Attachment A

To

RFP No. 4280

Mississippi Department of Mental Health

Electronic Health Records System

ITS Project No. 45588

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

Attachment A to RFP No. 4280
DMH Electronic Health Records - Technical Requirements

I. GENERAL

A. General Overview and Background

1. The Mississippi Department of Mental Health (DMH) is responsible for overseeing the State's six Mental Health facilities throughout Mississippi. These facilities include East Mississippi State Hospital (EMSH), North Mississippi State Hospital (NMSH), South Mississippi State Hospital (SMSH), Mississippi State Hospital (MSH), Central Mississippi Residential Center (CMRC), and Specialized Treatment Facility (STF).

2. The inadequate and sometimes manual processes offered by the incumbent EHR solution do not fully meet DMH patient health records, interoperability, and compliance reporting needs. Further, the incumbent solution fails to position DMH to become eligible for incentives related to the delivery of higher quality and more cost-efficient health care by providers. Examples are Merit-based Incentive Payment System (MIPS) and Advanced Alternative Payment Models (APMs).

3. The current electronic health records system resides at the ITS Datacenter located in Jackson, MS. It is a CRM platform with a SQL backend for storing data. DMH has SQL replication to a data warehouse that is used for reporting to comply with State and Federal requirements such as SAMHSA - Substance Abuse Mental Health Services Administration.

4. Among the six DMH facilities, there are 750 total active beds and 1,500 potential users of the incumbent electronic health records system.

5. DMH seeks to cure the known deficiencies of the incumbent solution, to automate manual processes, and to enhance current workflows.

6. Some are the known deficiencies of the incumbent solution are:

   a. The inability to meet meaningful use (MU) measures;
   b. Interoperability;
   c. The administration of patient medication;
   d. Interactions with labs and pharmacies; and
   e. The transfer of patients between facilities.

B. Solution Requirements Overview

7. Health information technology is bound to standards set by the Department of Health and Human Services – Public Welfare - CFR Title 45 (see link below). Vendor acknowledges and agrees to propose an electronic health record (EHR) solution that is compliant with all relevant EHR requirements referenced in CFR Title 45 in its most current form at the time of the response to this RFP/Attachment A.

   https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=572531b4d86d19d7ec5e6fafb3ca72e2&mc=true&n=pt45.2.170&r=PART&ty=HTML

8. The Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) have established standards and other criteria for structured data that EHRs must meet in order to qualify for use in Promoting Interoperability Programs (PIP). PIP incentives are provided to eligible facilities that demonstrate adoption, implementation, upgrading, or meaningful use of certified EHR technology (CEHRT). The State expects the proposed solution to be ONC certified to ensure the State's eligibility for any related CMS program incentives.

9. The State expects Vendors in the certified EHR marketplace who are proposing a solution to the State of Mississippi to be fully cognizant of all federal and state laws, compliance standards, and requirements applicable to health information technologies, specifically as they relate to certified EHR solutions. Vendor's base offering and all subsequent customizations and configurations must comply and remain in compliance with all such governing authorities.

10. The State expects best practice, industry standard tools and methodologies and will not accept proprietary formats.

11. If any of the requirements of this RFP/Attachment A conflict with or represent less stringent standards than the governing Federal and State requirements, Vendor will be bound to comply with the Federal and State requirements.

12. If any of the DMH requirements of this RFP/Attachment A are more stringent than the Federal or State requirements, Vendor will be bound to satisfy the DMH requirements, so long as there is no conflict with the governing authority.

13. The Institute of Medicine (IOM) has identified key capabilities and core functions that EHR systems should be capable of performing. The State considers these capabilities to be base offerings for an acceptable EHR system. They are described as:

    a. Storing clinical information and health data in an electronic format that can be retrieved and viewed efficiently;
    b. Providing results management such as the ability to manage test results;
    c. Providing order management such as the electronic processing of orders and prescriptions;
    d. Providing decision support such as risk warnings and information to assist in clinical decision making;
    e. Providing interoperability for electronic communications and connectivity across multiple care settings;
    f. Providing patient support such as facilitating patient information and communications with their provider(s);
    g. Providing administrative processes and practice management functionality such as billing and scheduling; and
    h. Providing robust management and compliance reporting to produce and share reports on clinical data concerning patient population health.

14. The State expects the proposed solution to provide essential functionality for the electronic management of patient data, patient care, decision support, results management, administrative processes, and reporting.

15. Because behavioral/mental health workflows are unique and often more challenging than those managed by traditional electronic health records solutions, the State is seeking a Vendor with expertise in the behavioral/mental health environment.

16. The State intends for all six of the DMH facilities to access and use the awarded EHR. Vendor must acknowledge and agree that specific functions and workflows will be enabled as needed.

17. The State expects the proposed solution to deliver interoperability with any and all third-party systems and processes as required by the State. The Vendor must acknowledge that the State expects interoperability in every form required by the Federal Government, the

State of Mississippi, or DMH, including, but not limited to, reporting Mental Health and Substance Use at no additional cost to the State.

18. The State expects the comprehensive solution proposed by the Vendor to address the functional and technical requirements set forth in this RFP/Attachment A including all applicable compliance standards.

C. Vendor Qualifications

19. Vendor must be capable of and have previous experience in the development, implementation, and support of EHR solutions of similar size and scope. At least two of the vendor references submitted in Section IX of RFP No. 4280 must substantiate this experience.

20. Vendor must have been in the business of providing such solutions for at least the last three years.

21. Vendor must provide an introduction and general description of its company's background and years in business providing vendor hosted, EHR applications.

22. Vendor must specify the location of the organization's principal office and the number of executive and professional personnel employed at this office.

23. Vendor must specify the organization's size in terms of the number of full-time employees, the number of contract personnel used at any one time, the number of offices and their locations, and structure (for example, state, national, or international organization).

24. Vendor must disclose any company restructurings, mergers, and acquisitions over the past three (3) years and/or any planned, future restructures or mergers.

25. Vendor headquarters must be located in the United States and must provide U.S. based customer support.

D. Vendor Implementation Team

26. Vendor must demonstrate that all team members have the necessary experience for design, installation, implementation, training, and support of the services required by this RFP. At a minimum, Vendor response should include team member roles, functional responsibilities, and experience with projects similar in size and scope to the services required by this RFP/Attachment A.

27. Identify the participating key staff members who will be responsible for the execution of the various aspects of the project, including but not limited to: Project Manager, Development Team, Business Analyst(s) and Technical Architect(s).

28. For each participating key staff member, provide a summary of qualifications, years of experience and length of employment with your company.

29. Vendor must ensure that each team member assigned to this project has the ability to communicate clearly in the English language both verbally and in written form.

E. Compliance Standards

30. **Mandatory**: So that DMH will be able to meet ONC PIP standards, the proposed solution must be ONC certified. To that end, proposed developer and solution must be found on the below website which reflects the certification status of developers, products, and versions. Only ONC certified developers and products will be considered eligible for consideration by DMH.

https://chpl.healthit.gov/#/collections/api-documentation

31. Vendor must agree that all EHR data will be subject to all data privacy laws including but not limited to HIPAA.

32. Solution must be HL7 compatible. HL7 helps bridge the gap between health IT applications and makes sharing healthcare data easier and more efficient.

33. All DMH facilities must comply with the Mississippi Department of Health requirements regarding the electronic submission of public health data. See below:

    https://msdh.ms.gov/msdhsite/_static/14,0,356.html

34. All DMH hospital facilities must comply with the Minimum Standards of Operation for Mississippi Hospitals. See below:

    https://msdh.ms.gov/msdhsite/_static/resources/7419.pdf

35. Solution must comply with all Federal Clinical Document Architecture (CDA) requirements and guidelines in effect at the time of the response to this RFP/Attachment A.

F. RFP 4280 Compliance Documents

36. Reference documents and required standards cited by this RFP/Attachment A will be considered compliance documents.

    a. If Federal or State compliance documents or standards are updated during the scope of this implementation, the Vendor must agree to recognize and comply with the updated documents or standards.

37. If Vendor proposes changes to compliance documents during the scope of this implementation, Vendor agrees to:

    a. Identify existing material needs to be replaced or updated;
    b. Identify the proposed new material and/or associated data items;
    c. Provide a rationale for using the new items including cost, schedule, performance and supportability impact; and
    d. Obtain State approval.

II. Functional/Technical Requirements

A. Hosting Environment

38. DMH is seeking a Vendor hosted solution. At start-up, the hosted environment must be capable of supporting the EHR application at maximum user capacity (currently 1,500 users) as well as the system's database functions.

39. The solution must be scalable to accommodate growing numbers of patients and users at no additional cost to DMH.

40. For a Vendor hosted solution, Vendor must meet the following minimum requirements.

    a. Vendor must provide Managed Services, including migration of any on-premise services as detailed in this RFP.
    b. The proposed solution must be Vendor-hosted in an environment that adheres to the Enterprise Security Policy.
    c. Vendor must provide professional services such as monitoring, help desk support, security, etc.

B. Web Access – Authorized Users

41. Vendor must propose a secure, encrypted, web-enabled application that does not require server configuration on end-user devices.
42. The proposed solution must offer a secure, web-accessible portal to grant access to credentialed users for DMH defined functions. The web-accessible portal for the solution must be intuitive and easy to navigate.
43. Solution must be browser neutral -- and must be compatible with the current version and two preceding versions of common browsers including Chrome, Microsoft Edge, Firefox, Safari, and Microsoft Explorer 11. Vendor must provide a current list of supported browsers and describe their process for certifying their proposed solution on specific browsers.
44. Solution must be accessible to all end user equipment types such as desktops, laptops, tablets, and all other devices.
45. Vendor must specify any downloads, plug-ins, or additional software (add-ons) (e.g. Java, Flash, etc.) required to access the proposed solution.
46. For any necessary downloads, plug-ins or add-ons, instructions for access and installation must be easily accessible to participants as a part of the proposed solution. Vendor must describe how the additional software is presented to the user and detail the process for download and installation of the software. Vendor should include a sample screen shot or sample instructions with Vendor's response to this requirement.
47. For any necessary downloads, plug-ins or add-ons, Vendor must describe the process for educating users on installation and maintenance, including new users as they are added.
48. Any costs associated with the use and maintenance of these downloads, plug-ins or additional software must be included in RFP No. 4280, Section VIII Cost Information Submission.

C. Mobile Access

49. Solution must be accessible to IOS and Android mobile devices. Vendors must provide detailed information that describes their process for maintaining/testing the solution on newer IOS and Android OS versions.
50. Solution must be compatible with Microsoft tablet, Android tablet, IOS, and related devices for the current and two immediately preceding versions.
51. Solution must incorporate mobile viewing for credentialed users.
52. Solution must accommodate system management functions on mobile platforms.
53. Solution must provide real-time data exchange with all field devices having adequate access.

D. Behavioral Health Workflows

54. Solution must accommodate configurable workflows and business rules that are common to best practice behavioral/mental health EHR solutions.
55. Vendor will be responsible for the configuration and maintenance of workflows and business rules to accommodate DMH's business processes.
56. Solution business rules and workflows must allow multiple, related triggers as defined by DMH.

57. Solution must provide configurable triggers that will initiate events and/or data driven workflow actions that will result in automatic updates.
58. Solution must allow authorized users to redirect workflows in response to circumstances that require temporary or permanent changes.
59. Workflow routing must accommodate, track, and report on due dates as defined by DMH.
60. Solution must distribute EHR tasks to relevant parties simultaneously.
61. Solution must display workflows in simple, graphic formats which are easily understood by system users.
62. Workflow graphics must indicate the current status of a work item in the workflow.
63. Solution must allow workflows to be saved as templates to be reused for other types of EHR actions.
64. Solution must provide the ability to create and modify workflows using built-in administrative tools.
65. Workflows must be capable of routing EHR functional responsibilities to specific staff member work queues.
66. Workflows must be configurable with drag-and-drop tools through a graphic user interface.
67. Authorized DMH staff must be able to reassign and/or override workflow tasks as necessary to manage workloads, staffing, and processes.
68. Solution must offer pre-configured workflows for processes common to EHR solutions of similar size and scope.
69. Solution must provide automated workflows that advance without manual intervention.

E. General Functionality

70. For all requirements, base solution must offer functionalities common to best practice EHR solutions.
71. Solution must offer best practice data entry functionality whether or not it is specified by this RFP/Attachment A.
72. Solution must comply with all functions and requirements related to Electronic Medication Administration Record (MAR).
73. Once entered into system, data must populate all relevant modules in the Vendor's solution, as well as any applicable third-party applications in use, such as (but not limited to) LabCorp, and QS1.
74. Solution must able to hide certain fields, such as SSN, as determined by DMH.
75. Solution must be able to capture multiple client IDs for the purpose of following patient history from multiple providers.
76. Solution must have controls in place to prevent the creation of duplicate records for existing patient identities.
77. Solution must provide common word processing capabilities, including spell-check, in text fields as well as drop down menus where appropriate.
78. Solution must have the ability to print customized patient labels for mailings, encounters, labs, etc.

79. The solution must be able to run a daily census to report the number of occupied beds and vacated beds in the State DMH facilities.
80. Solution must accommodate and manage waitlists for vacant beds common in EHR solutions of similar scope and size.
81. Solution must provide HIPAA compliant FAX send and receive functionalities.
82. Solution must provide HIPAA compliant internal/external email capabilities that meet or exceed the ITS cloud hosting security requirements specified by this RFP/Attachment A.
83. Solution must issue alerts as determined by DMH when faxes are received and scanned into EHR.
84. Solution must allow authorized users to customize layouts and views based on user preferences.
85. Solution must accommodate subprogram codes to separate statistical and financial data.
86. Solution must allow authorized users to re-open closed records to correct coding errors, edit content, etc.
87. Solution must allow authorized users to create customized internal procedure codes with or without associated fees.
88. Solution must be able to generate patient specific problem lists in accordance with best practice behavioral/mental health standard definitions, and/or as determined by DMH. For each problem, authorized users must be able to create, review, or amend information regarding a problem or problem status change.
89. Authorized users must be able to view and print patient information as determined by DMH. Examples include demographic information, patient appointments, problem lists, etc.
90. Authorized users must be able to generate letters, referrals, and updates, etc. to providers.
91. Solution must allow authorized users (MDs, Providers, Nurses, etc.) to sign off on chart/results.
92. Whenever a patient window is open, solution must display the patient's current vital signs as specified by DMH and must maintain a cumulative table or graph that reflects ongoing patient history.
93. Authorized users must be able to enter the patient's allergies, weight, blood pressure, pulse, O2 stats, height, etc. The solution must calculate BMI and populate it into other forms as determined by DMH.
94. Solution must issue an alert when elevated blood pressure readings are entered. Solution must prompt for a second, manual reading.
95. Upon opening, patient charts must alert and reveal any activity that has taken place since the last time the chart was closed.
96. Solution must allow simultaneous user viewing and/or editing of a patient's individual record.
97. Authorized users must be able to view and sort vital patient information for all patient encounters.
98. Solution must populate standard orders that authorized users can customize to meet individual needs.

99. Solution must maintain up-to-date diagnoses using DSM 5/ICD10 coding. Further, solution must maintain logs of both current and prior diagnoses that are updateable as necessary. The solution must store multiple diagnoses.
100. Upon re-admission, patient's prior progress notes must be accessible to authorized users.
101. Solution must maintain patient immunization records, including any adverse effects.
102. Solution must be capable of collecting and uploading patient immunization histories to the Mississippi State Department of Health and/or other immunization registries. Immunization histories must be viewable and printable by authorized users.
103. Solution must be able to interface with a camera for patient ID pictures and must allow patient pictures to be attached to their records and printed as needed.
104. Authorized users must be able to attach multiple pictures to patient records to document wounds, scars, etc.
105. Authorized users must be able to view client caseload assignments.
106. For Medical Nutrition Therapy, the dietary recall sheet must be viewable and printable.
107. Solution must be able to document the patient's orders including prescriptions, dispensing of medications, recommendations for follow-up, or referrals for other services.
108. Solution must ensure that all patient information from any source or any service is maintained and/or transmitted in compliance with HIPAA requirements.
109. Solution must provide context sensitive help, error messaging and instructions for users throughout the EHR process from origination to archival.
110. Solution must support typical Microsoft Office functions such as cut, copy, paste, and spell/grammar check, etc.
111. Solution must include flexible output formats such as .pdf, .xls, or any other common format used by the DMH.
112. Proposed solution must provide familiar keyboard shortcuts such as those common to Microsoft Windows applications.
113. Solution must allow the viewing of multiple screens simultaneously, along with the ability to minimize and resize windows as needed.
114. Solution must be customizable for data elements as required by DMH. The base DMH data elements required at implementation of the awarded solution are represented by but not limited to the elements listed in Appendix 1 of this document.
115. Data elements must be accessible through dropdown menus, checkboxes, and data pickers, etc. to ensure standardization of DMH processes and data collection formats.
116. Solution must be capable of interfacing with appropriate devices to apply, manage, and verify digital signatures of practitioners, patients, and users for all forms, actions, and services targeted by DMH.
117. Solution must provide data import and export capabilities.
118. Solution must provide a User Interface (UI) to build and manage templates.
119. Solution must allow authorized users to configure and maintain templates and components.

120. Task logs must reveal daily assigned tasks, task details, task due dates, task status, and all other details pertinent to task management.
121. Solution must prevent users from permanently deleting records.
122. Authorized DMH staff must be able to change a record status to inactive.
123. The solution must be compatible with current Microsoft products available through the DMH enterprise agreement. These include, but are not limited to Microsoft Office 365, SharePoint, Azure, etc.

F. Administrative Management

124. Base solution must offer administrative management features and functionality common to all best practice EHR solutions, whether or not they are specified by this RFP/Attachment A.
125. The proposed solution must provide configurable, role-based, administrative tools and controls.
126. Solution must assign a unique name and/or number for identifying and tracking user identity.
127. Solution must allow authorized users to set security and permissions by user or user group, including customized access permissions.
128. Solution must be highly configurable and at a minimum, allow authorized users to generate, modify, and delete user accounts.
129. Solution must be highly configurable and at a minimum, allow authorized users to configure business rules, data elements, screens, workflows, triggers, navigation, and dashboards.
130. The proposed solution must accommodate the need for DMH staff and system administrators to perform necessary administrative functions, including but not limited to creating and maintaining user accounts, backing up and restoring files, exporting files, and generating reports, etc.
131. DMH administrators must be able to use input workflows to test new and modified types of transactions (TOTs). The TOTs can be any of those ingested by or created as output by any other workflow.

G. Document Capture, Imaging, and Managing

132. Base solution must offer document management features and functionality common to best practice EHR solutions, whether or not they are specified by this RFP/Attachment A.
133. Solution must offer a full featured document management system (DMS) that accommodates generating, scanning, indexing, manipulating, editing, and storing paper and electronic documents.
134. In addition to scanning on demand, proposed solution must provide the functionality to import/ingest bulk scanning of paper documents.
135. Proposed document manager must provide a robust, organized, and user-friendly document storage and retrieval structure.
136. Proposed document manager must accept and upload large gigabyte documents, including but not limited to All Microsoft Office formats, .pdf, and all photo formats including JPEG, TIFF, GIF, and PNG.

137. Proposed document manager must be able to import and print multiple formats. Examples are .CSV, HL7, DICOM, CDA, 835, 837, and 999.
138. Proposed document manager must accommodate printing and/or exporting maintained and managed documents, including but not limited to multiple documents in a single batch job.
139. Proposed document manager must be able print to standard printers as well as zebra/thermal printers for printing labels.
140. Proposed document manager must be able to format and print arm bands.
141. Proposed document manager must be able to generate letters (missed appointment, immunizations, services eligibility) in the patient's preferred language which, at a minimum, includes English and Spanish.
142. Proposed document manager must be able to provide/print patient education material in patient's preferred language.
143. Each document that prints from the proposed document manager must include the patient's unique identifier and any other information as determined by DMH.
144. Proposed document manager must allow mobile users to upload and attach documents to targeted EHR records.
145. Proposed document manager must allow permission-based review and editing of documents in the document manager.
146. Proposed document manager must offer and manage document collaboration among authorized users.
147. Proposed document manager must accept the import of migrated documents and other digital assets presently used by DMH. Common DMH process document formats include: All Microsoft Office formats, .pdf, and all photo formats including JPEG, TIFF, GIF, and PNG.
148. Proposed document manager must accommodate all methods by which a user/practitioner could import data, including but not limited to: CD/DVD, Flash Drive, .pdf, paper.
149. Proposed document manager solution must allow authorized users to design and implement workflow-aware document templates.
150. Proposed document manager must include standard email templates, correspondence templates and the ability to produce mailing labels based on user defined criteria.
151. Proposed document manager must provide a User Interface (UI) to build and manage templates.
152. Proposed document manager must allow authorized users to configure and maintain templates and components.
153. Proposed document manager must allow authorized users to remove documents from patient records if attached in error and must keep an audit trail of such actions.
154. Proposed document manager must allow DMH to send customer service surveys via email.
155. Based on workflow and EHR criteria determined by the DMH, proposed document manager must provide automatic document routing to appropriate work queues for users and/or automatic response.

156. Proposed document manager must offer common features as described below:
    a. Customizable document types;
    b. Customizable flags and meta-data for document types;
    c. Attach multiple file types to patient history, including proprietary file types;
    d. Viewer for all allowed document file types;
    e. Documents can be searched by file name and metadata;
    f. Documents can be searched by content;
    g. Documents can be searched within a patient record and across patient records;
    h. Documents can be attached to patient records and linked to patient events;
    i. User-initiated and system-initiated OCR of pdfs;
    j. Notification can be sent to users when a new document is attached to a patient file;
    k. Customizable document retention policies based on document type;
    l. Customizable document organization and display, using folders, tags, column sort, and views, etc.;
    m. Documents can be scanned directly into EHR and OCR'd;
    n. Generated documents can be distributed to multiple people (internal and external), and system captures/displays to whom the document was sent;
    o. Documents can be redacted, and both the original and redacted versions are saved;
    p. Document title/file name can be modified;
    q. Documents can have "draft" status, and drafts can be modified;
    r. Documents can have "final" status, and cannot be further modified;
    s. Queue for documents waiting for signature;
    t. Multiple documents can be attached/copied/printed with a single action, including by drag-and-drop;
    u. Users can bookmark documents;
    v. Documents can be annotated or marked-up within the DMH processes;
    w. Documents can be attached directly from email;
    x. Documents from a batch letter generation can be saved to the applicable patient files; and
    y. Approval workflow available for generated documents.

H. Reports and Dashboards

157. Solution must offer pre-designed, standard reports and dashboard features and functionalities common to all best practice EHR solutions, whether or not they are specified by this RFP/Attachment A.

158. Solution must accommodate the creation and modification of standard reporting templates as defined by DMH.

159. Solution must accommodate user defined reporting for the purpose of creating custom reports from any and all data elements for which DMH requires tracking and/or reporting. Examples include monthly reports by type of service, acute illness, number of new patients registered, outside referrals, ER visits, number of clinic visits, missed appointments, and others as required by DMH.

160. Solution must allow authorized DMH staff to create their own reports using an interface that does not require specialized knowledge of a third-party tool such as Crystal Reports.
161. User defined reporting tool must be intuitive and easy for the user to comprehend.
162. Solution must provide the ability to save user-generated reports and queries under user profiles.
163. Solution must provide the ability to store report specifications in a central report repository (save ad hoc reporting parameters).
164. Solution must be capable of exporting reports into file formats including but not limited to PDF, MS Excel, and MS Word.
165. Solution must be able to distribute reports through the workflow as HIPAA secure email attachments.
166. Solution must automatically generate reports on a configurable schedule and distribute them to selected users.
167. Authorized users must be able to run on-demand reports as necessary.
168. Authorized users must be able to run QA reports (random selection of files and criteria/program specific).
169. Authorized users must be able to control page formatting features and must be able to include header information, date and run time, and page numbers on reports.
170. Solution must offer print preview functionality.
171. Authorized users must be able to send outputs to user-selected printers.
172. Solution must log and track all exported/printed data.
173. The solution must provide ad hoc reports of all users with system access, including level of access and the date/time of last access.
174. Solution must provide dashboard views that provide system users with pertinent information related to their workloads and patient cases to assist them in visualizing and prioritizing work.
175. Solution must provide configurable dashboards for users to manage open tasks.
176. Solution must provide dashboards that can be configured according to roles and preferences of individual users.
177. Solution must provide dashboard functionality at multiple user levels to represent multiple factors as determined by MDH. Examples are patient arrival time, facility location, and number assigned to patient, etc.
178. Solution must provide configurable dashboards on throughput performance measures and system activities.

I. Notifications and Alerts

179. Solution must auto-generate emails or notifications based on conditions and thresholds set by DMH.
180. Solution must provide email and/or correspondence templates for notification purposes.
181. The solution must provide user customizable alert screens to capture message details.

182. Authorized users must be able to forward alerts to specific providers or other authorized users via secure email or other secure electronic communications.

183. Solution must provide task management functions that will issue alerts for pending, due, or past due tasks. This function should interface with the dashboard function to give users a visual representation of the status of their tasks.

184. Solution must accommodate customized patient alerts such as fall risk, drug allergies, etc.

185. Solution must be able to issue medication interaction alerts and warnings.

J. Search Function

186. Solution must offer full featured, configurable data search functions that can be scheduled to run automatically and/or upon demand from authorized users.

187. Solution must allow users to search by any indexable attribute required by DMH.

188. Solution must be able to search on all data elements and have full key word search capability.

189. Solution must be able to produce search results that represent the search term, as well as subtle variations of the search term.

190. Solution must offer pre-defined searches that would be common to EHR behavioral/mental health management activities.

191. Search results must be exportable or downloadable to common file formats such as Excel, .pdf, xml, and csv.

192. Users must be able to save frequently used searches for repeated use.

193. Users must be able to search by groupings or related matters such as outcomes, settlements, and dispositions, etc.

194. Users must be able to search for items opened or closed during specific time frames.

195. Users must be able to search for upcoming events, deadlines, or other quantifiable parameters as determined by DMH.

196. Solution must provide global search functionality. At a minimum, this function should allow a user to search for any data or combination of data in the system. The results should be presented in a prioritized structure determined by the relevance to the search criteria. All connected or relatable data based on the search criteria should be presented within the prioritized results.

197. Authorized users must be able to search for medications by NDC#'s or by description.

K. Calendar Function

198. Solution must allow users to schedule meetings, doctor visits, and other relatable events connected to DMH staff's activities. At a minimum, solution must offer calendar functions as described below:

    a. Can generate calendars based on DMH specified activities. Calendar event can be sent to Outlook calendars. If event is updated, Outlook event is automatically updated;
    b. Accommodates configurable meeting notification and event fields display;
    c. Calendars can be shared with participating entities, as determined by DMH;
    d. Calendars are exportable;

e. Events can be displayed in calendar style; and
f. Users can subscribe to calendar events.

L. Audit Function

199. Base solution must offer common audit trail functions inherent to best practice EHR management solutions and must at a minimum, include:
    a. Ability to audit based on activity type (view, modify);
    b. Ability to set audit requirements based on data type or service type;
    c. Ability to set audit retention schedule based on data type or service type;
    d. Ability to audit user activity including but not limited to logins, logouts, views, and changes within a record;
    e. Ability to restrict access to auditing data;
    f. UI for query/search and reporting of audit data; and
    g. Ability for users to customize audit reports.
200. For tracking and audit purposes, solution must assign unique identifiers to all users.
201. The solution must timestamp all actions taken by users and reflect the activity in the audit trail.
202. The solution must maintain an audit trail of data changes including but not limited to previous and new values, change dates, and the identity of the person making the change.
203. Audit trails must be accessible in real time by authorized DMH staff.
204. The proposed solution must also be able to produce an audit trail of the historical security access changes for each user.
205. Solution must provide an audit trail for all patient encounter functions including but not limited to the identity of the person who entered the encounter and the date it was entered.

M. Record Retention/Archival

206. It is the policy of the Mississippi Department of Mental Health that all patient medical records be perpetually retained unless otherwise directed by DMH.
207. The proposed solution must maintain and archive all DMH patient records in compliance with DMH and HIPAA requirements, as well as any other applicable Federal and State retention and archival requirements.

N. Optional Functions

208. Patient Portal: DMH may in the future require a secure patient portal to accommodate approximately 10,000 users per year. If available, but not included in base offering, Vendor must include pricing for a secure patient portal, as well as any hosting and support fees, as separate *Optional Function* line item(s) in RFP No. 4280, Section VIII Cost Information Submission.
209. Speech to Text Capability: DMH may in the future want to consider speech to text functionality. If available, but not included in base offering, Vendor must present pricing for speech to text functionality as a separate *Optional Function* line item in RFP No. 4280, Section VIII Cost Information Submission.

III. Patient Care

A. Patient Intake

210. The solution must accommodate all present intake procedures being administered by the incumbent solution. Present intake procedures are considered to be common to behavioral health entities of similar size and scope. Vendor must agree to work with DMH to improve and expand current procedures as necessary, including the automation of any manual procedures. Any process improvement plans recommended by the Vendor must be pre-approved by DMH prior to implementation.

211. The solution must accommodate data entry and update of multiple patient information fields, as determined by DMH. Examples are: first, middle, and last names, maiden name, alias, mother's maiden name, date of birth, sex, social security number, race, and preferred language.

212. The solution must accommodate DMH screening requirements which govern the process after intake information has been gathered. Screening processes aid in uniform decision-making and making appropriate referrals.

213. The solution must be able to import patient health history data from the existing DMH EHR system.

214. The solution must present a chronological, filterable, and comprehensive view of patient's EHR, which may be summarized and printed subject to privacy and confidentiality requirements.

215. Solution must be able to note if a pregnancy test was negative or positive and populate the results to the problem list.

216. Solution must include a required field for citizenship status.

B. Patient Eligibility

217. Solution must be configurable to capture financial assessment information as determined by DMH.

218. Solution must be able to capture whether a person is a Mississippi resident, whether they are Medicaid eligible, and whether they have other insurance provider(s).

219. Solution must be able to capture, produce, and print eligibility information onto a customized electronic socioeconomic form that can accept dated e-signatures.

C. Consent Tracking and Patient Forms

220. Solution must accommodate and track notice of legal rights and services.

221. Solution must accommodate and track statements of authority for those authorized for guardianship and those legally authorized to provide consent.

222. Solution must accommodate and track consents to use/release records, including date of the request and date of release.

223. Solution must allow authorized users to customize additional consents.

224. Solution must issue alerts for missing consents.

225. Solution must require safeguards to prevent the release of data without proper authorization.

226. Authorized users must be able to create and edit customized patient forms, templates, and letters.

D. Screening and Service Requests

227. Solution must maintain data provided by referral sources.
228. Solution must accept electronically submitted data from external referral sources.
229. Solution must be able to transfer a patient's chart to a different provider or facility.
230. Solution must be able to make/receive internal referrals to/from programs, and notification that the referrals were received.
231. Solution must maintain data pertaining to medical history and past significant medical needs.
232. Solution must maintain medical/physical exam findings, current health status, medical needs, and monitoring.

E. Scheduling

233. Solution must be able to schedule appointments based on requested date/time.
234. Solution must be able to schedule appointments by type of behavioral/mental health service.
235. Authorized users must be able to view and print daily schedules.

F. Patient Encounter

236. Authorized users must be able to add and view *notes* to the encounter recording screen.
237. Authorized users must be able to flag incorrect coding and encounter notes and transmit to provider for correction. Authorized users must be able to reject and request resubmission to provider for further correction.
238. Solution must provide the full range of DMH data elements collected at the time of patient encounters. See Appendix A for representative data elements.
239. Solution must display full charges and sliding fee charges for patients.
240. Solution must be able to accept dental billing service codes.
241. Authorized users must be able to document all encounters on progress notes, whether or not they are billable.
242. Solution must provide ability to capture and print assessments, progress notes, treatment plans, and discharge paperwork to Courts.

G. Patient Discharge

243. Solution must accommodate the discharge of patients to external facilities.
244. Solution must automatically create the encounter and populate patient discharge information, CPT codes completed by providers, and diagnosis codes.
245. Solution must accept program and subprogram codes on discharge encounters.
246. Solution must allow notes to be entered on the encounter recording screen.
247. Upon discharge, authorized users must be able to enter service specific codes and descriptions for services rendered to patient.
248. Solution must be able to document patient discharge date and time.

IV. Service Specific Requirements

A. Communicable Disease

249. Vendor agrees to maintain EHR functional compliance with any future changes in Federal and/or State requirements related to communicable disease at no additional cost to DMH.
250. Solution must be able to receive reportable disease and condition reports electronically from hospitals and providers.
251. Solution must be able to transmit reportable disease and condition reports electronically to Mississippi State Department of Health.
252. Solution must be able to generate reports on reportable conditions.
253. Solution must be able to create monthly reports to include disease cases for reportable and non-reportable conditions.
254. Solution must accommodate assessments and questionnaires to guide authorized users through established communicable disease protocols.

B. Pharmacy

255. By tracking the unique identifier assigned to each user, the solution must maintain an audit trail of all pharmacy activities. Authorized users must be able to view pharmacy audit trails.
256. Solution must maintain up-to-date patient prescription profiles that include drug names, strengths, dose forms, quantities/dates dispensed, directions for use, number of refills, prescriber, dispenser, and indications.
257. Solution must account for all items and quantities necessary to satisfy DMH EHR inventory reporting requirements. Examples are date, item description, item NDC#, package size, quantity on hand, unit price, extended price.
258. Solution must be able to generate labels for in house drugs.
259. Solution must be able to electronically send prescriptions to outside pharmacies.
260. Solution must be able to generate labels for client prescriptions in both English and Spanish.
261. Solution must be able to print all prescriptions.
262. Solution must be able to print drug pamphlets for clients in English and Spanish.
263. Solution must be able to select from list a list of providers.
264. Solution must be able to generate audit reports on all prescription related activities.

C. Lab

265. By tracking the unique identifier assigned to each user, the solution must maintain an audit trail of all lab related activities. Authorized users must be able to view lab audit trails.
266. Solution must be able to order and receive labs results electronically.
267. Solution must be able to electronically record, submit, retrieve, and report clinical lab results, including all fields necessary to identify the testing lab.
268. Solution must provide fields to enter lab results that show units, normal ranges, and the name of the testing facility.
269. Solution must be able alert labs of pending orders.
270. Solution must be able to notify appropriate staff when lab results are ready for review.

271. Solution must be able to alert for certain elevated lab results and required responses, such as the need to alert the Lead Nurse.
272. Authorized staff must be able to amend, correct, hide, or deactivate lab orders. Authorized staff are those who have received signed permission from the provider.
273. Solution must be able to manage reflex and confirmation testing when applicable.
274. Solution must be able to interface with lab information systems such as Lab Corp.
275. Solution must be able to generate patient labels at the time lab tests are ordered.
276. Solution must be able to create a test profile list to simplify order entry.
277. Solution must be able to check orders not completed by a certain date.
278. Solution must be able to create a worklist for reference labs.
279. Solution must be able to acknowledge that a sample was received and added to the worklist.
280. Solution must be able to access lab samples and place them on the correct worklist with the date and time collected.
281. Solution must be able to order batch and stat tests.
282. Solution must be able to list pending and completed tests for each patient.
283. Solution must be able to print cumulative lab results over a specified date range.
284. Solution must be able to track daily quality control for test procedures.
285. Solution must be able to interface with instruments to capture quality control data and data ranges inputted by control lot number. Vendors must describe how they have successfully interfaced with multiple instruments.
286. Solution must be able to generate Levy-Jennings charts using lab data.
287. Solution must be able to show Mean values and Standard Deviation (SD) for each index prepared at the end of each lot number of control.
288. Solution must be able view and print current Mean and SD values.

D. Radiology

289. Base solution must be able to accommodate access to a third-party radiology system, via a hyperlink to NovaRad software which much be updatable by DMH system administrators.

V. Financial Management

A. Billing

290. By tracking the unique identifier assigned to each user, the solution must maintain an audit trail of all billing activities. Authorized users must be able to view billing audit trails.
291. Authorized users must be able to assign programs to the appropriate sliding fee scale.
292. Authorized users must be able to view patient Sliding Fee Scale (SFS) percentage by program.
293. Authorized users must be able to add/update fees and SFS with beginning and ending dates.

294. To eliminate redundant data entry, solution must be able to link existing clinical information to the billing functions.
295. Solution must be able to establish a patient account status or code to reflect payment status.
296. Solution must be able to integrate third-party coding programs and update codes in the future.
297. Solution must be able to accommodate typical mental/behavioral health financial transactions such as patient specific information, services provided, co-pays, adjustments, methods of payment, amount of payment, net balance, and private statements for clients.
298. Solution must allow billing of third-party payers with payer's name, policy number, group number, expiration date, etc.
299. Solution must generate reports of funding generated, source of payment per service, claim number, payer name, date of service, status of claim (paid/not paid), etc.
300. Solution must be able to detail transactions in chronological order by date, including the date of service, posting date, transaction type, line item description, dollar amount, etc.
301. Solution must offer best practice, industry standard revenue analysis summaries for specified data ranges and service lines, including total fees charged, total adjustments, total revenue generated, etc.
302. Solution must offer best practice, industry standard revenue trend analysis reports including average charge per visit, average revenue per visit, and other elements as determined by DMH.
303. Solution must offer the ability to print invoices with Company Name and Address with patient information, services (service code and description), and total charges for company.
304. Solution must be able to print standard CMS federal forms for patient data.
305. Solution must be configurable to issue patient statements as determined by DMH. For example, statement may be scheduled to issue every 30, 60, 90 days and then stop. When a payment is made or a new service is added, statements may begin again for 30, 60, or 90 days.
306. Solution must be able to send a weekly billing report to the billing staff as determined by DMH.

B. Claims

307. By tracking the unique identifier assigned to each user, the solution must maintain an audit trail of all claims related activities. Authorized users must be able to view claims audit trails.
308. Solution must allow claims to be submitted electronically and by paper.
309. Solution must be able to create batch files based on guarantor group or individual guarantors.
310. Solution must be able to create batch files based on program and subprograms.
311. Solution must be able to distinguish between the original billing and re-billing of claims and to process them accordingly.

312. Solution must be able to electronically submit standard 837P Professional Medicaid/Health Choice claims and Federal 837D Dental Medicaid/Health Choice to Medicaid and State Reporting. Please refer to DHM website, http://www.dmh.ms.gov/wits-documentation/.

313. Solution must be able to electronically submit and print standard federal claim forms for Medicaid and Medicare billing.

314. Solution must be able to download remittance advice documents.

C. Payments

315. By tracking the unique identifier assigned to each user, the solution must maintain an audit trail of all payment posting activities. Authorized users must be able to view posting activity audit trails.

316. Solution must offer configurable payment screens for the purpose of capturing and posting multiple payment types.

317. Payment screens must display programs and subprograms for services.

318. Authorized users must be able to post payments, adjustments, transfers and corrections to payments, adjustments and transfers.

319. Payment screens must be configurable to accommodate payments made by cash, credit/debit, Medicaid or other EFT, etc.

320. Solution must interface with credit/debit card swipe machines to automatically post payments.

321. Solution must be able to post payments and adjustments by standard 835 Federal electronic files for Medicaid/Medicare insurances.

D. Deposits

322. By tracking the unique identifier assigned to each user, the Solution must maintain an audit trail of all deposit activities. Authorized users must be able to view posting audit trails.

323. Deposit reports must be customizable to display the name of the person who entered the payment, the program and subprogram codes, service codes, description, etc.

324. Deposit reports must be customizable to list the patient name, patient unique client number, posting code and description, amount received and posted, etc.

325. Solution must accommodate electronic deposits and manually entered paper-based deposits.

326. Solution must provide summary deposit information as required by DMH. For instance, all deposits made for a specific date, including appropriate deposit descriptions as determined by DMH.

VI. System Design

A. Data Management

327. Vendor shall not store or transfer State data outside of the United States. This includes backup data and disaster recovery locations.

328. Vendor agrees that the State shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Vendor shall not access State user accounts or State Data, except in the course of data center operations related

to this solution, in response to service or technical issues as required by the express terms of this service, or at the State's written request.

329. Vendor agrees to maintain and archive State data in non-proprietary formats to facilitate any future transition from the hosted solution to another solution.

B. Service Availability and Restoration

330. For the initial term and any extended terms of service, the Vendor must maintain accessibility of the solution twenty-four (24) hours a day, seven (7) days a week, three hundred sixty five (365/366) days a year, excluding regularly scheduled maintenance and unavailability due to a catastrophic event, at an uptime rate of at least 99.98 percent , to be measured monthly.

331. Vendor agrees to include as unavailable time:

    a. Any unscheduled maintenance or repairs; and
    b. Planned upgrades where DMH users do not have access to and the use of EHR services.

332. For purposes of this requirement, "catastrophic event" is defined as a natural or man-made disaster that destroys both the primary and the disaster recovery sites or renders both unusable due to fire, water damage, earthquake, radioactive leak, large-scale power outage, declared medical pandemic, or a large-scale communications infrastructure outage (telephones and Internet access). Large-scale means at least affecting the city where the site is located.

C. Continuity of Operations Plan/Disaster Recovery

333. Vendor shall provide an alternate business site if Vendor's primary business site becomes unsafe or inoperable. The alternate business site shall be fully operational 24/7/365.

334. The requirements of this RFP 4280/Attachment A express the need for continued operations if a local or regional event adversely affects access to the primary site or interrupts normal operations. So that DMH can assess Vendor's ability to provide continued business operations, Vendor must submit a Continuity of Operations Plan (COOP).

335. COOP services include but are not limited to the provision of hosting, system data, and documentation to ensure essential services in the event of a disaster declaration. Essential functions are defined as those functions that enable Vendor to provide normal operations under any and all circumstances.

    a. The COOP must include plans for periodic training drills involving all pertinent personnel, equipment, and systems to maintain readiness to respond to disaster declarations. DMH and Vendor will agree on the timing of disaster training drills.
    b. The COOP must document procedures to ensure the performance of essential functions during abnormal conditions, including system maintenance and system upgrades.

336. Vendor agrees that COOP services will be considered a part of system maintenance and will be covered by the system maintenance fees.

337. At a minimum, the COOP must:

    a. Ensure continuous performance of essential functions and operations during an emergency or planned outage;

b. Protect essential system functionality, continuity of records, and other assets;
c. Reduce or mitigate disruptions to operations; and
d. Achieve a timely and orderly recovery from an emergency and resume full service to users.

338. At a minimum, the capabilities provided by the Vendor in the COOP must:

a. Be capable of providing 100 percent of the EHR services both with and without warning/scheduling; and
b. Be continuously operational in a hosted environment during normal operations.

339. At a minimum, the COOP must address:

a. Plans and procedures;
b. Identification of essential functions;
c. Alternate facilities;
d. Interoperable communications;
e. Vital records and databases; and
f. Tests, training, and monthly exercises and drills.

340. Upon implementation, the COOP must:

a. Outline a decision process for determining appropriate actions in implementing COOP plans and procedures.
b. Establish a roster of fully equipped and trained emergency provider and State personnel with the authority to perform essential functions and activities.
c. Establish reliable processes and procedures to acquire resources necessary to continue essential functions.

341. Declaration of Disaster

a. In the event of a declared disaster, DMH expects the Vendor to be completely responsible for the restoration of EHR operations.
b. Vendor will be expected to invoke the appropriate disaster recovery plan within four (4) hours from the disaster declaration and the disruption of normal EHR operations.
c. DMH must be able to log on to the Vendor's failover system at the disaster recovery site immediately upon the disaster declaration.
d. Vendor shall have 100% capacity of the operational system regardless of the declaration of the disaster by the State or the Vendor.
e. Vendor's failure to make a declaration of a Disaster within four (4) hours shall result in any system downtime, as a result of this incident, being deemed as unscheduled downtime.
f. In the event of a disaster declaration, Vendor must remain in regular and consistent communications with DMH, keeping all relevant managers and responders informed and updated on efforts to restore normal operations.

342. The Vendor shall conduct an annual test of the Disaster Recovery process and Business Continuity Plan (COOP) and submit the resulting Test Report that includes the outcome, corrective action plan, and revisions, if any, to the State within 30 days of completion.

VII. IMPLEMENTATION REQUIREMENTS – STATEMENT OF WORK

A. Vendor Acknowledgement

343. This section outlines the DMH minimum expectations of the awarded Vendor for implementation of the selected solution. Implementation deliverables will reveal the Vendor's expertise in project management, EHR process management and improvement, data migration, and acceptance testing, etc. DMH expects the proposed preliminary implementation plans to be refined by the awarded Vendor and DMH project managers during the implementation process. Whether the awarded Vendor will need to be onsite at any time will be determined by the implementation project demands. DMH reserves the right to require onsite Vendor participation if it would be in the best interest of DMH.

344. The State expects the awarded Vendor to be responsible for design, configuration, implementation, testing, training, hosting, maintenance, and support of the awarded solution.

345. The State expects implementation with limited interruption to incumbent behavioral/mental health services and business operations. Any interruption to such operations must be approved by DMH and conducted in a way to prevent loss of service.

346. Upon award, DMH intends for the requirements set forth in Attachment A and Section VII of the RFP and the Vendor's proposal, including any subsequent, agreed upon provisions and revisions, to act as the Implementation Statement of Work.

B. Project Management Plan

347. Project Management Plan (PMP): DMH desires to implement the proposed solution as rapidly as possible after contract execution. So that DMH can assess Vendor's ability to successfully implement the proposed solution, Vendor must submit a preliminary PMP. At a minimum the PMP must address design and development, all implementation tasks, data migration, estimated hours per task, major project milestones, quality assurance checkpoints, testing, and end-user training for all facets of the solution.

348. Vendor's PMP must reflect industry best practice standards and must detail Vendor's plans for planning, monitoring, supervising, tracking, and controlling all project activities.

349. Vendor's PMP must include a preliminary Integrated Master Schedule (IMS). The IMS must estimate the time necessary to complete all phases of implementation from the point of contract execution through completion of go-live, final system acceptance, and user training.

350. The PMP, which will require DMH approval, must reveal plans for multiple environments, including design and development, user testing, acceptance testing, production, end user training, and help desk support. In the user testing environment, all customizations, integrations, interfaces, and interoperability must be tested and validated.

351. Vendor's PMP must describe the organizational structure of the implementation team, team member roles and responsibilities, resources, processes, and all other information necessary for DMH to assess your ability to manage the EHR implementation.

352. Upon award, the Vendor and DMH will jointly modify the proposed PMP and IMS as appropriate to meet implementation objectives. DMH expects the Vendor to work with the DMH Project Manager to ensure effective project management during all implementation phases and ongoing operations.

353. Vendor will be responsible for any interface, integration, interoperability, conversion, migration, or other issues that may arise during implementation.

354. As it relates to this procurement, state all Vendor assumptions or constraints regarding the proposed solution and overall project plan, timeline and project management.

355. Identify any potential risks, roadblocks, and challenges you have encountered in similar implementations that could negatively affect a timely and successful completion of the project. Recommend a high-level strategy to mitigate these risks.

356. DMH will have limited resources available to the awarded vendor for implementation.

C. Data Migration

357. Vendor must be capable of migrating existing EHR data for each DMH facility from the incumbent solution to the awarded solution. Each DMH facility will decide whether or not to migrate legacy data. These facilities include East Mississippi State Hospital (EMSH), North Mississippi State Hospital (NMSH), South Mississippi State Hospital (SMSH), Mississippi State Hospital (MSH), Central Mississippi Residential Center (CMRC), and Specialized Treatment Facility (STF). Vendor must submit separate line item pricing for the migration of data for each facility in RFP No. 4280, Section VIII Price Information Submission.

D. User Acceptance Testing

358. Vendor agrees to support DMH's User Acceptance Testing (UAT) to prove that the EHR system fully meets the requirements of this RFP/Attachment A.

359. So that DMH can assess Vendor's ability to conduct UAT, Vendor must submit with this proposal a preliminary User Acceptance Testing Plan. DMH will accept a sample plan from a previous implementation of similar size and scope and Vendor may redact the plan if necessary.

360. At a minimum, the UAT Plan must incorporate the following minimum components:

    a. UAT Test Procedures and Methodologies, including final acceptance testing to confirm that the awarded solution performs in accordance with the requirements of this RFP;
    b. UAT Test Report; and
    c. Training Materials;

361. At a minimum, the UAT Plan must:

    a. Include both scripts and normal operations to test end-to-end workflows, customizations, and integrations; all DMH interoperability and interfaces must be tested and validated.
    b. Provide a full suite of reports generated during the UAT period to validate the reporting functions.
    c. In the user testing environment, all customizations, integrations, and interfaces must be tested and validated.

362. Upon award, Vendor agrees to finalize the preliminary UAT plan with input from the DMH project team.

    a. Vendor agrees that the final UAT plan requires approval from DMH.
    b. Vendor agrees that DMH retains the right to determine the success or failure of individual UAT tests.
    c. Vendor must provide the personnel to support the services identified in the UAT, including DMH Final Acceptance Review (FAR).

363. Vendor must agree to regular status meetings with DMH project management team to review progress on UAT.

    a. Vendor agrees to submit meeting agendas, presentation materials, and subsequent meeting minutes.

E. User Training and Documentation

364. Awarded Vendor must provide complete user training documentation and keep it updated as appropriate. Web-accessible format is acceptable to DMH.

365. Awarded Vendor must provide thorough online tutorial/training geared toward DHM users.

366. Prior to go-live, Vendor must agree to adequately train 40 - 50 DMH staff users and administrators in how to use the system to successfully perform their respective tasks and workflows. Vendor must use a train the trainer approach. Online or onsite training is acceptable.

367. Awarded Vendor must train DMH staff users and administrators in the effective use of the document management system.

368. Awarded Vendor must train the primary system administrators in all facets of system use, including but not limited to oversight, reporting, security, workflow, archival, and audit trail functions.

369. Solution must provide on-line training modules to address system customization that may be performed by DMH authorized users.

370. Awarded Vendor must provide pre-implementation training.

371. For training that is not included in the cost of the base offering, Vendor must provide itemized costs in response to Section VIII of RFP No. 4280, Cost Information Submission. Vendor must include a fully loaded daily rate for any on-site training that is not included in the cost of the base offering.

F. Change Management and Control

372. Vendor must agree that upon award, Vendor will describe, justify, and submit all proposed changes to the agreed upon project deliverables to DMH for approval. Such proposed changes include but are not limited to project scope, any and all implementation requirements, technical, functional, and configuration requirements, and/or all other agreed upon project deliverables.

373. The Project Manager must develop a Change Management Plan (CMP) for DMH which will be executed during implementation and followed throughout the lifecycle of the EHR project. At a minimum, the CMP must include the following components:

    a. Readiness assessments;
    b. Communication and communication planning;
    c. Change management activities/events and related roadmaps;
    d. Coaching and manager training for change management;
    e. Developing and providing all facets of user training, including train the trainer;
    f. Mitigation of change resistance to the awarded solution;
    g. Data collection, feedback analysis, and corrective actions;
    h. Celebrating and recognizing success; and
    i. After-project review.

374. Vendor must agree to follow the State's process for change control, which consists of the following minimum components:
    a. Change Request Identification via Change Request Form - Documentation of change details such as type of change, benefits of change, resources, time and cost estimates, authorizations, etc. (Vendor);
    b. Change Request Assessment (State);
    c. Change Request Analysis (State/Vendor);
    d. Change Request Approval (State);
    e. Change Request Implementation (Vendor, overseen by State); and
    f. Change Log – Project details such as project number, priorities, target date, status, etc. (Vendor).

VIII. Software Administration and Security

A. General

375. For hosted services, the design must be compliant with the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy. For access to the State of Mississippi Enterprise Cloud and Offsite Hosting Security Policy, send an email request to khelli.reed@its.ms.gov. Include a reference to this RFP/Attachment A requirement as justification for your request.
376. Solution must provide controlled access to features and functions by configurable, role-based permissions as defined by DMH.
377. Solution must allow the system administrator to set rights for access to data by individual or group.
378. Solution must prevent unauthorized access to the system.
379. Solution must accommodate administrator user rights to any and all workflows and tasks as determined by DMH.
380. Authorized DMH staff must be able to restrict specific user groups from being able to view or print certain types of documentation.
381. Roles, security, and access rights must be easily configurable without Contractor assistance.
382. The proposed solution must adhere to all current, relevant security, and privacy standards.
383. The proposed solution must offer up-to-date, best practice identity management tools to govern user access, such as forced password changes, historical password checks, and the setting of temporary passwords, etc.
384. Solution must auto terminate sessions after a specified time of inactivity.
385. Solution must accommodate two-factor authentication.

B. Cloud or Offsite Hosting Requirements

386. Data Ownership - The State shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Vendor shall not access State User accounts, or State Data, except (i) in the course of data center operation related to this solution; (ii) response to service or technical issues; (iii) as required by the express terms of this service; or (iv) at State 's written request.

387. Data Protection - Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Vendor to ensure that there is no inappropriate or unauthorized use of State information at any time. To this end, the Vendor shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions:

388. All information obtained by the Vendor under this contract shall become and remain property of the State.

389. At no time shall any data or processes which either belong to or are intended for the use of State or its officers, agents, or employees be copied, disclosed, or retained by the Vendor or any party related to the Vendor for subsequent use in any transaction that does not include the State.

390. Data Location - The Vendor shall not store or transfer State data outside of the United States. This includes backup data and Disaster Recovery locations. The Vendor will permit its personnel and contractors to access State data remotely only as required to provide technical support.

391. Encryption - The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.

392. For engagements where the Vendor stores non-public data, the data shall be encrypted at rest. The key location and other key management details will be discussed and negotiated by both parties. Where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection. Additionally, when the Vendor cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. The policy shall comply with the following requirements:

    a. The policy shall be issued by an insurance company acceptable to the State and valid for the entire term of the contract, inclusive of any term extension(s).
    b. The Vendor and the State shall reach agreement on the level of liability insurance coverage required.
    c. The policy shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.
    d. At a minimum, the policy shall include third party coverage for credit monitoring. notification costs to data breach victims; and regulatory penalties and fines.
    e. The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Vendor's limit of liability.
    f. The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.
    g. The Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.
    h. The coverage under the policy shall be primary and not in excess to any other insurance carried by the Vendor.
    i. In the event the Vendor fails to keep in effect at all times the insurance coverage required by this provision, the State may, in addition to any other remedies it may have, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.

393. Breach Notification and Recovery - Unauthorized access or disclosure of non-public data is considered to be a security breach. The Vendor will provide immediate notification and all communication shall be coordinated with the State. When the Vendor or their sub-contractors are liable for the loss, the Vendor shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least 3 years, mailing costs, website, and toll free telephone call center services. The State shall not agree to any limitation on liability that relieves a Vendor from its own negligence or to the extent that it creates an obligation on the part of the State to hold a Vendor harmless.

394. Notification of Legal Requests - The Vendor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Vendor shall not respond to subpoenas, service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

395. Termination and Suspension of Service - In the event of termination of the contract, the Vendor shall implement an orderly return of State data in CSV or XML or another mutually agreeable format. The Vendor shall guarantee the subsequent secure disposal of State data.

396. Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Vendor shall not take any action to intentionally erase any State data.

397. Termination of any services or agreement in entirety: In the event of termination of any services or of the agreement in its entirety, the Vendor shall not take any action to intentionally erase any State data for a period of 90 days after the effective date of the termination. After such 90 day period, the Vendor shall have no obligation to maintain or provide any State data and shall thereafter, unless legally prohibited, dispose of all State data in its systems or otherwise in its possession or under its control according to National Institute of Standards and Technology (NIST) approved methods. Within this 90-day timeframe, Vendor will continue to secure and back up State data covered under the contract.

398. Post-Termination Assistance: The State shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement.

399. Secure Data Disposal: When requested by the State, the provider shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods. Certificates of destruction shall be provided to the State.

400. Background Checks - The Vendor warrants that it will not utilize any staff members, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty. The Vendor shall promote and maintain an awareness of the importance of securing the State's information among the Vendor's employees and agents.

401. Security Logs and Reports - The Vendor shall allow the State access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period of time as well as the ability for an agency customer to request reports of

activities of a specific user associated with that agency. These mechanisms should be defined up front and be available for the entire length of the agreement with the Vendor.

402. Contract Audit - The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State's expense.

403. Sub-contractor Disclosure - The Vendor shall identify all of its strategic business partners related to services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.

404. Sub-contractor Compliance - The Vendor must ensure that any agent, including a Vendor or subcontractor, to whom the Vendor provides access agrees to the same restrictions and conditions that apply through this Agreement.

405. Processes and Procedures - The Vendor shall disclose its non-proprietary security processes and technical limitations to the State so that the State can determine if and how adequate protection and flexibility can be attained between the State and the Vendor. For example: virus checking and port sniffing — the State and the Vendor shall understand each other's roles and responsibilities.

406. Operational Metrics - The Vendor and the State shall reach agreement on operational metrics and document said metrics in the Service Level Agreement. At a minimum the SLA shall include:

a. Advance notice and change control for major upgrades and system changes
b. System availability/uptime guarantee/agreed-upon maintenance downtime
c. Recovery Time Objective/Recovery Point Objective
d. Security Vulnerability Scanning

IX. Final Acceptance Review

407. Vendor agrees that upon the successful completion of all implementation phases, DMH will conduct a Final Acceptance Review (FAR) to determine whether or not Vendor has satisfied the terms and conditions of the awarded contract, which includes the requirements of this Attachment A to RFP No. 4280.

X. Support and Maintenance

A. Customer Support

408. The Vendor must provide a continual, around the clock (24/7/365), manned network operating center (NOC) support and monitoring. This includes but is not limited to operating system support, network monitoring and health performance, network availability, and network security reporting. These services must be offered within the continental United States.

409. Vendor must provide a toll-free telephone number for DMH staff to call 24/7/365 and an always-accessible website for trouble reporting. All telephone customer support must originate in the Continental United States and all support staff must be able to communicate clearly in the English Language. In addition to live, telephone support, other acceptable formats for technical support are web-based live chat and email.

410. Vendor must disclose instances where a third party or sub-contractor is being used for any portion of customer support services, including the intake of reported problems.
411. Vendor must keep the appropriate DMH management and technical support staff updated on the status of trouble resolution.
412. Vendor agrees to provide adequate training for the effective access and use of support services as requested by the State.
413. Vendor agrees to provide always-updated documentation of all support processes.

B. Issue Tracking

414. The Vendor shall use an industry standard tracking system to thoroughly document issues and requests for DMH.
415. Describe how operational trouble issues are submitted, prioritized, tracked, and resolved.
416. Describe how software performance issues are submitted, prioritized, tracked, and resolved.
417. Describe how user support issues are requested, prioritized, tracked and resolved.
418. Detail your escalation procedures for responding to trouble tickets, software performance, and user support issues.
419. The Vendor shall provide a customer portal for DMH to track help desk ticketing and incident resolution.
420. Details of DMH environments must be readily available to any authorized support personnel of the provider, including but not limited to architecture diagrams, network connectivity diagrams, service level agreements (SLA), contacts, backups, and monitoring alerts.
421. The Vendor must provide a monthly issue tracking report as defined by DMH. For example, the report must detail and comment on any open tickets at month's end, all issues opened and closed within the past month, and other details as required by DMH.
422. For issue tracking, solution must be capable of on demand as well as auto-run reporting.

C. Service Level Agreements

423. DMH requires notifications of service outages or degraded performance. The Vendor shall communicate notifications via a support ticket, email, telephone call, or by all three methods, depending upon the severity of the situation. Upon service restoration, the provider shall provide fault isolation and root-cause analysis findings in restoration notices to DMH points of contact.
424. Vendor must provide root-cause analysis notifications within two business days of the incident. The Vendor must have proven technology, processes, and procedures to escalate problems to DMH points of contact via a call tree-based solution, depending on the severity and type of issue.
425. The Vendor must provide a work effort estimate once a root-cause analysis is complete and be willing to expedite issues which rate "Critical" or "Severe" depending on the root-cause.
426. The provider shall follow the problem severity guidelines specified in Table 1 for assigning severity levels for incident creation.

Table 1- Service Level Agreement

Priority Level	Description of Deficiency	Acknowledge-ment	Action Plan/Follow up	Resolution Time
1 Critical	Critical defects are defined as anything that hampers the data-to-day operation of the system for the majority of the end users, no workarounds have been defined and there a potential negative impact to the State.	1 – 2 hours	4 – 8 hours from intake	12 hours
2 Severe	Severe defects are defined as anything that frequently impacts some of the State's end users, and a work around has been identified.	2 – 3 hours	8 – 12 hours from intake	24 hours
3 Moderate	Moderate defects are defined as something that infrequently impacts some of the State's end users.	4 hours	24 hours	40 hours
4 Low	Low defects are defined as something that rarely impact a small number of the State's end users.	4 hours	40 hours	80 hours

D. Remedies for Failure to Meet Service Levels

427. Vendor agrees that service credits will accrue for unscheduled downtime, including Vendor's failure to meet system availability requirements and response and resolution time requirements for curing deficiencies.

428. For purposes of assessing service credits, response timeframes will be measured from the time the Vendor is properly notified until the State determines that the deficiency has been resolved.

429. For purposes of assessing service credits, Vendor agrees that credits will be measured in monthly cumulative minutes/hours for unresolved deficiencies and unscheduled downtime.

430. The monthly required system availability hours will be calculated as follows: (24 hours a day) X (7 days a week) X (52 weeks per year) X .9998 ÷ 12. The total unscheduled downtime minutes per month are calculated as follows: Total hours per month X (1 – Uptime Range Column in Table 2a.

431. Vendor agrees that all downtime exclusive of scheduled maintenance will entitle the State to service credits in accordance with Table 2a, Service Credit Assessments.

432. Without limiting any other rights and remedies available to State, Vendor agrees to issue service credits in accordance with the measures prescribed by Tables 2a & b, Service Credit Assessments.

433. Vendor agrees that service credits will be calculated separately for each applicable deficiency and will be assessed at the end of each month of system maintenance.

434. Vendor agrees that service credits are not penalties and, when assessed, will be deducted from the State's payment due to the Vendor.

Table 2a – Service Credit Assessments for Unscheduled Down Time

Uptime Range	Length of Unscheduled Monthly Down Time	Monthly Service Credits for Down Time
100% - 99.98%	0 – 8.74 minutes	$0.00
<99.98% - 99.45%	>8.74 minutes – 4 hours	$3,000.00
<99.45% - 98.35%	>4 hours – 12 hours	$9,000.00
<98.35% - 96.70%	> 12 hours – 24 hours	$18,000.00
	Each additional block of: Up to 4 hours >4 hours - 12 hours or > 12 hours - 24 hours	 $3,000.00 $9,000.00 $18,000.00

Table 2b – Service Credit Assessments Per Incident for Timeframes Defined in Table 1

Priority Level	Service Credit for Failure to Meet Response Requirement	Service Credit for Failure to Provide Action Plan/Follow Up	Service Credit for Failure to Meet Resolution Requirement
Severity 1 – Critical Respond: 1 – 2 hours Action Plan: 4 – 8 hours Resolve: 12 hours	$1,500.00	$1,500.00	$3,000.00

Priority Level	Service Credit for Failure to Meet Response Requirement	Service Credit for Failure to Provide Action Plan/Follow Up	Service Credit for Failure to Meet Resolution Requirement
Severity 2 – Severe Respond: 2 – 3 hours Action Plan: 8 – 12 hours Resolve: 24 hours	$1,000.00	$1,000.00	$2,000.00
Severity 3 – Moderate Respond: 4 hours Action Plan: 24 hours Resolve: 40 hours	$500.00	$500.00	$1,000.00
Severity 4 – Low Respond: 4 hours Action Plan: 40 hours Resolve: 80 hours	$250.00	$250.00	$500.00

E. System Monitoring

435. Vendor agrees to provide monitoring services to cover all the services provided by the Vendor, including but not limited to:

a. Network connectivity (i.e., whether the network is up or down, and real-time bandwidth usage);
b. Full stack application monitoring;
c. Services running on the operating systems;
d. Performance indicator;
e. Network latency;
f. Utilization (e.g., memory, disk usage);
g. Trending (for minimum of one year);
h. Sharing of the monitored data with DMH through a portal;
i. High Availability—provider must have capabilities to detect failover to another region or availability zone in the event DMH workload and services failover; and
j. Vendor must provide detailed examples of how it has integrated alerts that are triggered by monitoring technologies into their support processes.

F. Backup Services

436. The Vendor must be able to configure, schedule, and manage backups of all the data including but not limited to files, folders, images, system state, databases, document management system, and enterprise applications.

437. The Vendor must maintain backup system security and application updates.

438. The Vendor must provide hosted backup options.

439. The Vendor must encrypt all backup files and data and must manage encryption keys. At a minimum, the backup options must encompass a strategy of daily incremental and weekly full backups. All instances must include options for snapshots and backups of snapshots.

440. The encrypted backup should be moved to another geographical region. Regardless of the method of backup, weekly full backups must include system information. DMH minimum retention requirement for all backups is 30 days. Backup retrieval must be started within

two hours of notification from DMH. Vendor must monitor all disaster recovery instances, including replication and instance performances.

441. Solution must be capable of running backup reports on a weekly basis, or whatever sequence is required by DMH. For example, report should reveal which jobs successfully completed, which jobs failed, and which jobs restarted, etc.

442. For backup reporting, solution must be capable of on-demand as well as auto-run reporting.

443. The Vendor must be willing to provide backups on demand related to development, database changes, or emergency situations.

G. Patching

444. The Vendor must provide patching capabilities for all DMH systems. Patching must cover all Microsoft and non-Microsoft vulnerabilities.

445. The Vendor must manage deployment of new patches in DMH environment before production deployment and must be capable of excluding patches from normal patching based on requests from DMH. This may include service packs and other application-specific patches.

446. The Vendor must provide DMH with a list of patches to be applied before each patching event.

447. From time to time, DMH may request that specific patches be performed outside of the normal monthly patching cycle. The provider must be capable of supporting these out-of-cycle patch requests.

H. Processes

448. The Vendor shall have mutually agreed upon processes and policies in place to support EHR operations.

    a. Any modifications to the agreed upon policies and processes must receive prior approval from DMH.
    b. Such processes and policies must be thoroughly documented.
    c. Such processes and policies must be reviewed by the Vendor and DMH at least annually.

I. Product Updates

449. The State requires notice in advance of product updates. Describe your release management methodology, and processes for updating your software for all types of releases, including but not limited to:

    a. Security Updates;
    b. System Maintenance;
    c. System Enhancements; and
    d. Education and Training.

450. Describe how new functions and features are released and how much control clients have over which new features are implemented.

451. Enhancements and updates must be included with annual maintenance fees which must be included in RFP No. 4280, Section VIII Cost Information Submission.

J. Software Updates

452. Once available, Vendor must provide all software updates necessary to keep current with the proposed solution's technology standards, industry standards, third party software upgrades, enhancements, updates, patches, and bug fixes, etc.
    a. Such Software updates shall include but not be limited to enhancements, version releases, and other improvements and modifications to the core solution software, including application software.
    b. The State requires notice in advance of software updates.
453. Vendor agrees that maintenance services will also include maintaining compatibility of the solution software with any and all applicable contractor provided interfaces.
454. Vendor agrees that prior to installation of any third-party software or any update thereto, Vendor must ensure compatibility, promptly upon release, with the then current version of the software.
    a. Vendor agrees to ensure compatibility with all required or critical updates to third party software, including without limitation, service and compatibility packs, and security patches.
    b. Vendor agrees that third party application software incorporated by the Vendor is subject to the same maintenance and service obligations and requirements as the application software components that are owned or are proprietary to the Vendor.

K. Technology Refresh and Enhancements

455. Vendor agrees to conduct joint technology reviews with the State to guarantee that the software and system security are adequate for State purposes and are consistent with then-current technology used in similar systems.

XI. DELIVERABLES

A. General

456. Vendor must agree to provide the deliverables described in Table 3 below. So that the State can evaluate Vendor capabilities, Vendor must submit with the proposal these preliminary deliverables with as much detail as possible to show compliance with the specific RFP requirements. Post award and prior to implementation, Vendor and DMH will amend deliverables as appropriate. DMH approval is required for all deliverables prior to implementation.

Table 3 - Deliverables

Deliverable/Plan Title
1. Continuity of Operations Plan – (COOP) - Section VI C
2. Implementation Requirements - Section VII
Project Management Plan (PMP) - Item B
User Acceptance Testing Plan (UAT Plan) - Item D
User Training Documentation - Item E

Table 3 - Deliverables

Deliverable/Plan Title
Change Management Plan (CMP) - Item F
3. System manuals and project documentation - complete and all inclusive.

XII. APPENDIX 1 PATIENT ENCOUNTER DATA ELEMENTS

Proposing Vendors may review the *Patient Encounter Data Elements* from the ITS Website, where it is individually posted by name beneath Attachment A to RFP No. 4280.