal business name and address. Include business entity designation, e.g., sole proprietor, Inc., LLC, or LLP.	
What state was the company formed in?	
Main phone number	
Website address	
DUNS# AND/OR CCR# (if applicable):	
Number of years in business and number of employees	
Legal business name and address of parent company, if any	
Has your company (or any affiliates) been a party to litigation against Michigan State University? If the answer is yes, then state the date of initial filing, case name and court number, and jurisdiction.	
Experience	
Describe relevant experiences from the last 5 years supporting your ability to successfully manage a contract of similar size and scope for the services described in this RFP.	
Experience 1	
Company name Contact name Contact role at time of project Contact phone Contact email	
1. Project name and description of the scope of the project 2. What role did your company play? 3. How is this project experience relevant to the subject of this RFP?	
Start and end date (mm/yy – mm/yy)	
Status (completed, live, other – specify phase)	
Experience 2	
Company name Contact name Contact role at time of project Contact phone	

MICHIGAN STATE UNIVERSITY

Contact email	
1. Project name and description of the scope of the project 2. What role did your company play? 3. How is this project experience relevant to the subject of this RFP?	
Start and end date (mm/yy – mm/yy)	
Status (completed, live, other – specify phase)	
Experience 3	
Company name Contact name Contact role at time of project Contact phone Contact email	
1. Project name and description of the scope of the project 2. What role did your company play? 3. How is this project experience relevant to the subject of this RFP?	
Start and end date (mm/yy – mm/yy)	
Status (completed, live, other – specify phase)	

SCOPE OF WORK

Please address each of the sections below in a written response (which can be completed on a separate sheet (using the same section headings), in addition to the Excel format provided.

A. Background.

Michigan State University (MSU) is a large public research university in East Lansing, Michigan and serves a diverse population of approximately 52,000 students. University Health and Wellbeing is a major administrative unit with a stated purpose to support the university community with health and wellbeing equitably woven throughout all aspects of Spartan life, enhancing accessibility and safety through a culturally sensitive and holistic lens. Two distinct administrative units within University Health and Wellbeing will be utilizing a common electronic health record. Several distinct services within CHS are primary care, gynecology, allergy and immunizations, a clinical laboratory, occupational health, travel medicine, and nutrition. CAPS provides psychiatry, individual therapy, group counseling visits, triage/initial consultation appointments, crisis interventions, clinical training and outreach/community engagement.

B. Scope of Work.

Provide a concise reply to each request providing sufficiently detailed information to allow the University to confirm that the functionality is present in the product offered. If the functionality is not present, it would be appropriate to identify if it is on a roadmap and approximately when the features will be available.

EHR Functional

1. Describe confidentiality within the product. Specifically, we want to see how different types of charts, patients and data are treated. Examples could include primary care and behavioral health (example: "breaking the glass"), legal name/first name used/pronouns and charts with a familial relationship. Audit trails and access controls-can you set up different levels of access.
2. Describe your data analytics and reporting tool. Differentiate between tactical (operational) and strategic reporting.
3. Describe the scheduling and calendaring ability within the product. Specifically, MSU is interested in patient online scheduling for new and established patients and provider calendaring functionality for a single provider schedule. A priority with having capability to build open schedules and ability to free text when freezing a schedule with reason.
4. Describe the document completion, routing, alerting and accountability within the product. The ability for the EHR to keep track of when annual forms are due. Minor consent needs notification upon scheduling/pre-registration. MSU is interested in the continuum of care for patients and effective document routing and sign off.
5. Describe how your product allows for sharing content and standards across the user base. Examples are leveraging existing content from the vendor's user base as well as any other add-on software/systems that may be available. These could be encounter plans, documents, forms and/or policies from the user base (internally and/or externally).

6. Describe the patient portal including: Functional use registering, online scheduling for initial visits and follow-ups (with this having availability for patient to input student number at the time of scheduling online), patient forms, uploading documentation, patient to provider messaging and linkage to the chart. Patient access to the portal. (mobile, web, app, etc.).
7. Describe a typical primary care patient from first contact to final signed encounter. This should include ordering prescriptions (especially that with completing a controlled substance script), labs (how they are reported back to the provider and to patient), and/or other applicable items, such as referrals/radiology orders.
8. Describe a typical group counseling visit, including participant management, documentation, and scheduling.
9. Describe the ability to use a campaign to provide outreach to the student population. Example: Fall flu shots available, announcements via the portal, mailers, SMS, also availability to cancel a whole provider/department schedule via campaign.
10. Describe your audit trail for accessing, downloading, and printing any records within the system.
11. Describe the patient check-in process as it relates to digitally filling out forms and/or signing documents (such as: privacy, release, PHM and/or ROS, sending out screening tools, Occupational Health questionnaires). Discuss the ability to interrogate insurance eligibility within the EHR as this is an important part of our check-in process. Also share the ability to customize registration fields for student numbers.
12. Describe the level of workflow customization. This should include the depth to which a workflow can be customized as well as the best practices within the product for customization. The departments we are specifically looking for are: psychiatry, counseling, primary care, gynecology, occupational health/travel clinic, allergy/immunization and nutrition.
13. Describe creation and customization of forms and content within the system (example: DOT driver physical forms). This should include technology, process, best practices, and leveraging data between forms/content.
14. Describe your internal reporting tool. This should include accessing reports, dashboards, canned reports, and the ability to create custom reports.
15. Describe scheduling and process for telehealth visits.
16. Describe availability and process for satisfaction/feedback surveys.
17. Provide what vendor services will be needed to support requirements of the MSU EHR (example: billing, online scheduling, pre-registration).
18. Show patient portal including accessibility and security protections
19. Describe any enhancements and AI functionality built in or available for add-on.

Laboratory Specifications

1. Product must have the ability to self-manage the testing compendium and be able to update and create POCT tests as well as the test orders that will be completed in the laboratory.
2. Creation of AOE (ask on order entry questions) that can be connected to a diagnosis or test order or order set.
3. Ability to order “generic” or “miscellaneous” testing for esoteric tests that are not in compendium with a space for adding comment for test requested.
4. The capability to create order sets and connect them to diagnosis codes as recommended test orders.
5. The ability to create reports for test usage and track testing result trends.

6. Ability to print registration and patient insurance information to attach to external lab orders if necessary.
7. Bidirectional orders and results. The capability to send test orders electronically to the Harvest system as well as receive results within the system HL7 message interface.
8. The capability to register patients and complete laboratory testing outside of a patient visit.-
Example: testing for external providers to be excluded from the EHR but capable of billing those tests without a patient visit.
9. (Not all test results or orders will need to be a part of the EHR but may need to be billed.)
10. Order tracking-ability to verify provider sent/signed orders.
11. Ability to assure that orders and results match up.
12. Allow for display of test results to contain all necessary data including result ranges and flagging, customizable test result formats.
13. Allow for interpretive comments to be added to test results and be displayed on report within the system and easily seen by providers.
14. Ability to order testing for standing orders or future testing.
15. Capable of Ordering add on tests to already sent laboratory orders.
16. Patient demographics, registration, and insurance updates within the EHR send updates to the LIS.
17. Show how an internal provider orders testing and receives results
18. How would an order from an external provider be handled.
19. Ability to print laboratory test orders for patients who want to bring the order to external laboratory.
20. How would the system work with reference laboratory test results-like from Sparrow or other external laboratory, would those results be interfaced? Can test results come through Mihin/glhc?

CAPS Specifications

1. Describe a typical individual counseling/psychotherapy visit, including documentation, scheduling and how notes can be routed to clinical supervisor for review.
2. Describe a typical group counseling visit, including participant management, documentation, and scheduling.
3. Describe how clinical supervision documentation occurs within the platform to include both PHI and non-PHI within EHR.
4. Describe how all clinical documentation can be routed for clinical supervisor review and signature.
5. Demonstrate how video recording and storage of video recordings are integrated within or can be interfaced with preexisting platforms (e.g., Zoom/Teams) for the purpose of clinical supervision.
6. Demonstrate how EHR interfaces with CCMH and CCAPS.
7. Demonstrate how non-clinical/quasi-clinical appointments/tasks (e.g., documentation, seminars, meetings, clinical supervision are scheduled and documented in calendar function.
8. Demonstrate how community engagement/caps connect and other quasi-clinical functions are documented which may and may not connected to individual patients.
9. Demonstrate single-point of access for CAPS utility (with preference to not having to create new user ID for each student).

10. Demonstrate reports that can be created for individual providers (e.g., Trainees) to accurately detail service, effort, scheduling/attendance rates, etc.
11. Demonstrates what psychological testing documentation looks like.
12. Demonstrate how note templates can be developed for individual needs to unit (e.g., referral coordination, referrals, etc)
13. CAPS: Data analytics and reporting that is accessible to select users
14. Data analytics and reporting tools that can differentiate types of clinical and non-clinical appointments.
15. Clinical charting for non-billable clinical appointments.
16. Routing features for clinicians-in-training or limited license to staff to have supervisor signature.
17. Describe ways clinical supervision or other non-clinical appointments function within the platform including if specific forms can be created or utilized.
18. Describe internal communication to the platform (e.g., forward to box, chat, etc).
19. Describe integration of routine outcome monitoring for best practice in service delivery

Billing/Insurance

1. Describe capability to have fee schedules customized by department and whether departments bill insurance or operate as prepay only.
2. Describe capability to customize charges (example: prompt pay options).
3. Ability to create “rules” to hold billing charges for payment verification for Prompt pay testing and update billing/charge information as needed.
4. Manage our own rates and CPT coding for client billing; including department, insurance, or patient bill options.
5. Describe interdepartmental billing options (occ health/travel/ and primary care currently use case policies that work like insurance packages).
6. Ability to bill for laboratory testing outside of a patient visit.-most laboratory testing is billed on date of test completion not necessarily date of service.
7. Explain how many tiers of resolution provided in billing.
8. Describe revenue cycle with the EHR.
9. Describe how billing is done with lab (example: how does the system know to go directly to JVHL). _Current system will “flip” an insurance package to add the JVHL package as a reference package and add the location code to ensure that JVHL will be billed for the insurance without changing the patient’s insurance data for clinic billing.
10. Describe how subsidized visits would be supported and tracked for straight forward office visits, and split bills (E/M code could be subsidized, while testing and immunizations would need to still be billed.)
11. Multi-Source Billing Support-/complex billing
 - a. Direct Patient Billing – Generate invoices for self-pay patients
 - b. Insurance Billing – Integration with clearinghouses for electronic claims
 - c. Departmental Billing – Bill specific clinic departments directly
 - d. Bundling or unbundling testing groups based on insurance requirements.
 - e. Adding external providers for billing purposes- need to have capability to continuously add to provider tables and locations
 - f. Create one claim for multiple charges from the same date
 - g. Ability to edit claims to update CPT codes, dx codes or add modifiers when

needed

- h. Able to bill duplicate CPT codes for same date of service

IT Technical Requirements

Please find the most current version of the HECVAT security survey here: [Higher Education Community Vendor Assessment Tool \(HECVAT\)](#). Review the information on the page, download and complete the questionnaire, and return the completed form to MSU as part of your proposal.

System Architecture & Deployment

1. Provide a comprehensive description of the current system architecture, including:
 - a. Development methodology
 - b. Server architecture (on-premises, cloud, hybrid)
 - c. Security principles and compliance frameworks
 - d. Application deployment methodology for end-user devices
 - e. Hosting solutions and service-level agreements (SLAs)
2. Describe all end-user device types supported, including:
 - a. Recommended (not minimum) system requirements for optimal performance
 - b. Supported operating systems (Windows, macOS, Linux, mobile OS)
 - c. Any special hardware requirements (e.g., peripherals, biometric devices)
3. Identify any thick/thin client applications required on user workstations and provide details on:
 - a. Deployment methods, including compatibility with Microsoft SCCM
 - b. Any web-based components and supported browsers
4. Explain your approach to interoperability, including:
 - a. Integration capabilities with third-party systems via API, HL7, FHIR, batch ETL, or other methods
 - b. Prebuilt connectors with regional Health Information Exchanges (HIEs), EHRs, lab systems, and medical devices
 - c. Integration capabilities with enterprise applications like SAP, PeopleSoft, and other ERP systems
 - d. Standards and protocols supported for integration

System Updates, Monitoring & Support

1. Describe the typical update cycle for both software and hardware, including:
 - a. Frequency and types of updates (major, minor, security patches)

- b. Communication processes with MSU teams before, during, and after updates
 - c. Expected impact on users and downtime mitigation strategies
- 2. Explain your system monitoring and alerting capabilities, including:
 - a. How uptime, performance, and security incidents are tracked
 - b. Procedures for downtime scenarios, including user notifications and system recovery
 - c. Historical uptime statistics and SLAs for system availability
- 3. Describe IT support services provided, including:
 - a. Support for MSU practices (e.g., IT helpdesk, tiered support structure)
 - b. Patient support (e.g., patient portal troubleshooting, mobile app support)
 - c. Support availability (24/7, business hours, emergency response)

Security, Compliance & Disaster Recovery

- 1. Explain your approach to securing sensitive data, including HIPAA and FERPA compliance, by addressing:
 - a. Data encryption (in transit and at rest)
 - b. Security certifications and audits (SOC 2, HITRUST, etc.)
 - c. Multi-factor authentication and endpoint security measures
- 2. Describe how your product enforces least privilege access in compliance with:
 - a. NIST Special Publication (SP) 800-53 AC-6
 - b. HIPAA 45 CFR § 164.308(a)(4)(ii)(B)
- 3. Detail your disaster recovery (DR) and business continuity processes, including:
 - a. Backup and restore procedures
 - b. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
 - c. Failover mechanisms and redundancy strategies
- 4. Describe your ongoing security testing and vulnerability management practices, including:
 - a. Penetration testing frequency and methodologies
 - b. Threat detection and mitigation strategies
 - c. Security patching cadence and emergency response procedures

Accessibility, Identity Management & Authentication

- 1. Please review and complete the VPAT 2.5Rev WCAG edition located at [Voluntary Product Accessibility Template files](#), or a VPAT that was completed in the last two years. The completed form should be included part of your proposal. Explain your system's compliance with

accessibility standards (e.g., WCAG 2.1, Section 508) and include any historical downtime statistics and typical user impact.

2. Describe your Single Sign-On (SSO) integration capabilities, including:

- a. Compatibility with Microsoft Entra (Azure AD) and/or Okta
- b. Support for SAML, OAuth, etc.

3. Detail your badge/ID system integration for card-swipe authentication, including:

- a. Compatibility with MSU's existing ID management system
- b. Use cases such as workstation login, patient check-in, and secure access to restricted features

Additional Capabilities

1. Medical Interface Capabilities

- a. Describe available integrations for lab and radiology systems. Currently all EHR inbound information and outbound registration information flows to the ORCHARD HARVEST laboratory system via Rhapsody interfaces and connections with MIHIN.
- b. Provide details on prebuilt connectors with major diagnostic products
- c. Describe how your software interfaces between the EHR and the Michigan Care Improvement Registry (MCIR) which contains the Michigan Immunization Portal and the Michigan Automated Prescription System (MAPS) which helps to track prescribed controlled substances.

2. Digital Signature Capture

- a. Describe built-in electronic signature capabilities for providers and patients

3. Payment Processing

- a. Explain your solution's ability to process online and in-person payments
- b. Identify supported payment gateways and compliance with PCI-DSS

PRICING

Please include a Pricing proposal as identified below on a separate sheet.

Your pricing proposal must identify all costs applicable to licensing, configuration, implementation, training and customer technical support for an initial period of (3 years). The University is interested in understanding the total cost of ownership for the initial period and will seek to fix pricing for renewal years at an escalation factor equal to or less than CPI.

Suppliers are welcome to include other value-added services that the university may be interested in with ALA Cart pricing. (ex. Clinical billing services, patient satisfaction, etc.)

You may submit multiple pricing scenarios; pricing must be inclusive of all fees as outlined above.



MASTER SERVICE AGREEMENT

(see following page)

Please refer to Section 9 of the RFP Instructions when reviewing the Master Services Agreement terms and conditions.

Master Service Agreement
(Software as a Service and Externally Hosted Applications)

This Master Services Agreement (this “**Agreement**”) is agreed to between the Board of Trustees of Michigan State University, a Michigan constitutional body corporate (the “**University**” or “**MSU**”) and [INSERT COMPANY NAME] (“**Supplier**”), a [INSERT STATE & ENTITY STATUS, E.G., A MICHIGAN CORPORATION OR A TEXAS LIMITED LIABILITY COMPANY]. This Agreement is effective on [MONTH, DAY, YEAR] (“**Effective Date**”), and unless earlier terminated, will expire on [MONTH, DAY, YEAR] (the “**Term**”).

This Agreement may be renewed for up to three (3) additional two (2) year periods. Renewal must be by written notice from the University and will automatically extend the Term of this Agreement.

1. Definitions.

“**Accept**” or “**Acceptance**” has the meaning set forth in **Section 4.2(b)**.

“**Action**” has the meaning set forth in **Section 17.1**.

“**Administrative Users**” means an individual authorized by the University with log-in rights to access and use the administrative features of the Service Software in accordance with the terms of this Agreement and the Documentation, subject to the maximum number of Administrative Users specified in the Statement of Work.

“**Agreement**” has the meaning set forth in the preamble.

“**Agreement Administrator**” is the individual appointed by each party to (a) administer the terms of this Agreement, and (B) approve and execute any Change Notices under this Agreement. Each party’s Agreement Administrator will be identified in the Statement of Work.

“**Availability Requirement**” has the meaning set forth in **Section 5**.

“**Business Day**” means a day other than a Saturday, Sunday or University Holiday.

“**Change Notice**” has the meaning set forth in **Section 2.2**.

“**Confidential Information**” has the meaning set forth in **Section 14.1**.

“**Documentation**” means all generally available documentation relating to the Services, including all user manuals, operating manuals and other instructions, specifications, documents and materials, in any form or media, that describe any component, feature, requirement or other aspect of the Services, including any functionality, testing, operation or use thereof.

“**DR Plan**” has the meaning set forth in **Section 16.1**.

“**Effective Date**” has the meaning set forth in the preamble.

“**End User**” means all public facing individuals and other Persons who access or use the Service Software as a customer of the University.

"Fees" has the meaning set forth in **Section 8.1**.

"FERPA" has the meaning set forth in **Section 10**.

"Force Majeure Event" has the meaning set forth in **Section 21.1**.

"HIPAA Rules" has the meaning set forth in **Section 12**.

"Law" means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree or other requirement or rule of any federal, state, local or foreign government or political subdivision thereof, or any arbitrator, court or tribunal of competent jurisdiction.

"Loss" means all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers. **"Losses"** has a correlative meaning.

"PCI DSS" has the meaning set forth in **Section 13.1**.

"PII" has the meaning set forth in **Section 9.3**.

"Person" means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

"Process" means to perform any operation or set of operations on any data, information, material, work, expression or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or (c) block, erase or destroy. **"Processing"** and **"Processed"** have correlative meanings.

"RPO" or **"Recovery Point Objective"** means the maximum amount of potential data loss in the event of a disaster.

"RTO" or **"Recovery Time Objective"** means the period of time to fully restore the Services in the case of a disaster.

"Reject" or **"Rejection"** has the meaning set forth in **Section 4.2(b)**.

"Representatives" means a party's employees, officers, directors, consultants, legal advisors and, with respect to Supplier, Supplier's Subcontractors.

"RFP" means the University's request for proposal designed to solicit responses for Services under this Agreement.

“Service Level Agreement” means the service level agreement attached as **Schedule B** to this Agreement, setting forth Supplier’s obligations with respect to the hosting, management and operation of the Service Software.

“Service Software” means any and all software applications and any third-party or other software, and all new versions, updates, revisions, improvements and modifications of the foregoing, that Supplier provides remote access to and use of as part of the Services.

“Services” has the meaning set forth in **Section 2.1**.

“Specifications” means the specifications for the Services set forth in the Statement of Work and, to the extent consistent with and not limiting of the foregoing, the Documentation.

“Statement of Work” means the statement of work, attached as **Schedule A** to this Agreement, which details the Service Software and the corresponding Services that Supplier is providing under this Agreement.

“Subcontractor” means a third-party engaged by Supplier that performs any Services under this Agreement.

“Supplier” has the meaning set forth in the preamble.

“Supplier Personnel” means all employees and agents of Supplier, all Subcontractors and all employees and agents of any Subcontractor, involved in the performance of Services.

“Supplier Service Manager” has the meaning set forth in **Section 2.6**.

“Support Service Level Requirement” has the meaning set forth in **Section 3**.

“Term” has the meaning set forth in the preamble.

“Transition Period” has the meaning set forth in **Section 7.3**.

“Transition Responsibilities” has the meaning set forth in **Section 7.3**.

“University” has the meaning set forth in the preamble.

“University Data” has the meaning set forth in **Section 9.1**.

“University Service Manager” has the meaning set forth in **Section 2.8**.

“University Systems” means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the University or any of its designees.

“**User Data**” means any and all information reflecting the access or use of the Services by any End User, including any end user profile, visit, session, impression, click-through or click-stream data and any statistical or other analysis, information or data based on or derived from any of the foregoing.

2. Services.

2.1 Services. Throughout the Term and at all times in connection with its actual or required performance under this Agreement, Supplier will, in accordance with all terms and conditions set forth in this Agreement and the Statement of Work, provide to the University the following services (“**Services**”):

(a) the hosting, management and operation of the Service Software and other services for remote electronic access and use by the University, its Administrative Users, and End Users as described in the Statement of Work;

(b) maintain the Availability Requirement set forth in the Service Level Agreement, attached as **Schedule B** to this Agreement;

(c) provide the maintenance and support services set forth in the Service Level Agreement, attached as **Schedule B** to this Agreement;

(d) implement and maintain the security requirements set forth in **Section 15** to this Agreement;

(e) maintain a DR plan in accordance with **Section 16** of this Agreement; and

(f) such other services as may be specified in the Statement of Work.

2.2 Change Notices. Any modifications or changes to the Services will be effective only if and when memorialized in a mutually agreed written change notice (each, a “**Change Notice**”) signed by both Parties, provided, however, that for any Services provided on a limited basis (for example, on a per-user or named-user basis), the University may, at any time, increase or decrease the number of its licenses hereunder subject to a corresponding forward-going adjustment of the Fees to reflect these changes in accordance with the pricing set forth in the Statement of Work.

2.3 Compliance with Laws. Supplier must comply with all applicable Laws as they concern this Agreement, including by securing and maintaining all required and appropriate visas, work permits, business licenses and other documentation and clearances necessary for performance of the Services.

2.4 Compliance with MSU Policies. Supplier must comply, where applicable, with written MSU policies, which are available at: <https://upl.msu.edu/for-suppliers/policies-requirements/index.html>.

2.5 Subcontracting. Supplier must notify the University in writing if it subcontracts any Services, in whole or in part, to a Subcontractor. Suppliers use of Subcontractors is subject to the following:

(a) Supplier must ensure each Subcontractor complies with all relevant terms of this Agreement, including all provisions relating to University Data or other Confidential Information of the

University, and will have in place written agreements with any such Subcontractor which ensures such compliance;

(b) Supplier will remain responsible and liable for any and all: (i) performance required hereunder, including the proper supervision, coordination and performance of the Services; and (ii) acts and omissions of each Subcontractor (including, such Subcontractor's employees and agents, who, to the extent they are involved in providing any Services, are deemed Supplier Personnel) to the same extent as if such acts or omissions were by Supplier; and

(c) any noncompliance by any Subcontractor or its employees or agents with the provisions of this Agreement or the Statement of Work will constitute a breach by Supplier.

2.6 Supplier Service Manager. Supplier will, subject to the prior written approval of the University, appoint a Supplier employee to serve as a primary contact with respect to the Services who will have the authority to act on behalf of Supplier in matters pertaining to the receipt and processing of support requests (the **"Supplier Service Manager"**). The University may request a change in the Supplier Service Manager if the level of service is not adequate to meet the University's needs.

2.7 Management and Payment of Supplier Personnel.

(a) Supplier is solely responsible for the payment of Supplier Personnel, including all fees, expenses and compensation to, by or on behalf of any Supplier Personnel and, if applicable, the withholding of income taxes and payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(b) Supplier may be required to perform criminal background checks of its Personnel pursuant to the MSU Contractor Criminal Background Check Requirements Policy (**"CBC Policy"**), available at <https://upl.msu.edu/common/documents/criminal-back-ground-check.pdf>. If Supplier is subject to the CBC Policy, Supplier must sign and deliver the Contractor Certification for Criminal Background Checks to University prior to the provision of any Services. University reserves the right to audit compliance with the CBC Policy requirements and may require further documentation of compliance from Supplier. Non-compliance with the Policy is considered a material breach of this Agreement, which may result in a termination for cause.

2.8 University Project Manager. The University will appoint and, in its reasonable discretion, replace, a University employee to serve as the primary contact with respect to implementation of the Services and ongoing service requests (the **"University Service Manager"**).

3. **License Grant and Restrictions.**

3.1 Supplier License Grant. Supplier hereby grants to the University a nonexclusive, royalty-free, irrevocable (except as provided herein) right and license during the Term and such additional periods, if any, as Supplier is required to perform Services under this Agreement, to access and use the Services, including in operation with other software, hardware, systems, networks and services, for the University's business purposes, including for Processing University Data.

3.2 License Restrictions. The University will not: (a) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make the Services available to any third party, except as expressly permitted by this Agreement or in the Statement of Work; or (b) use or authorize the use of the Services or Documentation in any manner or for any purpose that is unlawful under applicable Law.

4. Service Preparation, Testing and Acceptance.

4.1 Service Preparation. Promptly upon the parties' execution of this Agreement and the Statement of Work, Supplier will take all steps necessary to make the Services procured thereunder ready and available for the University's use in accordance with the Statement of Work and this Agreement, including any applicable milestone date or dates set forth in the Statement of Work.

4.2 Testing and Acceptance.

(a) When Supplier notifies the University in writing that the Services are ready for use in a production environment, the University will have thirty (30) days (or such other period as may be agreed upon by the Parties in writing) from receipt of the notice to test the Services to determine whether they comply in all material respects with the requirements of this Agreement and the Specifications.

(b) Upon completion of the University's testing, the University will notify Supplier of its acceptance ("**Accept**" or "**Acceptance**") or, if it has identified any noncompliance with the Specifications, rejection ("**Reject**" or "**Rejection**") of the Services. If the University Rejects the Services, the University will provide a written list of items that must be corrected. On receipt of the University's notice, Supplier will promptly commence, at no additional cost or charge to the University, all reasonable efforts to complete, as quickly as possible and in any event within twenty (20) days (or such other period as may be agreed upon by the Parties in writing) from receipt of the University's notice, such necessary corrections, repairs and modifications to the Services to bring them into full compliance with the Specifications.

(c) If any corrective measures are required under **Section 4.2(b)**, upon completion of all such measures, Supplier will notify the University in writing and the process set forth in **Section 4.2(a)** and **Section 4.2(b)** will be repeated; provided that if the University determines that the Services, as revised, still do not comply in all material respects with the Specifications, the University may, in its sole discretion:

- (i) require the Supplier to repeat the correction process set forth in **Section 4.2(b)** at no additional cost or charge to the University; or
- (ii) terminate this Agreement for cause.

(d) The parties will repeat the foregoing procedure until the University Accepts the Services or elects to terminate this Agreement as provided in **Section 4.2(c)(ii)** above. If the University so terminates this Agreement, Supplier must refund to the University all sums previously paid to Supplier within ten (10) Business Days of the University's written notice of termination, and the University will be relieved of all obligations thereunder.

5. Service Availability. Supplier will make the Services available, as measured over the course of each calendar month during the Term, in accordance with the provisions set forth in the Service Level Agreement, attached as **Schedule B** to this Agreement (the “**Availability Requirement**”).

6. Support and Maintenance Services. Supplier will provide maintenance and support services in accordance with the provisions set forth in the Service Level Agreement, attached as **Schedule B** to this Agreement (the “**Support Service Level Requirement**”).

7. Termination, Expiration and Transition.

7.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Agreement:

(a) The University may terminate this Agreement for cause, in whole or in part, if Supplier: (i) endangers the security of University Systems or University Data; (ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or (iii) breaches any of its material duties or obligations under this Agreement. Any reference to specific breaches being material breaches within this Agreement will not be construed to mean that other breaches are not material.

(b) If the University terminates this Agreement under this **Section 7.1**, the University will issue a termination notice specifying whether Supplier must: (a) cease performance immediately, or (b) continue to perform for a specified period. If it is later determined that Supplier was not in breach of this Agreement, the termination will be deemed to have been a termination for convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 7.2**.

(c) The University will only pay for amounts due to Supplier for Services accepted by the University on or before the date of termination, subject to the University’s right to set off any amounts owed by the Supplier for the University’s reasonable costs in terminating this Agreement. Supplier must promptly reimburse to the University any Fees prepaid by the University prorated to the date of such termination. Further, Supplier must pay all reasonable costs incurred by the University in terminating this Agreement for cause, including administrative costs, attorneys’ fees, court costs, and transition costs.

7.2 Termination for Convenience. The University may terminate this Agreement in whole or in part, upon thirty days advance written notice, without penalty and for any reason. The termination notice will specify whether Supplier must: (a) cease performance immediately, or (b) continue to perform in accordance with **Section 7.3**. If the University terminates this Agreement for convenience, the University will pay all reasonable costs for University approved Transition Responsibilities, and will forfeit any prepaid fees for the Services (provided such fees do not span more than one calendar year).

7.3 Transition Responsibilities. Upon termination or expiration of this Agreement for any reason, Supplier must, for a period of time specified by the University (not to exceed 90 calendar days; the “**Transition Period**”), provide all reasonable transition assistance requested by the University, to allow for the expired or terminated portion of the Agreement to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the University or its designees. Such transition

assistance may include but is not limited to: (a) continuing to perform the Services at the established Fees; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to the University or the University's designee; (c) taking all necessary and appropriate steps, or such other action as the University may direct, to preserve, maintain, protect, or return to the University all University Data; and (d) preparing an accurate accounting from which the University and Supplier may reconcile all outstanding accounts (collectively, the "**Transition Responsibilities**"). The Term of this Agreement is automatically extended through the end of the Transition Period.

7.4 Effect of Termination. Upon and after the termination or expiration of this Agreement for any or no reason:

- (a) Supplier will be obligated to perform all Transition Responsibilities specified in **Section 7.3**;
- (b) Supplier will, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Supplier), provide to University an extract of University Data in the format specified by the University; and
- (c) Supplier will (i) return to the University all documents and tangible materials (and any copies) containing, reflecting, incorporating, or based on the University's Confidential Information; (ii) permanently erase the University's Confidential Information from its computer systems; and (iii) certify in writing to the University that it has complied with the requirements of this **Section 7.4(c)**, in each case to the extent such materials are not required by Supplier for Transition Responsibilities, if any.

7.5 Survival. The rights, obligations and conditions set forth in this **Section 7.5** and **Section 1** (Definitions), **Section 7.4** (Effect of Termination), **Section 9** (University Data), **Section 14** (Confidentiality), **Section 15** (Security), **Section 17.1** (Indemnification), **Section 18** (Limitations of Liability), **Section 19** (Representations and Warranties), **Section 20** (Insurance) and **Section 23** (General Provisions), and any right, obligation or condition that, by its express terms or nature and context is intended to survive the termination or expiration of this Agreement, survives any such termination or expiration hereof.

8. Fees and Expenses.

8.1 Fees. Subject to the terms and conditions of this Agreement, the Statement of Work, and the Service Level Agreement, the University shall pay the fees set forth in the Statement of Work, subject to such increases and adjustments as may be permitted pursuant to **Section 8.2** ("**Fees**").

8.2 Fees during Option Years. Supplier's Fees are fixed during the initial period of the Term. Supplier may increase Fees for any renewal period by providing written notice to the University at least sixty (60) calendar days prior to the commencement of such renewal period. An increase of Fees for any renewal period may not exceed three percent (3%) of the Fees effective during the immediately preceding twelve (12) month period. No increase in Fees is effective unless made in compliance with the provisions of this **Section 8.2**.

8.3 Responsibility for Costs. Supplier is responsible for all costs and expenses incurred in or incidental to the performance of Services, including all costs of any materials supplied by Supplier, all fees, fines, licenses, bonds, or taxes required of or imposed against Supplier, and all other of Supplier's costs of doing business.

8.4 Taxes. The University is exempt from state sales tax for direct purchases and may be exempt from federal excise tax, if Services purchased under this Agreement are for the University's exclusive use. Upon request, the University will provide Supplier with a Tax Exemption Letter evidencing the same.

8.5 Invoices. Supplier will invoice the University for Fees in accordance with the requirements set forth in the Statement of Work, including any requirements that condition the rendering of invoices and the payment of Fees upon the successful completion of milestones. Supplier must submit each invoice via such delivery means and to such address as are specified by the University at <https://upl.msu.edu/for-suppliers/policies-requirements/invoicing-payments/index.html>. Each separate invoice must:

(a) clearly identify the Agreement and Purchase Order to which it relates, in such manner as is required by the University;

(b) list each Fee item separately;

(c) include sufficient detail for each line item to enable the University to satisfy its accounting and charge-back requirements;

(d) for Fees determined on a time and materials basis, report details regarding the number of hours performed during the billing period, the skill or labor category for such Supplier Personnel and the applicable hourly billing rates; and

(e) include such other information as may be required by the University as set forth in the Statement of Work.

8.6 Payment Terms. Invoices are due and payable by the University, in accordance with the University's standard payment procedures, which is 30 days after receipt of invoice, provided the University determines that the invoice was properly rendered.

8.7 University Audit of Supplier. University shall have access to and the right to examine and copy any directly pertinent books, documents, papers, and records of Supplier involving transactions related to this Agreement until the expiration of three (3) years after final payment hereunder. Supplier further agrees to promptly furnish, when requested by University, such books, documents, and records of Supplier as are necessary to verify the accuracy of the amounts invoiced to University against any past or current goods and services provided by Supplier. If any audit discloses an overpayment by University or a discrepancy in the amount invoiced by Supplier against the goods and services actually provided by Supplier, Supplier will promptly reimburse University within thirty (30) days of University's notification to Supplier of any such overpayment, rectify such discrepancy, or both, and further pay University a fee equal to 25% of the amount of any overpayment.

8.8 Payment Does Not Imply Acceptance. The making of any payment or payments by the University, or the receipt thereof by Supplier, will in no way affect the responsibility of Supplier to perform the Services in accordance with this Agreement, and will not imply the University's Acceptance of any Services or the waiver of any warranties or requirements of this Agreement, including any right to service credits under the Service Level Agreement.

8.9 Payment Disputes. The University may withhold from payment any and all payments and amounts the University disputes in good faith, pending resolution of such dispute, provided that the University:

- (a) timely renders all payments and amounts that are not in dispute;
- (b) notifies Supplier of the dispute prior to the due date for payment, specifying in such notice:
 - (i) the amount in dispute; and
 - (ii) the reason for the dispute set out in sufficient detail to facilitate investigation by Supplier and resolution by the parties;
- (c) works with Supplier in good faith to resolve the dispute promptly; and
- (d) promptly pays any amount determined to be payable by resolution of the dispute.

Supplier shall not withhold or delay any Services or fail to perform any other services or obligations hereunder by reason of the University's good faith withholding of any payment or amount in accordance with this **Section 8.9** or any dispute arising therefrom.

8.10 Service Level Credits. Supplier acknowledges and agrees that any credits assessed under the Service Level Agreement: (a) is a reasonable estimate of and compensation for the anticipated or actual harm to the University that may arise from not meeting the Availability Requirement, which would be impossible or very difficult to accurately estimate; and (b) may, at the University's option, be credited or set off against any Fees or other charges payable to Supplier under this Agreement or be payable to the University upon demand. Credits may not exceed the total amount of Fees that would be payable for the relevant service period in which the credits are assessed.

8.11 Right of Set-off. Without prejudice to any other right or remedy it may have, the University reserves the right to set off at any time any amount then due and owing to it by Supplier against any amount payable by the University to Supplier.

9. University Data.

9.1 Ownership. The University's data includes any and all data collected, used, processed, stored, or generated in connection with the Services that originates from the University, its Administrative Users, or End Users, including any User Data (collectively, "**University Data**"). University Data is and will remain the sole and exclusive property of the University and all right, title, and interest in the same is reserved by the University. This **Section 9.1** survives termination or expiration of this Agreement.

9.2 Supplier Use of University Data. At all times, University Data will be treated as Confidential Information. Supplier is provided a limited license to University Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display University Data only to the extent necessary in the provision of the Services. Supplier must: (a) keep and maintain University Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Agreement and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose University Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Agreement, the Statement of Work, and applicable law; (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available University Data for Supplier's own purposes or for the benefit of anyone other than the University without the University's prior written consent; and (d) not use, process, input, or analyze University Data (or permit any third party to do so), whether or not de-identified, anonymized, aggregated, or pseudonymized, for the purpose of training, developing, pre-training, fine-tuning, improving, enhancing, or otherwise creating or modifying any artificial intelligence, machine learning models, foundation models, generative AI systems, large language models, multimodal models, algorithms, or similar technologies (whether now known or hereafter developed), including as prompts, context, retrieval sources, or to generate outputs/derivatives/synthetic data for such purposes, except with the University's prior express written consent. Any breach of this Section shall constitute a material breach of this Agreement, entitling the University to seek appropriate remedies, including but not limited to injunctive relief and damages. This **Section 9.2** survives termination or expiration of this Agreement.

9.3 Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Supplier that compromises the security or confidentiality of University Data or the physical, technical, administrative, or organizational safeguards put in place by Supplier that relate to the protection of the security and confidentiality of University Data, Supplier must, as applicable: (a) notify the University as soon as practicable but no later than forty-eight (48) hours of becoming aware of such occurrence; (b) cooperate with the University in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the University; (c) in the case of personally identifiable information ("PII"), at the University's sole election, (i) with approval and assistance from the University, notify the affected individuals who comprise the PII as soon as practicable but no later than is required to comply with applicable law; or (ii) reimburse the University for any costs in notifying the affected individuals; (d) in the case of PII, and if required by law, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law; (e) perform or take any other actions required to comply with applicable law as a result of the occurrence; (f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the University in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution; (g) without limiting Supplier's obligations of indemnification as further described in this Agreement, indemnify, defend, and hold harmless the University for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the University in connection with the occurrence; (h) be responsible for recreating lost University Data in the manner and on the schedule set by the University without charge to the University; and (i) provide to the University a detailed plan within ten (10) calendar days of the occurrence describing the measures Supplier will undertake to

prevent a future occurrence. The University will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by the University in writing prior to its dissemination. This **Section 9.3** survives termination or expiration of this Agreement.

10. FERPA Compliance. University is a qualifying educational agency or institution under the U.S. Family Educational Rights and Privacy Act (“**FERPA**”). To the extent Supplier or its personnel have access to data protected by FERPA, Supplier acknowledges that for the purposes of this Agreement it is designated as a “school official” with “legitimate educational interests” in such data and associated metadata, as defined under FERPA and its implementing regulations, and agrees to abide by the limitations and requirements imposed on school officials under those regulations. Supplier agrees to use such data only for the purpose of fulfilling its duties under this Agreement, and will not monitor, share, or disclose any such data to any third party except as provided for in this Agreement, as required by law, or as authorized in writing by University. Supplier specifically agrees not to use any data for purposes of targeted advertising.

11. ADA Compliance. The University is required to comply with the Americans with Disabilities Act of 1990 (ADA), and has adopted a formal policy regarding accessibility requirements for websites and software applications. Supplier’s Service Software must comply, where relevant, with level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.2.

12. HIPAA Compliance. The University and Supplier must comply with all obligations under the Health Insurance Portability and Accountability Act of 1996, and the Health Information Technology for Economic and Clinical Health Act, and any amendments or implementing regulations thereof, (collectively, the “**HIPAA Rules**”). University and Supplier will enter into a separate Business Associate Agreement, if reasonably necessary to keep the University and Supplier in compliance with the HIPAA Rules.

13. PCI Compliance.

13.1 Supplier shall at all times, for as long as Supplier impacts the security of the University’s cardholder data environment, or stores, processes, handles or transmits cardholder data in any manner or in any format on behalf of the University, comply with all applicable requirements of the current version of the Payment Card Industry Data Security Standard (“**PCI DSS**”) for cardholder data that is prescribed by the Payment Card Industry Security Standards Council, as it may be amended from time to time. The most current versions of the PCI DSS requirements documentation are available at the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>.

13.2 Supplier must be designated by Visa as a Level 1 Supplier and be listed in Visa’s Global Registry of service providers. Service providers that self-assess their PCI compliance are not eligible to become a PCI Supplier for the University. Supplier shall validate compliance with PCI DSS as required, and shall have provided appropriate documentation to the University before the Agreement is signed and upon request by the University thereafter, at least annually, for as long as services are provided. Validation instructions and documentation are available at the PCI Security Standards Council website, <https://www.pcisecuritystandards.org/>. Supplier must notify the University of any failure to comply with the PCI-DSS requirements.

13.3 Supplier acknowledges and agrees that cardholder data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the card associations or as required by applicable law. Supplier is solely responsible for the security of cardholder data in its possession, or in the possession of a third-party retained by Supplier. In the event of unauthorized access to cardholder data which occurs during the access, storage, processing, or transmission of cardholder data by the Supplier, or by a third-party retained by Supplier, Supplier shall immediately notify the University, which shall not be more than forty-eight (48) hours after becoming aware of such unauthorized access.

13.4 In the event of unauthorized access to cardholder data which occurs during access, storage, processing, or transmission of cardholder data by the Supplier, or by a third-party retained by Supplier, Supplier will pay all fees, cost escalations, assessments, tariffs, penalties or fines that may be imposed under the Card Association Rules. Supplier further agrees to pay all other expenses that may be incurred by the University related to such unauthorized access.

13.5 Without limiting Supplier's obligations of indemnification as further described in this Agreement, Supplier must indemnify, defend, and hold harmless the University for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the University in connection with unauthorized access to cardholder data which occurs during access, storage, processing, or transmission of cardholder data by the Supplier, or by a third-party retained by Supplier.

14. Confidentiality.

14.1 Meaning of Confidential Information. The term "**Confidential Information**" means all information and documentation of a party that: (a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked "confidential" or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked "confidential" or with words of similar meaning; or, (c) should reasonably be recognized as confidential information of the disclosing party. The term "Confidential Information" does not include any information or documentation that was or is: (a) in the possession of the University and subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). Notwithstanding the above, in all cases and for all matters, University Data is deemed to be Confidential Information.

14.2 Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Agreement or to use such Confidential Information for any purposes whatsoever other than the performance of this Agreement. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential

Information confidential. Disclosure to the Supplier's Subcontractor is permissible where (a) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Subcontractor's responsibilities; and (b) Supplier obligates the Subcontractor in a written contract to maintain the University's Confidential Information in confidence. At the University's request, any of the Supplier's Representatives may be required to execute a separate agreement to be bound by the provisions of this **Section 14.2**.

14.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Agreement. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

14.4 Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of the University, at the sole election of the University, the immediate termination, without liability to the University, of this Agreement.

14.5 Surrender of Confidential Information upon Termination. Upon termination or expiration of this Agreement, each party must, within five (5) Business Days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. If Supplier or the University determine that the return of any Confidential Information is not feasible, such party must destroy the Confidential Information and certify the same in writing within five (5) Business Days from the date of termination to the other party.

15. Security. Throughout the Term and at all times in connection with its actual or required performance of the Services, Supplier will provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, transfer, commingling or processing of University Data that ensures a level of security appropriate to the risks presented by the nature of such data, consistent with industry best practices and standards. Supplier will, at a minimum, do all of the following:

15.1 Network Security. Supplier shall at all times maintain network security that includes, at a minimum: network firewall provisioning, intrusion detection, and regular third party penetration testing of the network and all relevant computer/data storage devices;

15.2 Hosting location. Supplier will ensure that the Services are hosted, supported, administered, and accessed in a data center that resides in the continental United States;

15.3 Data Transmission. Supplier shall ensure that any and all transmission or exchange of University Data shall take place by secure means, e.g., HTTPS or FTPS; and

15.4 Data Encryption. Supplier shall store and backup Data as part of its designated backup and recovery processes in encrypted form, using no less than 128 bit key encryption.

16. Disaster Recovery and Backup.

16.1 Disaster Recovery. Throughout the Term and at all times in connection with its actual or required performance of the Services, Supplier will maintain and operate a backup and disaster recovery plan to achieve a Recovery Point Objective (RPO) of 24 hours, and a Recovery Time Objective (RTO) of 48 hours (the “**DR Plan**”), and implement such DR Plan in the event of any unplanned interruption of the Services. Supplier will actively test, review and update the DR Plan on at least an annual basis using industry best practices as guidance, and maintain any additional backup requirements set forth in the Statement of Work. If Supplier fails to reinstate all material Services within the periods of time set forth in the DR Plan, the University may, in addition to any other remedies available under this Agreement, in its sole discretion, immediately terminate this Agreement as a non-curable default under **Section 7.1(a)**.

16.2 Backup of University Data. Supplier will conduct, or cause to be conducted periodic back-ups of University Data at a frequency that will ensure the RPO requirements set forth above. All backed up University Data shall be located in the continental United States.

17. Indemnification.

17.1 General Indemnification. Supplier must defend, indemnify and hold harmless the University, and the University’s Board of Trustees, departments, officers, employees, agents, and contractors from and against all Losses arising out of or resulting from any third party claim, suit, action or proceeding (each, an “**Action**”) that does or is alleged to arise out of or result from: (a) any breach by Supplier (or any of Supplier Personnel, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Agreement; (b) any infringement, misappropriation, or other violation of any intellectual property right of any third party; and (c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Supplier or any of Supplier Personnel, or by anyone else for whose acts any of them may be liable).

17.2 Indemnification Procedure. The University will notify Supplier in writing if indemnification is sought; however, failure to do so will not relieve Supplier, except to the extent that Supplier is materially prejudiced. Supplier must, to the satisfaction of the University, demonstrate its financial ability to carry out these obligations. The University is entitled to: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; (iii) employ its own counsel; and to (iv) retain control of the defense, at its own expense, if the University deems necessary. Supplier will not, without the University’s prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding.

18. Limitations of Liability.

(a) Disclaimer of Damages. NEITHER PARTY WILL BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS AGREEMENT

FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

(b) Limitation of Liability. OTHER THAN SUPPLIER'S OBLIGATIONS WITH RESPECT TO THE PROTECTION OF UNIVERSITY DATA, IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY TO THE OTHER PARTY UNDER THIS AGREEMENT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS AGREEMENT, EXCEED THE MAXIMUM AMOUNT OF FEES SPECIFIED IN THE STATEMENT OF WORK.

19. Supplier Representations and Warranties.

19.1 Authority and Bid Response. Supplier represents and warrants to the University that:

(a) it is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Agreement under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;

(b) it has the full right, power, and authority to enter into this Agreement, to grant the rights and licenses granted under this Agreement, and to perform its contractual obligations;

(c) the execution of this Agreement by its Representative has been duly authorized by all necessary organizational action;

(d) when executed and delivered by Supplier, this Agreement will constitute the legal, valid, and binding obligation of Supplier, enforceable against Supplier in accordance with its terms; and

(e) all written information furnished to the University by or for Supplier in connection with this Agreement, including Supplier's bid response to the RFP, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading;

19.2 Software and Service Warranties. Supplier represents and warrants to the University that:

(a) Supplier has, and throughout the Term and any additional periods during which Supplier does or is required to perform the Services will have, the unconditional and irrevocable right, power and authority, including all permits and licenses required, to provide the Services and grant and perform all rights and licenses granted or required to be granted by it under this Agreement;

(b) neither Supplier's grant of the rights or licenses hereunder nor its performance of any Services or other obligations under this Agreement does or at any time will: (i) conflict with or violate any applicable Law, including any Law relating to data privacy, data security or personal information; (ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or (iii) require the provision of any payment or other consideration by the University or any End User to any third party, and Supplier shall promptly notify the University in writing if it becomes aware of

any change in any applicable Law that would preclude Supplier's performance of its material obligations hereunder;

(c) as accessed and used by the University, its Administrative Users, or End Users in accordance with this Agreement and the Specifications, the Services, Documentation and all other Services and materials provided by Supplier under this Agreement will not infringe, misappropriate or otherwise violate any intellectual property right of any third party;

(d) the Service Software and Services will in all material respects conform to and perform in accordance with the Specifications and all requirements of this Agreement, including the Availability Requirement set forth in the Service Level Agreement;

(e) Supplier will perform all Services in a timely, professional and workmanlike manner with a level of care, skill, practice and judgment consistent with generally recognized industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet Supplier's obligations (including the Availability Requirement and Support Service Level Requirements) under this Agreement;

19.3 DISCLAIMER. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS CONTRACT, SUPPLIER HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE UNDER OR IN CONNECTION WITH THIS CONTRACT OR ANY SUBJECT MATTER HEREOF.

20. Insurance. While performing services under this Agreement, Supplier shall purchase and maintain the following insurance:

(a) Workers Compensation insurance, Coverage A, with limits statutorily required by any applicable Federal or state law and Employers Liability insurance, Coverage B, with minimum limit of \$500,000 per accident;

(b) Commercial General Liability insurance with a minimum limit of \$1,000,000 each occurrence/\$2,000,000 general aggregate. Coverage shall include bodily injury and property damage liability, personal and advertising injury liability, products/completed operations, and liability assumed under an insured contract;

(c) Automobile Liability insurance covering liability arising out of any owned, hired, and non-owned vehicles with minimum limit of \$1,000,000 each accident and Personal Injury Protection as required by statute;

(d) Professional Liability insurance for claims arising from negligent acts, errors or omissions by anyone providing professional services including but not limited to doctors, lawyers, architects, engineers, designers, appraisers and consultants. Minimum limit is \$1,000,000 per claim and \$3,000,000 annual aggregate; and

(e) For services that may impact the security of the University's electronic data, or Suppliers that store, process, handle or transmit University data in electronic format, Cyber Liability Insurance

coverage with limits no less than \$1 million.

Insurance policies shall be issued by companies licensed or approved to do business within the State of Michigan. Insurers shall possess a minimum A.M. Best rating of A. The insurance policies, except Workers' Compensation and Professional Liability shall be endorsed to name Michigan State University, its Board of Trustees, agents, officers, employees, and volunteers as "Additional Insureds." In the event any insurance policies required by this Agreement are written on a "claims made" basis, coverage shall extend for three years past completion and acceptance of Supplier's Services and must be evidenced by annual certificates of insurance. All policies of insurance must be on a primary basis, non-contributory with any other insurance and/or self-insurance carried by MSU. Prior to commencing services Supplier shall furnish the University with certificates of insurance. Supplier shall provide a minimum 30 days written notice to MSU via certified mail of cancellation or non-renewal of policies required under this Agreement and a renewal certificate at least 15 days prior to expiration.

21. Force Majeure.

21.1 Force Majeure Events. Subject to **Section 21.2**, neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of this Agreement, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure Event**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

21.2 University Performance; Termination. In the event of a Force Majeure Event affecting Supplier's performance under this Agreement, the University may suspend its performance hereunder until such time as Supplier resumes performance. The University may terminate this Agreement by written notice to Supplier if a Force Majeure Event affecting Supplier's performance hereunder continues substantially uninterrupted for a period of five (5) Business Days or more. Unless the University terminates this Agreement pursuant to the preceding sentence, any date specifically designated for Supplier's performance under this Agreement will automatically be extended for a period up to the duration of the Force Majeure Event.

21.3 Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of this Agreement:

- (a) in no event will any of the following be considered a Force Majeure Event:
 - (i) shutdowns, disruptions or malfunctions of the Supplier Systems or any of Supplier's telecommunication or internet services other than as a result of general and

widespread internet or telecommunications failures that are not limited to the Supplier Systems; or

- (ii) the delay or failure of any Supplier Personnel to perform any obligation of Supplier hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event; and

(b) no Force Majeure Event modifies or excuses Supplier's obligations under **Section 9** (University Data), **Section 14** (Confidentiality), **Section 15** (Security), **Section 16** (Disaster Recovery) or **Section 17** (Indemnification).

22. Software Escrow. The parties may enter into a separate intellectual property escrow agreement. Such escrow agreement will govern all aspects of source code escrow and release.

23. General Provisions.

23.1 Further Assurances. Each party will, upon the reasonable request of the other party, execute such documents and perform such acts as may be necessary to give full effect to the terms of this Agreement.

23.2 Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Agreement is to be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the parties, and neither party has authority to contract for or bind the other party in any manner whatsoever.

23.3 Use of the University Name, Logo and Marks. The University acknowledges that Supplier may make public statements regarding the existence of this Agreement, its terms and conditions and an accurate description of the products or services being supplied without the consent of the University. However, other than as permitted by the previous sentence, Supplier will not use the name, logo, or any other marks (including, but not limited to, colors and music) owned by or associated with the University, or the name of any representative of the University without the prior written permission of the University in each instance. Supplier may not imply, directly or indirectly, that MSU endorses any products or services supplied to MSU.

23.4 Notices. All notices, requests, consents, claims, demands, waivers and other communications hereunder, other than routine communications having no legal effect, must be in writing and addressed to the parties as follows (or as otherwise specified by a party in a notice given in accordance with this Section):

If to Supplier:

[SUPPLIER ADDRESS]

E-mail: [E-MAIL ADDRESS]

Attention: [NAME OF INDIVIDUAL TO RECEIVE NOTICES]

Title: [TITLE OF INDIVIDUAL TO RECEIVE NOTICES]

If to the University:

MSU Procurement

Hannah Administration

426 Auditorium Road, Suite 360

East Lansing, MI 48823

E-mail: vendor@msu.edu

Attention: MSU Procurement Contract Manager

Notices sent in accordance with this **Section 23.4** will be deemed effectively given: (a) when received, if delivered by hand (with written confirmation of receipt); (b) when received, if sent by a nationally recognized overnight courier (receipt requested); (c) on the date sent by e-mail (with confirmation of transmission), if sent during normal business hours of the recipient, and on the next business day, if sent after normal business hours of the recipient; or (d) on the fifth (5th) day after the date mailed, by certified or registered mail, return receipt requested, postage prepaid.

23.5 Headings. The headings in this Agreement are for reference only and do not affect the interpretation of this Agreement.

23.6 Assignment. Supplier may not assign this Agreement, nor any money due or to become due without the prior written consent of the University. Any assignment made without such consent shall be deemed void.

23.7 No Third-party Beneficiaries. This Agreement is for the sole benefit of the parties and nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Agreement.

23.8 Amendment and Modification; Waiver. This Agreement may only be amended, modified or supplemented by an agreement in writing signed by each party's authorized Representative. No waiver by any party of any of the provisions hereof is effective unless explicitly set forth in writing and signed by the party so waiving. Except as otherwise set forth in this Agreement, no failure to exercise, or delay in exercising, any right, remedy, power or privilege arising from this Agreement will operate or be construed as a waiver thereof; nor will any single or partial exercise of any right, remedy, power or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power or privilege.

23.9 Severability. If any term or provision of this Agreement is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability will not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal or unenforceable, the parties hereto

will negotiate in good faith to modify this Agreement so as to effect the original intent of the parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

23.10 Governing Law. This Agreement is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Agreement are governed by Michigan law, excluding choice-of-law principles.

23.11 Equitable Relief. Each party to this Agreement acknowledges and agrees that (a) a breach or threatened breach by such party of any of its obligations under this Agreement would give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy and (b) in the event of a breach or a threatened breach by such party of any such obligations, the other party hereto is, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, entitled to equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual damages or that monetary damages will not afford an adequate remedy. Each party to this Agreement agrees that such party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this **Section 23.11**.

23.12 Nondiscrimination Under Michigan Law. Pursuant to Section 209 of the Michigan Elliot-Larsen Civil Rights Act and Section 209 of the Michigan Persons with Disabilities Civil Rights Act, in providing services, the Supplier and its contractor(s) agree not to discriminate against any employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or any matter directly or indirectly related to employment, because of age, color, familial status, height, marital status, national origin, race, religion, sex, sexual orientation, gender identity or expression, weight, disability or genetic information that is unrelated to the individual's ability to perform the duties of a particular job or position.

23.13 Exclusion And Debarment. Supplier certifies that it is not presently debarred, suspended, proposed for debarment, declared ineligible, voluntarily excluded or otherwise ineligible for state or Federal program participation. In the event that Supplier becomes debarred, suspended or ineligible from state or Federal program participation, Supplier shall notify MSU in writing within three (3) business days of such event. To the extent that Supplier will provide services to any MSU medical entity, Supplier hereby represents and warrants that Supplier is not currently, and at no time has been sanctioned, debarred, suspended, or excluded by any state or federally funded healthcare program, including without limitation, Medicare and Medicaid. Supplier agrees to immediately notify MSU of any threatened, proposed, or actual sanctions, debarment action, suspension, or exclusion by or from any state or federally funded health care program during the term of this Agreement.

23.14 Federal Contract Compliance.

(a) **University is an equal opportunity employer and a federal contractor or subcontractor. Consequently, the parties agree that, as applicable, they will abide by the**

requirements of 41 CFR 60-300.5(a) and 41 CFR 60-741.5(a) and that these laws are incorporated herein by reference. These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender identity or national origin. These regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to protected veteran status or disability. The parties also agree that, as applicable, they will abide by the requirements of 29 CFR Part 471, Appendix A to Subpart A, relating to the notice of employee rights under federal labor laws.

(b) In accordance with (i) Public Law 115-91 and FAR 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities, (ii) Public Law 115-232 and FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, and (iii) FAR 52.204-30, Federal Acquisition Supply Chain Security Act (FASCSA) Orders Prohibition, Supplier is prohibited from delivering covered telecommunications equipment as defined in FAR 52.204-25, covered articles as defined in FAR 52.204-23, or covered articles as defined under FAR 52.204-30 and identified pursuant to an FASCSA order. Supplier hereby represents and warrants that it will abide by the prohibitions contained in this Section.

(c) Supplier acknowledges and represents, in accordance with the Final Rule implementing Executive Order 14117 issued by the U.S. Department of Justice, that if Supplier has access to Covered Data of the University (as defined under the Final Rule): (i) it is not located in China, Hong Kong, Macau, Russia, Iran, North Korea, Venezuela, or Cuba; and (ii) it will not provide access to any Covered Data to any person located in such countries unless University approves such access in writing. Non-compliance with this provision will be considered a material breach of this agreement.

23.15 Export Control. Supplier declares that all products or services purchased under the Agreement are neither subject to the International Traffic in Arms Regulations (ITAR) nor any of the Export Administration Regulations (EAR) Export Control Classification Numbers (ECCN's) in the 500 or 600 series as listed on the Commerce Control List (CCL). If any products or services are subject to ITAR or EAR ECCN's in the 500 or 600 series, Supplier shall notify University's Office of Export Control & Trade Sanctions (export@msu.edu) prior to shipment of the products or performance of the services. For the avoidance of doubt, unless Supplier has provided advance notice to University's Office of Export Control and Trade Sanctions, Supplier declares and warrants that (i) the products or services are not listed on the ITAR United States Munitions List (USML); and (ii) the products or services are not listed on the EAR CCL in ECCN's in the 500 or 600 series. Supplier declares that it fully understands that sourcing any products or services classified in any of the above categories could have material adverse implications and require extensive management for the University, and therefore Supplier agrees to defend, indemnify and hold harmless the University for any costs or liability related to Supplier's violation of this Section.

23.16 Conflict of Interest. Supplier warrants that to the best of Supplier's knowledge, there exists no actual or potential conflict between Supplier and the University, and its Services under this Agreement, and in the event of change in either Supplier's private interests or Services under this

Agreement, Supplier will inform the University regarding possible conflict of interest which may arise as a result of the change. Supplier also affirms that, to the best of Supplier's knowledge, there exists no actual or potential conflict between a University employee and Supplier.

23.17 Schedules All Schedules and Exhibits that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Exhibit 1 to Schedule A	Pricing
Schedule B	Service Level Agreement

23.18 Counterparts. This Agreement may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Agreement. A signed copy of this Agreement delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

23.19 Entire Agreement. This Agreement, including the Statement of Work and other Schedules and Exhibits attached hereto, constitute the sole and entire agreement of the parties to this Agreement with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, both written and oral, with respect to such subject matter. In the event of any conflict between the terms of this Agreement and those of any Schedule, Exhibit or other document, the following order of precedence governs: (a) first, this Agreement, excluding its Exhibits and Schedules; and (b) second, the Exhibits and Schedules to this Agreement as of the Effective Date. NO TERMS ON SUPPLIER'S INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE UNIVERSITY OR ANY ADMINISTRATIVE USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE UNIVERSITY AND THE ADMINISTRATIVE USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

[Signature Page Follows]

MSU

BY: _____

Name: _____

Title: _____

Date: _____

Supplier

By: _____

Name: _____

Title: _____

Date: _____

SCHEDULE A

Statement of Work

(To be completed by the parties after award)

SCHEDULE B
Service Level Agreement

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Section 1** shall have the respective meanings given to them in the Agreement.

“Actual Uptime” means the total minutes in the Service Period that the Services are Available.

“Availability” has the meaning set forth in **Section 2(a)**.

“Availability Requirement” has the meaning set forth in **Section 2(a)**.

“Available” has the meaning set forth in **Section 2(a)**.

“Corrective Action Plan” has the meaning set forth in **Section 3.5**.

“Critical Service Error” has the meaning set forth in **Section 3.4(a)**.

“Exceptions” has the meaning set forth in **Section 2.2**.

“High Service Error” has the meaning set forth in **Section 3.4(a)**.

“Low Service Error” has the meaning set forth in **Section 3.4(a)**.

“Medium Service Error” has the meaning set forth in **Section 3.4(a)**.

“Resolve” has the meaning set forth in **Section 3.4(b)**.

“Scheduled Downtime” has the meaning set forth in **Section 2.3**.

“Scheduled Uptime” means the total minutes in the Service Period.

“Service Availability Credits” has the meaning set forth in **Section 2.6(a)**.

“Service Error” means any failure of any Services to be Available or otherwise perform in accordance with this Schedule.

“Service Level Failure” means a failure to perform the Services fully in compliance with the Support Service Level Requirements.

“Service Period” has the meaning set forth in **Section 2(a)**.

“Software Support Services” has the meaning set forth in **Section 3**.

“Support Request” has the meaning set forth in **Section 3.4(a)**.

“Support Service Level Requirements” has the meaning set forth in **Section 3.4**.

2. Service Availability and Service Availability Credits.

(a) Availability Requirement. Supplier will make the Services Available, as measured over the course of each calendar month during the Term and any additional periods during which Supplier does or is required to perform any Services (each such calendar month, a “**Service Period**”), at least 99.95% of the time, excluding only the time the Services are not Available solely as a result of one or more Exceptions (the “**Availability Requirement**”). “**Available**” means the Services are available and operable for access and use by the University, its Administrative Users and End Users over the Internet in material conformity with the Agreement. “**Availability**” has a correlative meaning. The Services are not considered Available in the event of a material performance degradation or inoperability of the Services, in whole or in part. The Availability Requirement will be calculated for the Service Period as follows: $(\text{Actual Uptime}) \div (\text{Scheduled Uptime} - \text{Total Minutes in Service Period Services are not Available Due to an Exception}) \times 100 = \text{Availability}$.

2.2 Exceptions. No period of Services degradation or inoperability will be included in calculating Availability to the extent that such downtime or degradation is due to any of the following (“**Exceptions**”):

- (a) failures of the University’s, its Administrative Users’ or an End User’s internet connectivity;
- (b) Scheduled Downtime as set forth in **Section 2.3**.

2.3 Scheduled Downtime. Supplier must notify the University at least seventy-two (72) hours in advance of all scheduled outages of the Services in whole or in part (“**Scheduled Downtime**”). All such scheduled outages will: (a) last no longer than five (5) hours; and (b) be scheduled on a Saturday between the hours of 12:00 a.m. and 5:00 a.m., Eastern Time; provided that Supplier may request the University to approve extensions of Scheduled Downtime above five (5) hours, and such approval by the University may not be unreasonably withheld or delayed.

2.4 Software Response Time. Software response time, defined as the interval from the time the End User sends a transaction to the time a visual confirmation of transaction completion is received, must be less than two (2) seconds for 98% of all transactions. Unacceptable response times shall be considered to make the Software unavailable and will count against the Availability Requirement.

2.5 Service Availability Reports. Within thirty (30) days after the end of each Service Period, Supplier will provide to the University a report describing the Availability and other performance of the Services during that calendar month as compared to the Availability Requirement. The report must be in electronic or such other form as the University may approve in writing and shall include, at a minimum: (a) the actual performance of the Services relative to the Availability Requirement; and (b) if Service performance has failed in any respect to meet or exceed the Availability Requirement during the reporting period, a description in sufficient detail to inform the University of the cause of such failure and the corrective actions the Supplier has taken and will take to ensure that the Availability Requirement are fully met.

2.6 Remedies for Service Availability Failures.

(a) If the actual Availability of the Services is less than the Availability Requirement for any Service Period, such failure will constitute a Service Error for which Supplier will issue to the University the following credits on the fees payable for Services provided during the Service Period (“**Service Availability Credits**”):

Availability	Credit of Fees
≥99.95%	None
<99.95% but ≥99.0%	15%
<99.0% but ≥95.0%	50%
<95.0%	100%

(b) Any Service Availability Credits due under this **Section 2.6** will be applied in accordance with payment terms of the Agreement.

(c) Supplier's repeated failure to meet the Availability Requirements will constitute a material breach under the Agreement. Without limiting the University's right to receive Service Availability Credits, the University may terminate the Agreement for cause in accordance with terms of the Agreement.

3. Support and Maintenance Services. Supplier will provide maintenance and support services for the Services (collectively, “**Software Support Services**”) in accordance with the provisions of this **Section 3**. The Software Support Services are included in the Services, and Supplier may not assess any additional fees, costs or charges for such Software Support Services.

3.1 Support Service Responsibilities. Supplier will:

- (a) correct all Service Errors in accordance with the Support Service Level Requirements, including by providing defect repair, programming corrections and remedial programming;
- (b) provide unlimited telephone support 8 a.m. to 7 p.m. Eastern, Monday through Friday;
- (c) provide unlimited online support 8 a.m. to 7 p.m. Eastern, Monday through Friday;
- (d) provide online access to technical support bulletins and other user support information and forums, to the full extent Supplier makes such resources available to its other customers; and
- (e) respond to and Resolve Support Requests as specified in this **Section 3**.

3.2 Service Monitoring and Management. Supplier will continuously monitor and manage the Services to optimize Availability that meets or exceeds the Availability Requirement. Such monitoring and management includes:

- (a) proactively monitoring on a twenty-four (24) hour by seven (7) day basis all Services functions, servers, firewall and other components of Services security;

(b) if such monitoring identifies, or Supplier otherwise becomes aware of, any circumstance that is reasonably likely to threaten the Availability of the Services, taking all necessary and reasonable remedial measures to promptly eliminate such threat and ensure full Availability; and

(c) if Supplier receives knowledge that the Services or any Services function or component is not Available (including by written notice from the University pursuant to the procedures set forth herein):

- (i) confirming (or disconfirming) the outage by a direct check of the associated facility or facilities;
- (ii) if Supplier's facility check in accordance with clause (i) above confirms a Services outage in whole or in part: (A) notifying the University in writing pursuant to the procedures set forth herein that an outage has occurred, providing such details as may be available, including a Supplier trouble ticket number, if appropriate, and time of outage; and (B) working all problems causing and caused by the outage until they are Resolved as Critical Service Errors in accordance with the Support Request Classification set forth in **Section 3.4**, or, if determined to be an internet provider problem, open a trouble ticket with the internet provider; and
- (iii) notifying the University that Supplier has fully corrected the outage and any related problems, along with any pertinent findings or action taken to close the trouble ticket.

3.3 Service Maintenance. Supplier will continuously maintain the Services to optimize Availability that meets or exceeds the Availability Requirement. Such maintenance services include providing to the University:

- (a) all updates, bug fixes, enhancements, new releases, new versions and other improvements to the Services, including the Software, that Supplier provides at no additional charge to its other similarly situated customers; and
- (b) all such services and repairs as are required to maintain the Services or are ancillary, necessary or otherwise related to the University's, its Administrative Users, or an End Users' access to or use of the Services, so that the Services operate properly in accordance with the Agreement and this Schedule.

3.4 Support Service Level Requirements. Supplier will correct all Service Errors and respond to and Resolve all Support Requests in accordance with the required times and other terms and conditions set forth in this **Section 3.4 ("Support Service Level Requirements")**, and the Agreement.

(a) **Support Requests.** The University will classify its requests for Service Error corrections in accordance with the descriptions set forth in the chart below (each a "**Support Request**"). The University Service Manager will notify Supplier of Support Requests by email, telephone or such other means as the parties may hereafter agree to in writing.

Support Request Classification	Description: Any Service Error Comprising or Causing any of the Following Events or Effects
Critical Service Error	<ul style="list-style-type: none"> • Issue affecting entire system or single critical production function; • System down or operating in materially degraded state; • Data integrity at risk; or • Declared a Critical Support Request by the University and confirmed by Supplier;
High Service Error	<ul style="list-style-type: none"> • Primary component failure that materially impairs its performance; or • Data entry or access is materially impaired on a limited basis. • User interface portions of the Services are not compliant with Section 11 of the Agreement.
Medium Service Error	<ul style="list-style-type: none"> • Services is operating with minor issues that can be addressed with an acceptable (as determined by the University) temporary work around.
Low Service Error	<ul style="list-style-type: none"> • Request for assistance, information, or services that are routine in nature.

(b) Response and Resolution Time Service Levels. Response and Resolution times will be measured from the time Supplier receives a Support Request until the respective times Supplier has (i) responded to, in the case of response time and (ii) Resolved such Support Request, in the case of Resolution time. **“Resolve”** (including **“Resolved”**, **“Resolution”** and correlative capitalized terms) means that, as to any Service Error, Supplier has provided the University the corresponding Service Error

correction and the University has confirmed such correction and its acceptance thereof. Supplier will respond to and Resolve all Service Errors within the following times based on the severity of the Service Error:

Support Request Classification	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)
Critical Service Error	One (1) hour	Three (3) hours
High Service Error	One (1) hour	Four (4) hours
Medium Service Error	Three (3) hours	Two (2) Business Days
Low Service Error	Three (3) hours	Five (5) Business Days

(c) Escalation. With respect to any Critical Service Error Support Request, until such Support Request is Resolved, Supplier will escalate that Support Request within sixty (60) minutes of the receipt of such Support Request by the appropriate Supplier support personnel, including, as applicable, the Supplier Service Manager and Supplier's management or engineering personnel, as appropriate.

3.5 Corrective Action Plan. If two or more Critical Service Errors occur in any thirty (30) day period during (a) the Term or (b) any additional periods during which Supplier does or is required to perform any Services, Supplier will promptly investigate the root causes of these Service Errors and provide to the University within five (5) Business Days of its receipt of notice of the second such Support Request an analysis of such root causes and a proposed written corrective action plan for the University's review, comment and approval, which, subject to and upon the University's written approval, shall be a part of, and by this reference is incorporated in, the Agreement as the parties' corrective action plan (the "**Corrective Action Plan**"). The Corrective Action Plan must include, at a minimum: (a) Supplier's commitment to the University to devote the appropriate time, skilled personnel, systems support and equipment and other resources necessary to Resolve and prevent any further occurrences of the Service Errors giving rise to such Support Requests; (b) a strategy for developing any programming, software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of, such Service Errors; and (c) time frames for implementing the Corrective Action Plan. There will be no additional charge for Supplier's preparation or implementation of the Corrective Action Plan in the time frames and manner set forth therein.

3.6 Remedies for Service Level Failures. Supplier's repeated failure to meet the Support Service Level Requirements for any Critical Service Errors or High Service Errors, or any combination of such Errors, within the applicable Resolution time will constitute a material breach under the Agreement. Without limiting the University's right to receive Service Availability Credits, the University may terminate the Agreement for cause in accordance with terms of the Agreement.

HIPAA Business Associate Agreement

THIS HIPAA BUSINESS ASSOCIATE AGREEMENT (the "Agreement") is entered into effective [Add Date], by and between [Entity Name] ("Business Associate") and the Board of Trustees of Michigan State University, a Michigan constitutional body corporate ("Covered Entity").

The Business Associate may perform functions or activities on behalf of Covered Entity involving the use, disclosure, transmission, or maintenance of protected health information created or received by Business Associate on behalf of Covered Entity ("PHI"). Therefore, if Business Associate is functioning in this capacity for Covered Entity, Business Associate agrees to the following terms and conditions set forth in this HIPAA Business Associate Agreement.

1. **Definitions.** For purposes of this Agreement, the terms used herein, unless otherwise defined, shall have the same meanings as used in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), or the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and any amendments or implementing regulations, (collectively "HIPAA Rules").
2. **Compliance with Applicable Law.** The parties acknowledge and agree that, beginning with the relevant effective dates, Business Associate shall comply with its obligations under this Agreement and with all obligations of a business associate under HIPAA, HITECH, the HIPAA Rules, and other applicable laws and regulations, as they exist at the time this Agreement is executed and as they are amended, for so long as this Agreement is in place.
3. **Permissible Use and Disclosure of PHI.** Business Associate may use and disclose PHI as necessary to carry out its duties to Covered Entity pursuant to the terms of the Agreement and as required by law. Business Associate may also use and disclose PHI (i) for its own proper management and administration, and (ii) to carry out its legal responsibilities. If Business Associate discloses Protected Health Information to a third party for either above reason, prior to making any such disclosure, Business Associate must obtain: (i) reasonable assurances from the receiving party that such PHI will be held confidential and be disclosed only as required by law or for the purposes for which it was disclosed to such receiving party; and (ii) an agreement from such receiving party to immediately notify Business Associate of any known breaches of the confidentiality of the PHI.
4. **Limitations on Use and Disclosure of PHI.** Business Associate shall not, and shall ensure that its directors, officers, employees, subcontractors, and agents do not, use or disclose PHI in any manner that is not permitted by this Agreement or that would violate Subpart E of 45 CFR 164 ("Privacy Rule") if done by Covered Entity. All uses and disclosures of, and requests by, Business Associate for PHI are subject to the minimum necessary rule of the Privacy Rule and consistent with Covered Entity's minimum necessary policies and procedures.
5. **Required Safeguards To Protect PHI.** Business Associate shall use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 ("Security Rule") with respect to electronic PHI, to prevent the use or disclosure of PHI other than pursuant to the terms and conditions of this Agreement.
6. **Reporting to Covered Entity.** Business Associate shall report to Covered Entity within 48 hours: (a) any use or disclosure of PHI not provided for by this Agreement of which it becomes aware; (b) any breach of unsecured PHI in accordance with 45 CFR Subpart D of 45 CFR 164 ("Breach Notification Rule"); and (c) any security incident of which it becomes aware. To report any disclosures, breaches, or security incidents, contact the MSU HealthTeam Privacy Officer at (517) 355-1822.

Business Associate shall cooperate with Covered Entity's investigation, analysis, notification and mitigation activities.

7. **Mitigation of Harmful Effects.** Business Associate agrees to mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.
8. **Agreements by Third Parties.** Business Associate shall enter into an agreement with any subcontractor of Business Associate that creates, receives, maintains or transmits PHI on behalf of Covered Entity. Pursuant to such agreement, the subcontractor shall agree to be bound by the same restrictions, conditions, and requirements that apply to Business Associate under this Agreement with respect to such PHI.
9. **Access to PHI.** Within ten (10) business days of a request by Covered Entity for access to PHI about an individual contained in a Designated Record Set, Business Associate shall make available to Covered Entity such PHI for so long as such information is maintained by Business Associate in the Designated Record Set, as required by 45 CFR 164.524. In the event any individual delivers directly to Business Associate a request for access to PHI, Business Associate shall within ten (10) business days forward such request to Covered Entity.
10. **Amendment of PHI.** Within ten (10) business days of receipt of a request from Covered Entity for the amendment of an individual's PHI or a record regarding an individual contained in a Designated Record Set (for so long as the PHI is maintained in the Designated Record Set), Business Associate shall provide such information to Covered Entity for amendment and incorporate any such amendments in the PHI as required by 45 CFR 164.526. In the event any individual delivers directly to Business Associate a request for amendment to PHI, Business Associate shall within ten (10) business days forward such request to Covered Entity.
11. **Documentation of Disclosures.** Business Associate agrees to document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528 and HITECH.
12. **Accounting of Disclosures.** Within ten (10) business days of notice by Covered Entity to Business Associate that it has received a request for an accounting of disclosures of PHI, Business Associate shall make available to Covered Entity information to permit Covered Entity to respond to the request for an accounting of disclosures of PHI, as required by 45 CFR 164.528 and HITECH.
13. **Other Obligations.** To the extent that Business Associate is to carry out one or more of Covered Entity's obligations under the Privacy Rule, Business Associate shall comply with such requirements that apply to Covered Entity in the performance of such obligations.
14. **Covered Entity Obligations.** Covered Entity shall notify Business Associate of (a) any limitations in Covered Entity's notice of privacy practices under 45 CFR 164.520, to the extent that any such limitation may affect Business Associate's use or disclosure of PHI; (b) any changes in, or revocation of, the permission of an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI; and (c) any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be

permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity, except that Business Associate may, as set forth in Section 3 of this Agreement, use or disclose PHI for the management and administration and legal responsibilities of Business Associate.

- 15. Availability of Books and Records.** Business Associate hereby agrees to make its internal practices, books, and records available to the Secretary of the Department of Health and Human Services for purposes of determining Covered Entity's compliance with the HIPAA Rules.
- 16. Termination for Cause.** Business Associate authorizes termination of this Agreement and the Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of this Agreement and Business Associate has not cured the breach or ended the violation within the reasonable time specified by Covered Entity.
- 17. Effect of Termination.** Upon the termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall (a) retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities; (b) return to Covered Entity, or, if agreed to by Covered Entity, destroy, the remaining PHI that Business Associate still maintains in any form; (c) continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic PHI to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI; (d) not use or disclose the PHI retained by Business Associate other than for purposes for which such PHI was retained and subject to the same conditions set out in Section 3 which applied prior to termination; and (e) return to Covered Entity or, if agreed to by Covered Entity, destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities. This provision shall apply to PHI that is in the possession of Business Associate, subcontractors, and agents of Business Associate. Business Associate shall retain no copies of the PHI. Business Associate shall remain bound by the provisions of this Agreement, even after termination, until such time as all PHI has been returned or otherwise destroyed as provided in this Section.
- 18. Third Party Rights.** The terms of this Agreement do not grant any rights to any parties other than Business Associate and Covered Entity.
- 19. Independent Contractor Status.** For the purposes of this Agreement, Business Associate is an independent contractor of Covered Entity, and shall not be considered an agent of Covered Entity.
- 20. Changes in the Law.** The parties shall amend this Agreement to conform to any new or revised legislation, rules and regulations to which Covered Entity is subject now or in the future including, without limitation, HIPAA, HITECH, and the HIPAA Rules.

BUSINESS ASSOCIATE:

COVERED ENTITY:

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____