

MICHIGAN STATE UNIVERSITY

RFP# 916278 University Health and Wellness EHR

Addendum No. 1 Date: February 23, 2026

I. PURPOSE OF ADDENDUM

The purpose of this addendum is to formally expand the project scope to include Employee Assistance Program (EAP) operations within the proposed Electronic Health Record (EHR) solution. The University is interested in identifying suppliers capable of providing a unified platform that integrates traditional clinical services with specialized EAP management.

While EAP functionality is a desired component of the solution, the University remains interested in core EHR solutions that can demonstrate a path toward this integration.

II. ADMINISTRATIVE UPDATES

The following changes are hereby incorporated into the solicitation:

- RFP Due Date Extension: The proposal submission deadline is officially extended to **March 4, 2026, 3:00 pm Eastern**
- Document Update: The RFP document and RFP Excel Response sheet are updated to include the requirements listed below.



PROCUREMENT

Hannah Administration Bldg
426 Auditorium Rd Rm 360
East Lansing, MI
48824

517-355-0357
<http://upl.msu.edu/procurement>

Section: EHR Functional (added text is highlighted)

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”), **student records and employee records**, 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.
9. Describe the ability to use a campaign to provide outreach to the student **and/or employee** population. Example: Fall flu shots available, announcements via the portal, mailers, SMS, also availability to cancel a whole provider/department schedule via campaign

Section: EAP EHR Specifications

1. Provide examples of EAPs that your company has worked with in the past, and describe how the product has been able to support EAPs in workplaces that had multiple work units/departments, union environments, HR systems, confidentiality guarantees, etc.

2. Explain how to provide / guarantee confidentiality between EAP clients and other units that may also work with employees (e.g., Occupational Health, Nutrition) with regard to an employee who is seeking services in both areas. For example, would both areas be able to
3. Describe what demographic information is collected, with emphasis on information that is typically collected in an EAP setting that is not typically collected in a health care setting (e.g., unit/department, union, client type [staff, faculty, partner/spouse, etc.], presenting problems rather than diagnoses).
4. Describe a typical EAP individual counseling visit, and if there are any differences in how these are structured.
5. Describe how urgent or crisis cases are flagged.
6. Describe how organizational services (e.g. trainings, unit-based interventions, service overview, critical incident intervention) are recorded, and how attendance is measured and reported in utilization reporting.
7. (Similar to CAPS'. #7) Demonstrate how non-clinical and sub-clinical services (e.g., supervisor or employee consultations, crisis evaluations, last chance agreement sessions) are categorized, scheduled, and documented.
8. Demonstrate what validated measures can be incorporated into the chart, how these are displayed to the clinician, how they show up in utilization reporting, and if a pre- and post-test can be compared within the system. Also, if there are measures that we want to use that are not incorporated into your current system is there a method to build them in?
9. Does the product have a built-in telehealth/videoconferencing tool? If so, please demonstrate the client/patient experience with this.
10. AI Clinical Documentation (Optional/Desired): Does the platform offer integrated AI-assisted scribe or note-generation tools? If so, please describe how this functionality assists clinicians in drafting notes while maintaining data security.