Attachment A
to
RFP No. 4416

Mississippi State Department Of Health

Integrated Disease Surveillance Platform

ITS Project No. 46072

Attachment A to RFP No. 4416
MSDH Integrated Disease Surveillance Platform Technical Requirements

I. GENERAL

A. How to Respond

1. Beginning with Item 22 of this Attachment A, label and respond to each outline point in this section as it is labeled in the RFP.

2. The State is under the impression that Vendors have read and agree to all items in this RFP. Vendors should take exception to items to which they disagree.

3. The Vendor must respond with "WILL COMPLY" or "EXCEPTION" to each point in this section. In addition, many items in this RFP require detailed and specific responses to provide the requested information.   Failure to provide the information requested will result in the Vendor receiving a lower score for that item, or, at the State's sole discretion, being subject to disqualification.

4. "WILL COMPLY" indicates that the vendor can and will adhere to the requirement. This response specifies that a vendor or vendor's proposed solution must comply with a specific item or must perform a certain task.

5. If the Vendor cannot respond with "WILL COMPLY", then the Vendor must respond with "EXCEPTION". (See Section V, for additional instructions regarding Vendor exceptions.)

6. Where an outline point asks a question or requests information, the Vendor must respond with the specific answer or information requested.

7. In addition to the above, Vendor must provide explicit details as to the manner and degree to which the proposal meets or exceeds each specification.

B. Mandatory Provisions in Technical Requirements for this RFP

8. Certain items in the technical specifications of this RFP are MANDATORY. Vendors are specifically disallowed from taking exception to these mandatory requirements, and proposals that do not meet a mandatory requirement are subject to immediate disqualification.

9. Mandatory requirements are those features classified as "**MANDATORY**" in Section VII, Technical Specifications of RFP No. 4416 and/or Attachment A. Meeting a mandatory requirement means the Vendor meets the qualifications and experience required and/or requested functionality exists in the base solution.

C. General Overview and Background

10. The Mississippi State Department of Health (MSDH) and ITS are issuing this RFP to secure a qualified Vendor, through competitive procedures, to provide a Public Health communicable disease focused, integrated software solution and implementation services for a comprehensive, statewide, patient-centric Integrated Disease Surveillance Platform (IDSP). The Vendor will configure, implement, and maintain a Vendor-hosted web-based communicable disease reporting and surveillance system that provides MSDH with the required functionality to run and manage the Sexually Transmitted Diseases and Human Immunodeficiency Virus (STD/HIV), Tuberculosis (TB), and Epidemiology (EPI) programs by processing near real-time electronic laboratory results and electronic case records. It will also meet all Centers for Disease Control and Prevention (CDC) reporting requirements, allow for manual web-based reporting, and integrate associated, critical systems such as the MSDH

electronic health record system (Epic), geographic information systems, and other mission critical systems (e.g., immunization registry) required for each MSDH program to efficiently manage disease surveillance and response.

11. MSDH considers integrated to mean the IDSP will support all communicable disease programs in a modernized infrastructure. The current siloed surveillance systems utilized by the multiple MSDH program/office areas does not allow for a patient-centric approach that supports all public health events for a patient to be viewed from one central location. Functionality that currently exist in the multiple surveillance systems used by the various programs, including manual processes, will be integrated into a single, modernized IDSP infrastructure to support MSDH. A robust IDSP supporting STD/HIV, TB, and EPI will eliminate patient deduplication, decreased missed opportunities due to inaccessible data, increase efficiencies in case investigations, case reporting, outbreak management, contact tracing and reduce effort and cost for on-going maintenance and support.

12. An IDSP will help improve the agency's public health disease surveillance infrastructure to:

- Increase MSDH disease surveillance efficiencies by facilitating state public health department collaboration, by providing the ability to view MSDH patients in a public health holistic context,

- Increase MSDH's data analytical capabilities by providing an integrated data repository, which is a hub for infectious disease surveillance,

- Increase the timeliness of data reporting by reducing the data entry burden on public health professionals,

- Provide customizable tools such as easily configurable electronic disease data collection forms to quickly respond to emerging diseases,

- Reduce MSDH manpower requirements by removing the need to support multiple, siloed systems,

- Increase data availability by, connecting all MSDH disease surveillance programs to laboratories, healthcare providers, and national public health partners, utilizing existing standards,

- Provide a system that combines technology, standards, and disease surveillance to be used to affect public health regulations and policy, and

- Shift from paper to electronic data exchanges.

13. The Office of Communicable Diseases is responsible for statewide surveillance and investigation of reportable diseases and conditions. Activities include:

- Investigation of individual cases and outbreaks of communicable diseases,

- Collection, and analysis, to identify disease trends, including emerging infections,

- Dissemination of communicable disease information and education and training of public health and healthcare professionals on communicable disease prevention and control, and

- • Planning epidemiological strategies/responses – to the occurrence of diseases of public health concern, outbreaks and public health emergencies involving communicable diseases

To support these functions, the IDSP will be used to track disease reports received from hospitals, laboratories, physicians, and other health care providers. The system must be capable of receiving manual key-entered and electronically transmitted disease and laboratory reports, assigning case investigations, tracking workflow, generating management and surveillance reports, and exporting data.

Rules and regulations governing reportable disease and conditions can be found here: MSDH Reportable Disease and Conditions Regulations

A list of notifiable conditions can be found here: Reportable Disease List

The MSDH programs directly impacted by this RFP in the Office of Communicable Diseases are Epidemiology, TB, and STD/HIV.

14. The following table identifies the number of MSDH cases identified and laboratory reports for each program area that the new solution will support and is not reflective of state-wide data. This table does not include COVID-19 data.

Program	2018		2019		2020*	
	Cases** Identified	Lab*** Reports	Cases** Identified	Lab*** Reports	Cases** Identified	Lab*** Reports
Epidemiology	3,760	15,423	4,308	16,473	4,954	17,896
TB	80	644	58	628	43	393
STD/HIV	32,777	301,396	38,541	304,298	38,910	229,620

*Numbers may be artificially low due to pandemic.

**Cases identified are defined as how many cases are reported to MSDH.

***Lab reports are defined as electronic and manually lab reports provided to MSDH.

Additional MSDH disease statistics and data can be found at: Home - Mississippi State Department of Health (ms.gov)

a. Epidemiology: The Office of Epidemiology is responsible for monitoring the occurrences and trends of reportable and communicable diseases, investigating outbreaks of diseases, monitoring disease trends and impact on at-risk populations to develop public health measures to interrupt outbreaks or disease occurrences, and reporting trends to the medical community and other target groups. This office also provides consultation to health care providers and the public on communicable diseases and disease outbreaks.

The Office of Epidemiology will benefit from the IDSP, as the integrated and efficient collection and tracking reportable conditions and associated data will ensure:

- Automatic case creation based on HER/eCR, lab test type, and result;

- Prompt investigation of cases of selected reportable diseases to prevent further transmission;

- Analytical capabilities to assist in creation of epidemiological strategies and plans in response to public health emergencies and occurrence of diseases;

- Ability to look at risk factors and data across diseases for commonalities for individuals who have multiple diseases and to target educational and prevention efforts;

- Ensure that household or other close contacts of selected disease cases receive preventive treatment or appropriate evaluation, when indicated;

- Investigate disease outbreaks to identify and eliminate their sources;

- Receipt of HL7 files from participating labs and provide appropriate HL7 messages using CDC HL& Message Mapping Guides for outbound delivery;

- Determine whether reported cases meet specific surveillance definitions for inclusion in disease statistics;

- Prepare statistical reports and data dashboards; and

- Report to state and national disease registries.

b. Tuberculosis: Surveillance of TB cases is a key activity for MSDH. The Office of Epidemiology, the TB program will benefit from:

- Automated creation of patient TB records using electronic lab reporting

- A seamless integrated contact tracing tool to link cases and contacts

- The ability to timely track contracts and symptom monitoring allowing quicker initiation of control and prevention measures thereby limiting the spread of the disease in a community

- The ability to know the HIV status of TB patients, and

- Communication with other MSDH Program areas (specifically STD/HIV) regarding patient history and proper treatment.

c. Sexually Transmitted Disease (STD)/Human Immunodeficiency Virus (HIV): The MSDH STD/HIV Program provides screening/testing, surveillance, education, treatment, and partner notification for reportable STDs (syphilis, chlamydia, and gonorrhea) and HIV in the state.

Further benefits of the IDSP to benefit the STD/HIV program is:

- The automation of completion of CDC and MSDH forms;

- The ability to know the TB status of HIV patients; and

- The flexibility of supporting future reporting and form changes as necessary.

15. Epidemic, Pandemic, or Natural/Man-made Public Health Disaster Surveillance and Reporting

   Epidemic, pandemic, or natural/man-made public health disaster surveillance allows MSDH the ability to monitor and track the event as well as educate and inform the public of the appropriate measures for prevention. The IDSP shall have the capability to scale for supporting epidemic, pandemic, or natural/man-made public health disaster surveillance and reporting such as the Coronavirus (COVID-19) pandemic.

   When COVID-19 first presented, MSDH used their existing system to log and track cases identified throughout the state. However, as the numbers significantly increased over a short amount of time, it became apparent that another solution would need to be used for documenting and tracking the disease. In August 2020, all COVID-19 data began being tracked in the National Electronic Disease Surveillance System (NBS).

   In the event of epidemic, pandemic, or natural/man-made public health disaster, MSDH shall have the ability to use the IDSP for all surveillance purposes without the need for any other system or interruption in service.

Program	2020		2021	
	Cases Identified	**Lab Reports**	**Cases Identified**	**Lab Reports**
COVID-19	219,897	1,891,587	346,331	2,751,121

   Additional information and data reports regarding MSDH's COVID-19 program can be found at: Coronavirus COVID-19 - Mississippi State Department of Health (ms.gov)

16. Prior to the COVID-19 pandemic, there were approximately 500 internal and 250 external users. During the pandemic, there was an increase in the need for disease surveillance user accounts, both internally (approximately 1,200) and externally (approximately 2,800). The systems are available to input infectious disease reports on a 24/7/365 basis for disease control and disease surveillance purposes.

D. Statement of Understanding

17. Attendance at the Vendor Web Conference on Tuesday, October 11, 2022 at 11:00 a.m. Central Time is optional for any Vendor who intends to submit an RFP response.

   a. To access the Vendor Web Conference, Vendor must contact Khelli Reed via email no later than Monday, October 10, 2022 at 12:00 p.m. Central Time to receive instructions on how to enter into the web conference.

18. Because Cambria Solutions assisted in the preparation of this RFP Number 4416, they are disallowed from responding to this RFP.

19. Hourly Rates for Change Orders

   a. The Vendor must provide fully loaded, onsite and remote, off-site hourly change order rates for each proposed role as well as a fully loaded blended rate. Blended rates shall be used in pricing of any subsequent change orders

and will be based on milestones. Fully loaded rates include hourly rate plus travel, per diem, and lodging.

20. Additional Activities Proposed

   a. The Vendor is encouraged to recommend best practices or additional activities that would add value to the project in the RFP response. Any non-required activities which incur additional cost should be priced as an optional line item, separate from the required activities in the RFP response.

   b. MSDH reserves the right to use this procurement instrument to add additional and accompanying services that are in scope of this procurement, should they be needed.

21. Subsequent to Notice of Award and Contract Execution contract deliverables will be reviewed by MSDH and shall require formal written approval from MSDH before acceptance of the deliverable. The Vendor shall allow for a minimum ten (10) business days following receipt, per deliverable, for MSDH to review each deliverable and document its findings, except as specified by MSDH. Based on the review findings, MSDH may accept the deliverable, reject portions of the deliverable, reject the complete deliverable, or require that revisions be made. The Vendor shall make all modifications directed by MSDH within ten (10) business days of receipt. MSDH reserves the right to make modifications to these timelines and, if needed, will do so in writing with the successful vendor.

E. Vendor Qualifications

22. The Vendor shall provide a detailed narrative describing the background of the corporation that includes:

   a. Date established

   b. Ownership (e.g., public company, partnership, subsidiary)

   c. Location of the principal place of business

   d. Number and location of other satellite offices

   e. Total number of employees

      1. Full-time

      2. Vendors/Subcontractors

      3. Within the United States

      4. Off-shore/Near-shore

23. The Vendor shall demonstrate three (3) years of prior experience and consistent use with the proposed system including but not limited to:

   a. Vendor must have minimum of the three (3) Public Health IDSP projects with the proposed system in a large state, local, or territorial public health jurisdiction of similar scope, and complexity.

   b. Prior installation and success of an integrated disease surveillance platform in a large state, local, or territorial public health jurisdiction which included reporting required CDC disease tracking information.

    c. EPI management of statewide public health programs

    d. Standards-based information trading between public health trading partners

    e. Surveillance system exchanges

    f. Private system exchanges

    g. CDS disease tracking systems

        1. Development/Configuration

        2. Implementation

        3. Ongoing operations

        4. Support and maintenance

24. The Vendor shall document three (3) years prior experience with the proposed system in at least three (3) large state, local or territorial public health jurisdictions. Prior experience must describe meeting federal and state requirements that they identified and their timely incorporation into the system. Prior experience must include the project objectives, timelines, public health domains (e.g., epidemiology, tuberculosis, STD/HIV, etc.), and include relevant CDC examples if available. Prior experience should consider this RFP and provide a rational of why the experience shows that the Vendor has the experience to implement this RFP's requirements.

F. Staffing Requirements

25. Key Personnel (KP) designated as part of the proposed solution shall remain on the project team for the duration of the project unless a change in team is the result of a request or approval by MSDH in writing. If any key personnel leave the company, MSDH shall review resumes for any key personnel filling of vacancies.

26. The Vendor shall make provisions as needed for personnel to come on-site in Jackson, Mississippi and be available to personnel at an MSDH facility as determined by MSDH and mutually agreed upon. The Vendor shall describe in detail how it will collaborate with MSDH to ensure team member remote accessibility and team member on-site commitment.

    a. The Vendor shall provide all hardware, software, transportation and lodging necessary for Vendor personnel to fulfill the RFP requirements. MSDH can provide minimal office space for on-site staff allowing collaboration between MSDH staff and Vendor staff. MSDH will provide adequate meeting space for the duration of the project.

    b. The Vendor shall consider a full business day and make remote and/or on-site staff available during that time of 8:00 a.m. to 5:00 p.m. Central Time.

    c. MSDH expects the Project Manager (PM) to adjust on-site schedules to provide elevated coverage at critical times relative to the solutions integration into the MSDH environment. MSDH expects a PM on-site presence of ten (10) business days a month during implementation. MSDH also expects a PM presence at steering committee meetings, key status meetings, and other key meetings, upon MSDH request, when provided with a minimum of a two (2) week notice.

d. The Vendor's technical architect shall be on-site with full time availability during critical periods such as JADs, integration planning, integration testing, and implementation. MSDH can request and expects the Vendor to accommodate on-site presence for key stakeholder meetings and other key meetings when provided with a minimum of a two (2) week notice. MSDH expects the Vendor to propose the on-site availability periods with a minimum coverage of three (3) full business days a week during critical periods.

e. The Vendor shall propose the on-site availability of the business analysts assigned to the Project. MSDH anticipates there are times, such as during discovery, JADs and planning, where on-site presence will increase productivity and decrease project risk.

27. The Vendor shall provide a narrative of relevant experience for all proposed key personnel identified in the proposal. If the proposed individual is not an employee, a letter of commitment to join the project upon award is required.

   a. The Vendor Experience Narrative document is incorporated in the RFP as Attachment B. It must be attached to the resumes describing specific experience with the type of service to be provided within this RFP. The Vendor will be required to describe specific experience with disease surveillance projects and include any professional credentials, licenses, and recent and relevant continuing education.

28. The Vendor shall provide a staffing contingency plan for all Key Personnel, which shall be updated annually, at a minimum.

29. The Vendor shall ensure Key Personnel maintain adequate subject matter expertise in all public health disciplines throughout the duration of the project. Subject matter expertise is defined as personnel with significant experience and knowledge in state, local, and jurisdictional public health systems that impact this project.

30. (KP) Project Executive: For the duration of the entire project, the Vendor shall provide an overall Project Executive with on-site/virtual responsibilities once per month for the MSDH monthly Steering Group meetings.

31. (KP) Project Manager (PM) for the proposed IDSP instance(s). The PM shall have the following experience and skill set:

   a. Minimum of three (3) years of experience with a large state, local, or territorial public health jurisdiction.

   b. **MANDATORY:** Minimum of three (3) years of experience participating in a project related to a public health integrate disease surveillance system, with a large state, local, or territorial public health jurisdiction, project as a Business Analyst, Subject Matter Expert, Project Lead, Technical, or other similar role. Other roles proposed to meet this experience requirement will be approved at the sole discretion of MSDH. Vendor must describe how they will meet this requirement.

   c. **MANDATORY:** Must have at least one (1) year verifiable experience leading at least one (1) successful implementation of a public health integrated disease surveillance system, with a larger state, local, or territorial public health jurisdiction, and/or project of similar size, scope, and complexity (multiple

entities, systems, data sources, and/or modules) to this multifaceted project. Vendor must describe how they will meet this requirement.

d. Project Management Professional (PMP) Certification

e. Demonstrable knowledge of PMBOK project management theories and practices applicable to highly complex projects.

f. Experience making presentations to high-level executives and stakeholders.

g. Experience providing functional supervision and direction to high-level executives.

h. Experience in providing leadership to staff.

i. Experience in performing complex advanced level research.

j. Experience in identifying project risks, gaps, and providing solutions to complex high-level projects.

k. Proven negotiation and facilitation experience.

l. Experience implementing and using new technology and work processes to enhance decision-making.

m. Experience organizing and presenting information effectively, both orally and in writing.

n. Experience applying independent judgment in making critical decisions.

o. Experience leading and working cooperatively in a team environment.

p. The PM will be responsible for the following:

1. Performing overall project planning (including a detailed project plan in MS Project), project reporting, project management, quality assurance, and documentation as needed or required by MSDH;
2. Managing the overall project in accordance with the project plan;
3. Creating monthly overall status report;
4. Managing team members including the Technical Architect, Business Analysts, Testers, and any support staff;
5. Creating and maintaining Risk and Issue Registers;
6. Supporting the work of any oversight or IV&V Vendor testing, including UAT and validating performance, stress testing and other testing and validation as deemed necessary;
7. Reporting to the MSDH Project Manager and serving as liaison to any Independent Verification and Validation Vendor (IV&V) or Systems Integrator MSDH is using on a project;
8. Performing responsibilities on-site for a minimum of two (2) weeks per month (unless otherwise given written approval from MSDH) from Project Initiation until completion of Project Go-Live;
9. Performing on-site (unless otherwise given written approval from MSDH) responsibilities post Go-Live one (1) week per month, for duration of contract; and
10. Attending monthly Steering Group meeting at MSDH in Jackson, Mississippi and presenting overall status, issues, and risks to participants.

32. (KP) Technical Architect: One (1) Technical Architect to support the IDSP instance(s), as well as the integration of the solution into the MSDH technical and operational environment. Experience must clearly demonstrate prior experience such that focus is on MSDH integration, not on the job training.

   a. Technical Architect shall have experience in the key areas listed below. An explanation must be provided describing the candidate's specific experience in each key area and supported by the provided resume

      1. Minimum of three (3) years of experience as a technical architect or equivalent role, supporting the proposed system by integrating disease surveillance information technology into an existing public health infrastructure. Vendor must describe how they will meet this requirement.
      2. Minimum of two (2) years of experience with healthcare interoperability. Experience must demonstrate expertise and a working knowledge with SOA, HL7, FHIR, and HER portability standards and other common healthcare interoperability technologies.
      3. Experience collaborating with both public health and private sector technical teams in defining architectural roadmaps to meet business goals.
      4. Minimum of two (2) years of experience in end-to-end Cloud-based solution design and development.
      5. Experience in systems, hardware, and network design and developments.
      6. Strong, articulate communication skills, including ability to convey the right level of technical detail for multiple audiences (executives, IT staff, policy staff, program support staff, etc.).

   b. Technical Architect will be responsible for the following:

      1. Providing technical planning and design of the proposed solution for MSDH programs included in this RFP;
      2. Providing overall technical subject matter expertise;
      3. Providing on-site support and resources during all testing, for the duration of the contract; and
      4. Developing a "big picture" view driven from technical details and identifying "ripple effects" from any organizational technical decisions.
      5. Proficient with public health system interface implementation and interoperability using standard based solutions and protocols such as but not limited to HL7.
      6. Possess expert level knowledge of HL7 and additional interfaces to adequately support the Vendor product and meet all CDC reporting requirements.

33. Business Analyst: One (1) primary or lead business analyst is required.

   a. Business Analyst shall have the following experience and skill set:

      1. Minimum of five (5) years of experience with a large state, local or territorial public health jurisdiction information technology projects.
      2. Verifiable experience with a large state, local or territorial public health jurisdiction integrated disease surveillance system implementation(s) as an Implementation Consultant or a Business Analyst.
      3. Experience working with proposed solution as a Business Analyst.

4. Experience in the development, review, distribution, and presentation of project status reports.
5. Experience in developing, reviewing, and/or discussing project related deliverables.
6. Experience in documenting and escalating project action items, issues, risks, and/or decisions in timely manner to the client, and other project stakeholders as is necessary.

b. Business Analyst will be responsible for the following:

1. Participate in staff/team meetings and trainings:
2. Provide frequent, clear, and consistent communication to the client, team members, Vendor, and direct reports;
3. Analyze, review, and maintain Vendor and/or client-supplied documentation;
4. Assist in documentation review facilitation, tracking, and maintenance;
5. Perform assigned tasks efficiently and effectively, asking questions when instructions are unclear;
6. Perform responsibilities on-site at the Vendor provided office facility or a minimum of eighty (80) hours per month (unless otherwise given written approval from MSDH) from Project Initiation until completion of Project Go-Live;
7. Assist the MSDH teams with User Acceptance Testing (UAT) as well as with any changes, updates, patches or fixes as necessary and requested by MSDH relative to meeting requirements;
8. Provide on-site support and resources during all testing for all instances as well as the integration for a seamless an integrated disease surveillance system (for DDI and then after Go-Live) including for supporting the MSDH team in testing updates, patches, fixes, and upgrades, for the duration of contract; and
9. Provide ongoing support to MSDH after Go-Live by monitoring the effectiveness of the product in the MSDH environment.

34. Technical training staff responsibilities:

a. The Vendor shall provide trainers with relevant and appropriate experience dependent on the type of training being conducted.

b. The Vendor shall provide training that will use a combination of on-site in person, as well as web-based training that will provide technical training MSDH on the approach to integration development, functions of the proposed solution, workflows, procedures of proper operation, and reporting and audit logs.

c. The Vendor shall provide detailed training documentation and system documentation for the entire technical solution. All documentation shall be updated on a regular basis, with updates occurring minimally every six (6) months.

d. The training shall be phased over time and location to support the phased implementation of all proposed instances.

e. The technical training attendees shall be composed of selected MSDH program staff selected by the MSDH IDSP Steering Committee.

35. The Vendor must provide the appropriate quality and quantity of staff to successfully perform the services described in this RFP. The Vendor shall submit a Staffing Plan to MSDH with the response to the RFP. The Staffing Plan shall include how the Vendor plans to address staffing requirements, project roles and responsibilities with Key Personnel clearly identified, partners, subcontractors, and how changes in staff will be handled through all phases of the project.

   a. The plan shall include a team organization chart that clearly defines reporting relationships. The Vendor must provide a descriptive narrative indicating the key staff status, title, roles, and responsibilities of each resource or entity identified. All positions identified on the team organization chart that are not fulfilled by project Key Personnel must include a representative profile that includes qualifications, experience, and education.

   b. The plan shall indicate the Subject Matter Expert(s) (SME) assigned to the project and the specific knowledge areas matching the public health areas targeted by this RFP. Each SMEs qualifications, education, and/or training relevant to this project is required. MSDH minimally expects credentialed SMEs in epidemiology, tuberculosis, and STD/HIV to support integration activities into those program areas.

   c. The plan shall include a statement and chart that clearly indicates the time commitment of each of the proposed project personnel for each phase. The Vendor will be required to include a statement indicating to what extent, if any, the key project personnel may work on other projects during the term of the contract. MSDH may reject any proposal that commits the proposed key personnel to other projects during the term of the contract if MSDH believes that such commitment may be detrimental to the Vendor's performance or proposed project schedule.

   d. The Vendor shall provide an emergency contact list with full contact information for all relevant participants including any commercial partners or Vendors upon whose products or services operations are dependent.

   e. The Vendor will have limited office space at the MSDH facilities in Mississippi. Equipment and lifecycle management tools (such as a secure document repository, project software, etc.) as approved by MSDH shall be provided by the Vendor. MSDH is standardized on MS Office, and other MS project software.

36. The Vendor is encouraged to enhance the essential staff with additional personnel in the proposal as they see fit.

37. The Vendor shall provide aid and support to OHIT and communicable disease program staff during the transition to the new system. Support shall include available to answer questions, recommendations for approaches to move from as-is processes into solution processes, technical staff support, and if necessary, refresher or knowledge transfer on areas MSDH staff requires additional guidance.

38. The Vendor shall describe with real company experience, how it adapted and changed in reaction to evolving COVID-19 reporting requirements, reporting volume,

system utilization increases, and rapidly changing policy. Include how the company, based on the experience, has changed to better deal with future epidemic, pandemic, or natural/man-made public health disaster.

II. FUNCTIONAL REQUIREMENTS

G. Hosting Requirements

39. The Vendor shall follow Industry Standards and Best Practices for hosting and security per the Software Development Life Cycle (SDLC) procedures.

40. MSDH seeks a single host setting for all IDSP instances. Potential host settings to be considered are any cloud-based HIPAA certified facility that complies with Federal, State and local laws.

41. **MANDATORY:** The Vendor shall be aware that under no circumstances shall any data, or equipment associated with this project reside outside the continental United States, nor shall any data, or equipment associated with this project be accessible to people outside the continental United States. Vendor must describe how this requirement will be met.

42. The Vendor shall provide a disaster recovery (DR) data center location in the continental United States that is at least two hundred and fifty (250) miles from the primary facility. Vendor's proposal shall describe how the DR data center location minimizes risk in the event of disaster, including service levels for recovery and minimizing data loss.

43. The Vendor shall host all instances in a certified, Tier 2 data center or better, with the following:

    a. All equipment required to provision, maintain, monitor, and manage the circuit to the hosting and DR facilities;

    b. Network protection on MSDH servers and cloud servers to prevent attacks and to ensure MSDH data, information, software, and networks are secured from unauthorized access. This protection shall comply with the transmission security provisions of HIPAA, as well as all relevant federal, state, and local laws;

    c. Intrusion detection and abnormal data retrieval detection and alerts (for example, mass downloads of PHI);

    d. Perform recording and reporting on security incidents and breaches (both immediate reporting and summary reporting);

    e. Current Operating System security patches;

    f. Current antivirus software;

    g. Two factor authentications to access PHI by Vendor staff;

    h. Encryption in transit and at rest; and

    i. Encryption for each website.

44. Vendor must provide wide area network (WAN) encrypted tunnel or virtual private network (VPN) tunnel support to MSDH from both the primary and the DR site.

45. The Vendor shall ensure the facility is compliant with SSAE 16 (i.e., SOC 1) and HIPAA standards.

46. The Vendor shall provide dedicated services with no intermingling of data or resources with other clients other than MSDH. This includes all internet connectivity.

47. The Vendor shall provide the data center and hosting capacity sufficient to handle the bi-directional transactions discussed in this RFP and be capable of increasing and decreasing the hosting capacity and associated cost in a structured way based on current need.

48. Vendor must demonstrate in the proposal its ability to increase the size of the circuit in incremental increases of 100 Mbps and one Gbps should MSDH require an increase in the future. Pricing must be presented in RFP No. 4416 Section VIII, Cost Information Submission as an optional cost.

49. The Vendor shall provide system and data reliability through off-site system and data backup in accordance with the SLA.

50. The Vendor's Security service shall provide monitoring for timely reporting of threats and intrusions.

51. The Vendor's Security services shall include a security agent to control all traffic between the primary and disaster recovery center and the outside world and protect against unauthorized access or intrusions.

52. The Vendor's Security services shall allow reporting for firewall and other statistics from any Internet browser with monthly analysis and recommendations to improve security and throughput.

53. The Vendor shall submit a Technical Operations Plan (TOP) at the initiation of the project. The Vendor shall follow the approved plan and maintain the plan such that it remains current and accurate to the procedures established for the technical environment. The plan shall be made available to MSDH staff and designated auditors upon request.

H. System Requirements

54. ELR/eCR Capabilities

    a. The solution shall provide a workflow for onboarding new trading partners (laboratory and provider) for ELR/electronic case reports (eCRs).

        1. The solution shall provide onboarding resources whose duties include registering the trading partner within the system, establishing connections to partner system(s), message mapping, and message quality monitoring / tracking.
        2. **MANDATORY:** The solution shall support workflows that successfully process and ingest partner data.
        3. **MANDATORY:** The solution shall support workflows that successfully identify, schedule, package and transmit data to trading partner systems.
        4. The Vendor shall provide all data source partner onboarding services and, for production interfaces, quality assurance services that identify any incoming data issues, and is responsible for working with data sources and/or data source partners to resolve.

b. The solution shall detect and properly organize or flag ingested ELR/eCR, and other reports, automatic and manual, that are duplicates. Duplicate detection shall be rules based, and the system shall allow adjusting the rules to improve data quality. e.g., a report for the same disease on the same patient is received from two sources within a week could be flagged as a duplicate. Describe the solutions approach.

   1. **MANDATORY:** The solution shall allow duplicate patient records to be manually merged. Merged patient records are flagged for end user identification that a merge occurred.
   2. The solution shall provide the ability to unmerge patient records that have been manually or systematically merged. Unmerged lab reports must maintain original record integrity.
   3. **MANDATORY:** The solution shall consider merging patient records as inclusive of merging entire patients, eCRs, ELRs, and other discrete patient record parts supported by the solution.

c. The solution shall provide alerts.

   1. The IDSP will provide alerts based on Abnormal ELR and eCR activity (e.g., data quality issues, volume based on historical reporting, etc.).
   2. The IDSP will provide alerts based on programmatic or analytical rules (e.g., clusters of specific diseases in a small geographical area, co-morbidity across multiple data sets, etc.).
   3. The IDSP will provide authorized users the ability to define thresholds for alerts.
   4. The IDSP will provide an alert if ELR messages are not received within a defined time period.
   5. The IDSP will provide an alert if there is a system wide ELR failure (e.g., ELR messages are received into the system, but are not processed or are unusable by the end user).

d. **MANDATORY:** The solution shall be capable of automatically processing and storing ELR/eCR based on mapping rules with minimal queues or manual intervention (e.g., negative results are processed and stored automatically but do not generate worker alerts unless otherwise requested by MSDH.)

   1. The solution shall auto process manually entered or loaded lab reports and case records based on the same mapping rules and quality control goals as used for electronic automatic processing.

e. **MANDATORY:** The solution shall provide mapping rule authoring support allowing MSDH personnel to create new mapping rules, edit mapping rules, assign mapping rules to be used in appropriate workflows, and assign mapping rules to be used ad hoc to clear issues related to manually entered or electronic queue entries that must be processed with special circumstances.

   1. The solution shall allow communicable disease administrative staff to add, edit, and manage the list of new diseases and existing disease names available for mapping.

55. Federal Partner Reporting

a. **MANDATORY:** The solution shall support regularly scheduled reporting to the CDC, Health Resources and Services Administration (HRSA), and any other Federal Partners per all state and federal requirements. Vendor must provide detailed description of previous reports provided.

    1. **MANDATORY:** The solution shall have the ability to send weekly reports of selected disease to Security Access Management System (SAMS) in the required (NETSS.dat) format.

    2. **MANDATORY:** The solution shall automatically create and send a weekly CSV file to the CDC with Report of Verified Case of Tuberculosis (RVCT) data.

    3. **MANDATORY:** The solution shall automatically send any updates made to diseases that are sent to the CDC via HL7.

    4. **MANDATORY:** The solution shall create reports using required formats as directed by MSDH.

    5. **MANDATORY:** The solution shall automate TB case reporting in the Web-based CDC program National Tuberculosis Surveillance System Case Reporting (NTSSCR).

    6. **MANDATORY:** The solution shall automate all CDC reporting where applicable (e.g., if the CDC supports automatically reporting for that data, the solution shall automate reporting that data.)

    7. **MANDATORY:** The solution shall support additional reporting as required by MSDH.

b. **MANDATORY:** The solution shall support Message Mapping Guides (MMGs) as required by the CDC.

    1. **MANDATORY:** All MMG development and reporting shall be in accordance with CDC standards and remain current with all CDC required updates. All current MMGs shall be identified and implemented and deployed at Go-Live.

    2. **MANDATORY:** The solution shall support implementation of additional MMGs as required by the CDC and other Federal Partners requiring MMGs for MSDH reporting at no additional cost to MSDH.

56. User Interface

a. The Vendor shall provide a solution that supports a user interface that allows users to interact with elements of the system so that MSDH has visibility into the process being used to identify the single best record and its originating source.

b. The solution shall support manual activities in areas such as merging, unmerging patient files, unmerging lab results, reviewing logs, maintaining user security, testing matching logic, and searching stored persons.

c. The proposed solution screens shall be browser based and conform to project approved usability guidelines.

d. The proposed solution shall provide a password secured browser-based user interface with multifactor authentication.

e. The solution shall provide patient searches capable of finding information, allowing users to provide demographic, diagnostic factors, and identification

(ID) (e.g., medical record number (MRN), lab ID, patient ID, investigation ID) that limit results.

1. The solution shall support ad hoc research searches as well as named searches that are available by selection to all users, limited to user groups or individuals/creators.
2. The solution shall allow users to save ad hoc queries as named queries and copy and/or edit existing named queries.
3. The Vendor shall provide a solution that supports flexible search criteria during the person identification process: for example, partial name, common pseudonyms, Soundex, Social Security Number (SSN), medical record number, encounter number, date of birth, sex, or combinations of data searching and matching on persons stored in the proposed solution.
4. The proposed solution shall provide multiple methods to identify its persons when provided with partial person information, enabling exact and fuzzy match logic.
5. The proposed solution shall have logic that can score returned results ranked by potential matches when a failure to find an exact person occurs.
6. The proposed solution shall support limiting the number of returned matches to avoid excessive number of returned rows based on criteria or rules.

f. The solution shall display search results in a sorted, paginated tabular list form.

1. The results list shall support column order changing, resorting, hiding columns, showing columns, showing more results, and filtering within the results.
2. Search results shall respect security regarding user role-based record segregation and shall not display record results users would not otherwise have access to.

g. The solution shall allow users to drill-down or open detailed information from the search results.

1. The solution shall have the capability for the user to return or resume a search from the place where the user was prior to navigating into additional or detailed information. A new search shall not be required, nor shall it be difficult for the user to find the summary row in search results.

h. The solution shall allow uploading documents and images and associating the documents with a patient or a patient disease event or case. The solution shall support querying of uploaded data.

1. The solution shall support uploaded documents to be found in the context where they were uploaded and will be available for viewing with an appropriate external viewer.
2. The solution shall allow users to manage documents, where allowed by roles, during and after upload. This includes assigning types such as a medical record or radiology results, correcting mistakes, removing, reassigning when linked to the wrong record, moving from lower to higher folders within the record, and other typical activities that support document upload, document labeling, and quality control.

3. The solution shall be capable of managing document upload size, where possible, to balance network capacity, storage limits, and document quality.

4. Uploaded documents are limited to MSDH viewable formats such as Microsoft formats (e.g., Word, Excel, etc.), PDF documents, and JPEG images.

5. The solution shall support uploading whole genome sequencing (WGS) and other disease sub types using HL7 or other standard formats. Discovery (JAD) will be required to determine specific.

i. The system shall allow the end-user to update the patient case, such as, but not limited to, status of the case from suspected to confirmed. It shall also have the ability to note whenever a case has been clinically verified.

j. The solution shall provide a geographical mapping capability.

1. All incoming reports via ELR, eCR, or manual entry will be automatically geocoded.

2. IDSP will provide the end user the option to map individual disease events and/or multiple related disease events

3. Authorized end users will be able to create, view, download and export a map of individual disease events and/or multiple related disease events based on parameters entered by the end user (e.g., by district, disease, age/age group, date of event, etc.)

4. The system shall store region definitions that allow assignment of workers to regions.

5. The solution shall define regions using identifiable geographical boundaries, to be determined by MSDH.

6. The system shall determine county using address information and automatically assigns disease reports to a region and worker. Automatic assignments can be adjusted and changed by authorized personnel.

k. The solution shall support adding hyperlinks.

1. The solution shall support linking external systems allows workers to quickly jump to external systems providing additional or context specific information.

2. Hyperlinks can be functional links such as email links which open the default email application.

l. The solution shall provide informative worker alerts supporting MSDH's workflow. The Vendor shall describe how JADs will be used to elaborate alerts in the system.

1. The solution shall support alerts for both normal and abnormal events that require worker or administrative action or review to continue a normal automatic workflow.

2. The solution shall allow user, with appropriate access, to define what data elements will trigger an alert, such as patient name, geographical location, data change for specific patient, etc.

m. The solution shall provide an informational dashboard or landing page to workers upon login. The Vendor shall describe how JADs will be used to elaborate dashboards in the system.

1. Solution dashboards shall have the ability for program administrators to set dashboard parameters and content by user role.
2. Solution dashboards shall be customizable by user to present surveillance information, ability to monitor and identify trends / clusters, case workload, and alerts to different user types.
3. Solution dashboards shall allow for the user to view alerts in the system and set preference on types of alerts sent via email or text.
4. Alerts sent outside of the system shall only include enough secure information that the user can understand what triggered the alert and the case ID.

n. The solution shall provide enhanced functionality for all system lists that will be used in the MSDH workflows.

1. The Vendor shall ensure every list supports a default format.
2. The solution shall support lists with more than one column that are exportable, searchable, filterable, and sortable.
3. The solution shall support lists displaying detailed information about entity data such as person, lab or clinical information allow direct linking to the entity data.
4. The solution shall allow authorized administrative staff to add, edit, and manage the list of new diseases and existing disease names available for selection in a patient's case investigation record.
   a. Authorized administrative staff can limit which diseases are available to external users.

o. The solution shall maintain a queue or list of all ingested information that cannot be automatically integrated into existing patient records. This applies to all ingested information from any source.

1. The solution shall have the ability for multiple workers to simultaneously process individual records in the queue, access to the underlying message, message source, detected errors, and perform relevant lookups to disambiguate the record and complete processing.
2. The solution supports allowing multiple users to work in the same record or queue at the same time, are alerted of other users, and are protected to ensure one user is not allowed to inadvertently overwrite another user's update.
3. The solution shall support automatic disambiguation for all types of ingested information where possible.
4. Disambiguation support covers enhanced patient identity matching, automatic error detection and correction, and other solution specific processes that can work with partial or ambiguous information and resolve it such that it can be properly associated and stored.
5. All automatic and manual disambiguation is tracked and can be audited with the solution.

57. Online Reporting

a. The solution shall provide a public facing online reporting system.

1. **MANDATORY:** The system shall allow authenticated users to use the public facing system to enter patient demographics, lab reports, and medical case information, as required by MSDH.

    a. The online reporting system will have the capability for users to upload documents related to the disease event

    b. The online reporting system shall be capable of managing document upload size, where possible, to balance network capacity, storage limits, and document quality.

2. The solution shall automatically ingest and incorporate all information entered on the public facing system into normal MSDH workflows.

3. **MANDATORY:** The public facing system shall have automatic processing similar to the automatic Electronic Laboratory Reporting (ELR/eCR) processing with as minimal as possible additional manual worker intervention (e.g., cases are automatically created).

4. **MANDATORY:** The public facing system shall have automatic duplicate detection and manage the duplicate such that duplicate reports are tracked, managed, and incorporated and not misreported as separate events.

5. The public facing system shall provide the capability for authorized users to report aggregate Influenza-like Illness (ILI) data. The collected data will be available to MSDH to run reports and export the data to a CSV formatted file.

b. The public facing disease reporting system shall be configurable.

1. The solution shall allow MSDH Communicable Disease administrative staff to determine necessary and required fields, labels, help text, required fields, data entry method, valid formats, and valid value lists.

2. The solution shall allow all changes to the public facing system to be applied as an administration task by authorized Communicable Diseases staff.

c. The public facing disease reporting system shall prefill as much data as is known at each facility when web users create reports using the public facing system.

1. The solution shall allow authorized users to prefill information about facility, staff, and patients previously entered by the facility when creating new reports.

    a. Prefill shall apply to any information that can be anticipated to increase data entry accuracy or data entry volume such as facility name, ordering provider, test type and similar information that can be anticipated.

    b. The solution shall support batch entry. For example, the system might implement uploading a pre-defined spreadsheet template containing patient demographics, filled in by a web user, and uploaded to the IDSP for processing. The Vendor shall propose the solution, the

methodology, and any MSDH required data formats offered by the solution.

2. The solution shall ensure all information available for the facility or previously entered by the facility is prefilled where possible to assist in speedy and accurate data entry.

3. The solution shall allow prefilled data to be achieved using patient information search or other similar means but shall be strictly limited by the user login rules.

58. Interoperability. Describe how the solution achieves each.

Figure X: MSDH Desired Future IDSP Workflow

a. The solution shall provide bi-directional industry standard system interoperability communication protocols specific to secure MSDH's EHR Vendor, Epic.

1. The solution shall support and remain current with the complete HL7 interoperability standards, FHIR standards, as well as MSDH trading partners and, federal EHR reporting requirements at no additional cost to MSDH.

2. The system shall be capable of securely interfacing using Simple Object Access Protocol (SOAP) and Representational state transfer (REST) services. The system must have the ability to provide access to raw HL7
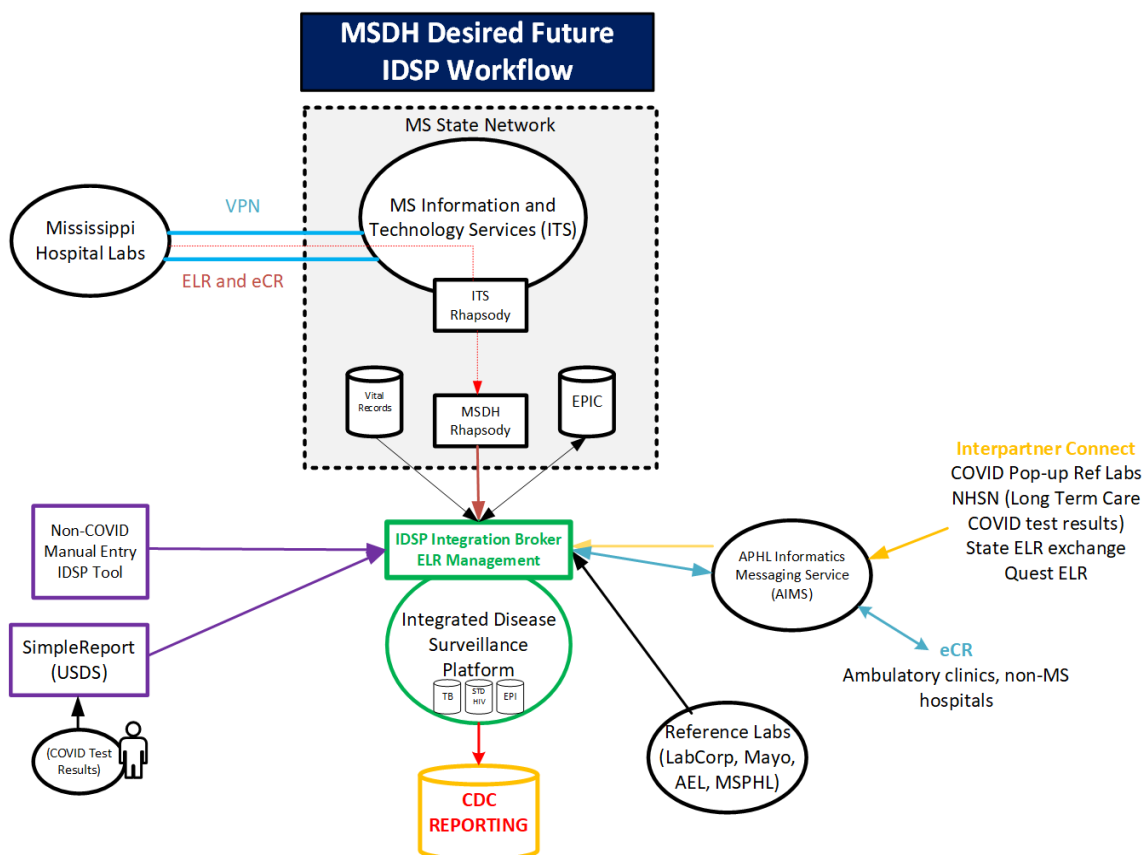
MSDH Desired Future IDSP Workflow

and FHIR messages for MSDH to assist trading partners with identifying message errors.

3. The solution shall have access to the state network via the internet via VPN. Any VPNs will need to terminate on the ITS Enterprise VPN solution.

b. The solution shall have the ability to provide near real-time information sharing with Epic (MSDH Community Connect instance of University of Mississippi Medical Center [UMMC]) EHR. Epic, or the current EHR for MSDH, is intended to remain the system of record for patient health records (clinical records). The ISDP will be the system of record for all surveillance data and perform all federal reporting. Specific details regarding the Epic integration with the IDSP will be detailed in the Interoperability Plan.

c. The solution shall be capable of both requesting health record updates as appropriately needed as well as receiving unsolicited updates from the Epic system that will be ingested into the IDSP solution for MSDH viewing in near real-time based on individual program needs.

   1. MSDH shall have the ability to collect any clinical data that is to be reported to the CDC.
   2. Unsolicited updates will be accepted and applied based on disease condition and may include, but are not limited to, notifications of clinical updates, address updates, demographic updates, etc.

d. The solution shall provide bi-directional industry standard system interoperability communication protocols defined by state and federal partners specific to secure electronic laboratory records.

   1. The solution shall support current ELR/eCR interoperability standards and remain current with industry standards, MSDH trading partners, and federal communicable disease requirements at no additional cost to the agency.
   2. The system shall be capable of securely interfacing with laboratories using SFTP, SOAP, and REST services. Robust HL7 acknowledgements shall be utilized in service responses to address quality issues.

e. The solution shall exchange information with all epidemiological, tuberculosis, and STD/HIV reporting systems, Vital Records, and Public Health Lab and any other relevant systems as identified by MSDH.

   1. The solution shall allow electronic message transfers for all electronic interfaces defined in the integration plan.
   2. The solution shall allow the creation of custom defined input and export file formats.
   3. The solution shall support receiving information from sources utilizing standardized HL7 interface specifications and information in the CSV file format.
   4. The solution shall provide a means to define, change, and incorporate into workflows CSV file formats as a system function for authorized users.
   5. The solution shall support export formats that generate files that can be automatically uploaded to the reporting agency or manually downloaded by a user.
   6. The solution shall support information pulled from other systems (e.g., Epic or any other designated MSDH systems) to be integrated into patient

records and be available to case workers. Such as any clinical data required to be reported to the CDC.

7. The solution shall support information pulled / consolidated from key MSDH systems to support public facing dashboard(s).

f. The solution shall automatically create a case record and investigation upon receipt of ELR/eCR HL7 messages in all cases where there is appropriate data.

g. The solution shall provide a patient level Vaccine Preventable Disease (VPD) query from the IDSP (for all systems (TB, STD/HIV, and EPI)) while the patient is in context, with the state's Immunization Registry (MIIX). Results will be available for the end user to import into the patient's case report.

h. The solution shall provide alerts (e.g., co-infections) for patients in all systems (TB, HIV/STD, and EPI). Alerts (and who will receive them) will be configurable by authorized Communicable Disease users.

i. The IDSP shall receive patient-level notifications from the Vital Records system related to births and/or deaths associated with select communicable diseases. This information can be incorporated into the IDSP record if deemed applicable by the end user.

59. Surveys and Forms

a. The solution shall provide a public facing survey system.

1. The solution shall provide the worker a link to a survey that can be sent electronically to an email address or SMS device.
    a. The solution shall accept multiple email or SMS addresses for bulk sending of survey requests.
2. The solution shall support completed survey results to be collected by the public facing system, be processed, and incorporated into all program survey workflows. Vendor must explain discovery process in detail.
3. The solution surveys must support linking with ongoing epidemiology investigations related to an outbreak or an existing case.

b. The solution shall provide survey generation system allowing workers to generate a custom survey.

1. The solution shall have availability of common survey capabilities such as multiple questions and varied answer modes such as fill in the blank, selection from a list, radio buttons, checkboxes, single choice, multiple choice, etc.
2. The solution shall have the ability to insert logic. Based on response to question, the solution will enable/disable additional questions and can sum values in tables.
3. The solution shall support surveys that can be saved and can be accessed by external individuals through the public facing web portal.

c. The solution shall provide a means for a worker to send a survey link out to email addresses provided by the worker.

1. The solution shall handle sending the survey request to the email address and uses information such as name and explanation provided by the worker and the saved survey selected.

2. The solution shall support maintaining a record of when the survey was sent and who the survey was sent to for a minimum of seven (7) years.

d. The solution shall allow workers to enter a survey on behalf of a recipient.

1. The solutions shall allow a MSDH worker to gather any information through other means necessary to complete the survey but record the results as if the link recipient filled out the survey.

2. Survey results shall be maintained as if the recipient filled out the survey but also track as MSDH worker entered.

e. The solution shall be capable of processing current CDC created forms and remain flexible to support future changes published or recommended by the CDC at no additional cost to MSDH.

1. CDC forms shall be protected and can be replaced by newly published CDC forms or altered by authorized staff based on CDC guidelines.

f. The solution must have the ability for users to search for forms and choose between view, edit, and delete.

g. System administrator shall have the ability to restrict user ability to edit and delete forms based on form type and user role.

h. The system shall be able to import previously created forms in file types as identified by the agency.

1. Forms may be added to forms being created and have the ability for the user to select Append, Replace or Cancel import.

i. The solution shall allow authorized users the ability to create different types of forms (e.g., Supplemental Form, Outbreak Event Form, and Outbreak Summary Form).

j. The solution shall allow for selection of type of form from drop down menu and based on type of form have required fields within the form. User shall receive error message if required field is not included on form.

k. The forms creation screen shall be customizable and user friendly, with the ability to create various sections of a form.

1. The solution shall have the ability to add elements in various form types (e.g., Free Text, Dropdown, Multiselect, Check Box, Core Data Question, Field Sets, Table, Label and Read Only).

l. The solution shall include common validation and advanced properties in forms creation. (e.g., required fields, cell spanning, label location, format (plain text), and max number of characters.)

m. The solution shall have the ability to insert logic. Based on response to question, the solution will enable/disable additional questions and can sum values in tables.

n. The solution shall have the ability for system administrators to see change history and revert changes.

o. The solution shall have the ability to promote the form to production and give alerts to the user if the promotion was successful or not.

p. The solution shall have the ability to link certain form types to an outbreak.

q. The solution shall support the capability for online survey submission by MSDH trading partners. When the online survey submission capability is utilized by a user, an email notification shall be sent by the system to the reporting entity when a survey is successfully submitted.

r. The solution shall have the ability for the user to clear the information entered in the form and revert all populated fields to original state.

s. The solution shall have the ability for the forms data to be exported to a CSV file.

t. The solution shall have the ability for a system user to filter the columns being viewed on the outbreak event line listing screen.

60. Auditing and Security

a. The solution shall provide an external facing, facility centric user management system.

   1. External facilities shall have the ability to register with the agency and independently manage users within their facility that can utilize online reporting.
   2. The external user management system shall follow MSDH user account and password management standards, including multifactor authentication.
   3. Additional security features are optional and can be enumerated.

b. Audit/Log: The Vendor shall provide a solution that is capable of auditing and logging events. Auditing and logging are integrated such that the system cannot take actions and avoid auditing and logging. Solution logging is available for review through various methods such as screens, reports, and Application Programming Interfaces (API)/messaging services.

   1. The proposed solution shall support the ability to audit all solution and component activities, meet federal and state regulations for privacy and, by user or process such as but not limited to:

      a. Additions/Deletions/Edits;
      b. Merges/Unmerges;
      c. Rejected merges;
      d. Logins;
      e. Errors;
      f. Searches;
      g. Exported data / Imported data;
      h. User actions;
      i. Reports run; and
      j. Messages received/sent.

c. The solution shall provide access to system audit data.

1. Audit data shall be the data that tracks all solution activities and can be used to report on success, warnings, and errors/failures.
2. Audit data shall include message warnings and errors, user activity, system events, and the typical logging of successful activities.
3. The solutions shall support users with appropriate program level access. the ability to search, view, filter, and export the logs.
4. Log search criteria shall at a minimum support time, event type, and user. Log exporting supports CSV.

d. The solution's private facing user interface shall provide a Single Sign-On (SSO) experience for MSDH personnel managed by the Department's Azure Active Directory. Azure Active Directory shall be used to manage user authentication and roles establishing user access rights within the solution. The SSO experience also fully supports multi factor authentication (MFA).

e. The solution shall provide role-based security.

1. Users shall have assigned roles that control what can be accessed, viewed, edited, and deleted within the system.
2. The solution shall support security administration for user roles and shall have the ability to hide menu items and screens within the system, can limit data entry fields making them view only by role, and can limit data visibility and editability using record data such as assigned worker or record owner.

61. Data, Data Import/Export, and Data Conversion

a. The Vendor shall import data from multiple legacy systems into the solution. Migration and conversion fees must be included in the Cost Information Submission, Section VII of the RFP.

1. The data import shall convert the legacy data into a homogenous, error checked extract that can be imported into the solution.
2. The Vendor shall be responsible for extracting data from the legacy system. MSDH anticipates providing technical assistance and guidance to Vendor data exports.
3. The Vendor shall work with MSDH and satisfactorily resolve incompatibilities where data is missing, duplicate, bad, or incompatible.
4. The Vendor shall propose a data import strategy that meets the requirement and is complete before implementation.
5. The Vendor shall review MSDH data infrastructure and systems being replaced and work with MSDH to define the data imports that are necessary for the solution and to support MSDH business processes moving forward.

b. The Vendor shall retain records in compliance with state, federal, and MSDH program data retention policies. It is the Vendor's responsibility and due diligence to identify and categorize data to remain within retention policy, which currently has most data retained for seven (7) years.

1. The Vendor shall inform MSDH when it discovers or is required to change or adjust data retention rules.

2. The Vendor shall follow a defined, auditable process, approved by the State, that removes data from the system once it exceeds data retention thresholds.

    c. The solution shall allow exporting of all data to common formats such as CSV and paginated PDF.

      1. The solution shall provide report searches capable of finding information, allowing users to provide demographic, diagnostic factors, and identification (ID) (e.g., Medical Record Number (MRN), lab ID, patient ID, and investigation ID) that limit results.

        a. Users shall be able to determine which date fields the search will be based on (e.g., Event Date, Lab Report Date, etc.).

        b. The solution shall have the ability to export search results and patient and/or case records.

        c. The solution shall provide export flexibility that allows for lists, a limited detail summary, detail, include/exclude components such as lab results and documents, and generate Health Insurance Portability and Accountability Act/Personal Identifiable Information (HIPAA/PII) compliant output.

I. Operational Requirements

62. The Vendor shall deliver, host, implement, maintain, and support the infrastructure and the software for the proposed solution in a Software as a Service (SaaS) offering for the life of the contract.

63. The proposed solution shall be able to:

    a. Receive and provide the appropriate acknowledgement to at least one hundred (100) electronic transactions per second, and

    b. Fully process and make available for worker action at least twenty-five (25) electronic transactions per second.

64. The Vendor shall provide the projected cost analysis over a five (5)-year period for maintenance, enhancements, upgrades, and any associated licensing or data storage fees.

65. The proposed solution shall respond to rapid increases in utilization such as occurs in an epidemic, pandemic, or natural/man-made public health disaster. MSDH may require special capacity elevation which is currently not included as a "routine" process. The special capacity would include the ability for the system to scale based on an unanticipated large influx of cases. Requests for such a process will be given seventy-two (72) hours in advance. The process cycle must be completed within two (2) business days of day requested. Special capacity can revert to "routine" process upon MSDH request.

    a. Vendor shall establish capacity baselines and inform MSDH all areas that are vulnerable to capacity overloading. Nominal values for all capacity areas are communicated to MSDH such that MSDH can make informed capacity change requests.

    b. The solution must be scalable to accommodate growing number of cases at no additional cost to MSDH.

    c. Vendor shall implement special capacity increases within two (2) business days of the day requested.

    d. When the system operates below capacity baselines for more than two (2) calendar days or special capacity increase levels more than two (2) calendar days after the seventy-two (72) hour notification, MSDH shall notify the contractor in the form of a Corrective Action Plan (CAP). The Contractor must respond to the CAP in three (3) business days.

66. All operational aspects, including the location of infrastructure must be in the continental United States of America (USA). All operational resources including help desk must be in the continental USA. Under no circumstances will PHI be moved offshore either for testing purposes or in production (the use of offshore and near-shore resources may be permitted for development efforts only).

67. The proposed solution shall remain current and compliant with HIPAA and NIST 800 standards for data privacy and data security.

68. The Vendor shall be responsible for System Security Plan (SSP) requirements associated with an IDSP.

    a. The SSP shall remain based on the current with NIST 800 updates, compliance from all third party affiliated systems and updates to the SSP for the system and affiliated systems.

    b. The Vendor shall follow the standards and best practices documented in the approved SSP to ensure security for all data and messages.

    c. The Vendor will complete vulnerability tests, penetration tests, and other appropriate audits yearly or upon request.

    d. The Vendor shall provide test and audit report results upon completion or provide the most recent report upon request.

69. The Vendor shall be required to participate in periodic MSDH sponsored security audits throughout the life of the contract.

70. The Vendor shall follow the standards and best practices to ensure security for all data and messages, and perform annual vulnerability tests and penetration tests, and all other, appropriate tests on a regularly scheduled basis, no longer than yearly, on the proposed solution and reporting results to MSDH on a mutually agreed upon schedule (typically monthly).

71. The Vendor shall use Transport Layer Security (TLS) 1.2 or higher if available as a standard and shall upgrade as the standard evolves, at no cost to MSDH.

72. The proposed solution must include the following access control requirements:

    a. Each instance must be equipped to establish role-based security levels based on user profiles;

    b. Each instance shall limit access to PHI and sensitive information based on the role of the user;

    c. Roles will be defined and provisioned to support MSDH workflows for staff, contractors, and other authorized persons, read only roles, and one or more administrative roles;

d. All access to PHI must be recorded and made available for reporting to include Timestamp, content accessed, person accessing, physical location of access with IP address, reason for access and method of access. Demographic data is PHI;

e. Data shall be available to MSDH staff, auditors, and HIPAA reporting/auditing upon request;

f. Data present in all test system/instances is synthetic or simulated using security and privacy best practices unless just cause is provided and approved by MSDH;

g. Each instance must prohibit unauthorized users from accessing PHI and other sensitive information according to state and federal confidentiality rules; and

h. Vendor staff including development and support staff shall use two factor authentications when accessing any aspect of the production application or its data.

i. The proposed solution shall include the following System Support Requirements:

1. The Vendor shall be responsible for the operational aspects of the proposed solution;
2. The Vendor shall be responsible for providing overall MSDH (MSDH staff, as well as support to other Vendor help desks that support MSDH persons) support and help desk services from implementation to termination of the contract. Help desk support shall not preclude creation and delivery of report requests, in an ad hoc fashion or for audit purposes;
3. The Vendor shall provide a toll-free support line for contacting the help desk;
4. The help desk shall be available during MSDH working hours (typically 7:00 a.m. to 7:00 p.m. Central Time Monday through Friday).
5. The Vendor shall keep current all user documentation, support, and train MSDH staff on help desk processes and procedures and provide periodic refresher training. Acceptable training approaches are in-person training, computer-based training, and/or training videos.
6. The Vendor shall provide a secure, Web-based MSDH user support center, including the ability for MSDH staff to report a problem and monitor its status.
7. The Vendor shall document MSDH end-user problems, referring problems to the resources required to resolve the problem, monitor problem resolution, escalate any problems that are not being addressed in a timely manner, and inform the reporting user of problem status.
8. The Vendor shall respond and resolve problems reported within SLA resolution timeframes.
9. The Vendor shall provide weekly reporting of response times, problems encountered, and solutions.
10. The Vendor shall keep the information in the Operations Guide current and accurate for the life of the contract.
11. The Vendor shall keep the information in the System Security Plan (SSP) current and accurate for the life of the contract.

12. The Vendor shall keep the information in the System Turnover Plan current and accurate for the life of the contract.

j. The Vendor shall develop a Software Deployment Plan outlining the approach. The plan shall include the following:

1. The Vendor shall implement and maintain Source Code Version Management and Configuration Control systems for all code, release notes, etc. so that releases can be rolled back;
2. The Vendor shall develop a method for deploying the current code into selected pre-production environment(s) and validating that the code is ready for deployment into the production environment; and
3. The Vendor shall use version control when upgrades are made to any instance.

k. The Vendor shall develop a System Turnover Plan that describes the methodology, schedule, and process for system turnover, detailing how the following specifications will be met:

1. The Vendor shall cooperate with the successor Vendor while providing all required turnover services at no additional costs to MSDH. This shall include meeting with the successor and devising work schedules that are agreeable for both MSDH and the successor Vendor;
2. The Vendor shall transfer solution and services documentation and all data in a mutually agreed format as requested by MSDH and delivered to the successor Vendor or to MSDH to ensure a successful launch; and
3. The Vendor shall turn over all data to MSDH, within a mutually agreed upon timeline. All data shall be properly disposed of after turnover, within a timeframe specified by MSDH according to the executed Business Associate Agreement (BAA) required to be executed at contract signing.

l. Vendor shall describe how the following will be addressed and include the MSDH staff hours/level of involvement necessary, if applicable:

1. Hardware inventory replacement/upgrade;
2. Ensuring Hardware Maintenance Agreements are current;
3. Ensuring Software Licenses are adequate to meet MSDH's needs;
4. Patch schedule; and
5. Technical Infrastructure Changes.

m. The Vendor shall develop a method for diagnosing reported system issues, determining if the issue is a defect, and assigning a MSDH approved severity. Vendor will be responsible for resolving all defects. Resolution timeframe is determined by the severity assignment.

n. The Vendor shall complete system updates as required by new mandates from state and federal legal authorities.

o. The Vendor shall ensure the system remains in compliance with all applicable federal and state rules, regulations, rulings, and policy. The Vendor is responsible for the timely discovery of compliance issues and shall implement system changes such that they can be tested and incorporated into MSDH worker processes prior to production implementation. Compliance is

considered routine system health maintenance covered by the maintenance budget.

p. The Vendor shall maintain known product defects and reported incidents in an appropriate incident tracking system. MSDH staff shall have access to the system to review known incidents, track progress, and provide information.

q. The Vendor shall propose an incident reporting system that allows incidents to be reported by MSDH staff and outside entities. Outside entities interact with the system through electronic reporting and the public facing Web site.

r. The Vendor shall ensure that secure protection, backup, and Disaster Recovery measures are in place and operational as a prerequisite to cutover from the current M&O Vendor to the Vendor's hosting and operations of the production (i.e., for end of Start-Up Period) and for the duration of the contract. The Vendor shall ensure no loss of data or configuration of the environments.

   1. Daily Data backup (incremental snapshots) will complete within twenty-four (24) hours.

s. The Vendor shall maintain and use MSDH approved operations quality assurance procedures, defined in the Operations Guide.

t. User based access related to password or access must be resolved within thirty (30) minutes from time of notification during normal MSDH working hours and within two (2) hours outside normal MSDH working hours.

u. The Vendor(s) Operations Guide shall ensure that:

   1. The Vendor detects and reports PHI data breaches within twenty-four (24) hours of occurrence;
   2. The Vendor begins resolving problems within thirty (30) minutes of initial help desk contact;
   3. The Vendor communicates to end-user / customer administrators within one (1) hour of initial escalation; and
   4. The Vendor contacts end-user/customer administrators with resolution/preventative action taken within eight (8) hours.

73. The Vendor shall develop an Operations Guide describing how the software is configured, integration with MSDH personnel, user management, error reporting, defect management, rule, and parameter changes, change requests, and interoperability with internal and external interfaces as well as external users. The Operations Guide allows the Vendor to demonstrate a mature process, and a robust system, networking, and integration infrastructure. Infrastructure goes beyond cloud offerings to show the Vendor has a robust, flexible, and mature technical solution. The plan establishes the Vendor's methods and procedures for technical infrastructure, and communications protocols during M&O. The guide is intended to remain current and operate as a definitive guide for M&O.

   a. Describe processes used by MSDH and external users to report errors, omissions, and change requests. It includes descriptions of any automated processes, escalation procedures, timeframes, prioritization processes, and any other necessary details.

b. Describe testing environments and testing procedures for all forms of updates. Include MSDH staff roles and responsibilities.

c. Describe the process for reporting and making any form, rule, and parameter changes. Include timeframes, MSDH roles and responsibilities, and other factors necessary to ensure smooth and accurate updates.

d. Describe procedures for changing user roles, changing users, changing passwords, password strength rules, managing multifactor authentication, available user roles, scope of roles, and all other security factors not listed here but present in the solution. Include MSDH roles and responsibilities.

e. Describe process for Vendor discovered errors or planned upgrades, updates, and software maintenance, not directly related to MSDH nor reported by MSDH. Include notification timeframes and notification approach as well as MSDH roles and responsibilities.

f. Describe Vendor procedures for detecting and reporting Private Health Information (PHI) data breaches.

g. Describe the Vendor's help desk, software, reports, help desk contact methods, escalation process, MSDH notification process, operational hours, after hours contact, and all other factors relevant to the Vendor help desk. Include all MSDH roles and responsibilities to ensure smooth problem reporting, prioritization, and resolution.

h. Provide a system Growth Plan (how the Vendor will size the proposed solution initially, address future growth, and address a future epidemic, pandemic, or natural/man-made public health disaster).

   1. Normal growth and flexibility for unusual peak demand as part of standard operations.
   2. Growth over time where the normal system loads grow over time increasing normally daily and peek loads.
   3. Epidemic, pandemic, or natural/man-made public health disaster level growth where normal growth due to widespread outbreak increases long term system utilization to many times normal.

i. Describe the process used to request and receive ad hoc reports. Ad hoc reports can be requested to support special legislative or judicial requests, internal research, auditing, and other not ordinary reporting.

j. Provide the product maintenance schedule and the processes used to manage the schedule, exceptions, emergency releases, and other release management descriptions. This includes product versions, release notes, testing results, opting out of a release, and other release specific information.

   1. Describe how other customer changes are integrated into the MSDH codebase, notifications, testing opportunities, scheduling, and options available to reject or delay changes.

k. Describe the process and procedure for testing during operations. Testing includes subjects such as roles and responsibilities, testing environments, the process for testing mapping rules, testing with partners providing ELR/eCR

data, code promotion between test environments and production, and other subjects related to quality assurance and testing.

1. Provide a clear testing process for onboarding ELR/eCR providers from initial connection through all testing required to ensure proper data mapping, and approval for making the connection live in production.

l. Describe the Service Level Agreements (SLAs), monitoring the SLAs, reports used, and the frequency of status reporting.

m. Business Continuity Plan (BCP): Identification of the core business processes involved in the production solution. The BCP must be included with the Vendor's proposal response. For each core business process include:

1. Identification of potential failures for the process;
2. Risk analysis;
3. Impact analysis;
4. Definition of minimum acceptable levels of service/output;
5. Definition of triggers for activating contingency plans;
6. Procedures for activating any special teams for business continuity;
7. Plan for recovery of business functions, units, processes, human resources, and technology infrastructure: and
8. Communication protocols and process for restoring operations in a timely manner.

n. Disaster Recovery Plan (DRP): Procedures for data backup, restoration, and emergency mode operations in the event of Hardware or Software Failures, Human Error; Natural Disaster; and/or Other unforeseeable emergencies. The DRP must be included with the Vendor's proposal response. Additional Disaster Recovery Plan Topics must include:

1. Retention and storage of backup files and software procedures;
2. Hardware backup for critical solution components procedures;
3. Facility backup procedures;
4. Backup for any telecommunications links and addresses incoming ELR/eCR interfaces, outgoing CDC reporting, manual entry, and any other tools identified and utilized by MSDH;
5. Backup procedures and support to accommodate the loss of any online communications;
6. A detailed file backup plan, procedures, and schedules, including rotation to an off-site storage facility;
7. Describe an off-site storage facility that providing security of the data stored there, including protections against unauthorized access or disclosure of the information, fire, sabotage, and environmental considerations;
8. An enumeration of the prioritized order of restoration for Vendor's proposed solution;
9. Describe providing a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss; and
10. Describe the Vendor's method, process, and content for providing annual Disaster Recovery test results.

o. Narratives addressing the following:

1. Systems Monitoring;
2. Patch Management;
3. Points-of-contact and backups;
4. Technical Support;
5. Health Insurance Portability and Accountability Act (HIPAA) Compliance;
6. Database Replication;
7. Licensing and Warranty Tracking for Hardware and Software;
8. Certificate Expiration Date Tracking; and
9. Other items as mutually agreed upon during discovery.

p. Describe the technical architecture and software that make up the solution. Description is accompanied by technical architecture schematic demonstrating where the hardware and software exist in the product infrastructure.

III. SYSTEM DESIGN

J. System Design Requirements

74. The Vendor shall provide a System Design Document, in a format approved by MSDH, that includes the changes necessary to configuration, workflows, interfaces and integrations, reporting, screens, security, and entities necessary to fulfill all requirements.

75. The Vendor shall provide an entity relationship diagram and data dictionary, in a formal approved by MSDH.

76. The Vendor shall describe all business rules/edit checks that will be used for the solution.

77. The Vendor shall provide a mockup or actual screen designs presented to the appropriate MSDH personnel.

78. The Vendor shall request and incorporate feedback on screen designs from MSDH and implement changes and suggestions into the design.

79. The Vendor shall provide a plan for compatibility and communication to include modular Geographic Information System (GIS) components, the geocoding of all incoming data, the application of geocoded data within the IDSP.

   a. The Vendor shall provide a plan for GIS components, data visualization strategies for different MSDH users (e.g., program managers, case managers, executive management, etc.) and the general public and geocoding for the initial go-live of the solution and a plan of how they will revise and mature the GIS components and geocoding once the solution is operational and additional data has been collected.

   b. The Vendor shall describe the solution's compatibility to receive disease reports through Web-based provider reporting. The plan shall include existing capabilities and reporting methods realized during the COVID-19 pandemic such as Comma-Separated Values (CSV).

   c. The Vendor shall provide a detailed Integration Plan. An Integration Plan describes how the solution becomes a part of the physical environment in which the solution is to become a part or module. It discusses all levels of IDSP integration.

1. The plan includes a complete description of the MSDH and ITS network components, MSDH systems sharing data with the IDSP, external ELR/eCR data partners, reporting to federal and state authorities, and all any other electronic data partner identified during discovery.

2. The plan describes how it will integrate with all identified system, roles and responsibilities, technical approach, risks, assumptions, and constraints.

3. The plan shall consider all types of laboratories that will be sending (reference labs, hospital labs, COVID-19 only pop-up labs, MS PHL, EPIC, and IDSP required systems critical systems such as the immunization registry. This may require the Vendor to perform additional technical specification analysis with other third-party Vendors, MSDH technical personnel and MSDH programmatic personnel.

d. The Vendor shall provide a plan for responding to a surge (outbreak, epidemic, pandemic, or natural/man-made public health disaster) that deals with massive increases in volume, users, processing time, storage, reports, reporting agencies, and cost.

e. The solution shall adhere to all CDC reporting standards when reporting any data to the CDC including data upon request by the CDC or any other Federal Partners.

80. The Vendor shall develop a System Turnover Plan that details the methodology, schedule, and process for system turnover. The plan is implemented at contract conclusion to ensure a smooth transition of system operations and data to a replacement Vendor or contract. The plan must support the plan purpose, transition to a different Vendor, as well as the following.

a. Provide the schedule necessary and overlap expected providing a reasonable path to meet with, scheduling with, export data, import data, review, test, and collaborate such that the successor has access to the Vendor during turnover;

b. Describe the process of transferring user-based documentation and any MSDH specific/derived configurations, rules, and workflows to the successor;

c. Describe how file formats, message formats, mappings, 3rd party integration, import/export procedures and templates developed for MSDH that are not unique to or proprietary to the solution shall be packaged and provided to the successor; and

d. Describe the process and timeline that ensures all MSDH data is purged from the solution, verification process, quality assurance testing, and MSDH staff involvement

IV. IMPLEMENTATION REQUIREMENTS

K. Vendor Acknowledgement

81. This section outlines the MSDH minimum expectations of the awarded Vendor for implementation of the selected solution. Implementation deliverables will reveal the Vendor's expertise in project management, process management and improvement, data migration, and acceptance testing, etc. MSDH expects the proposed preliminary implementation plans to be refined by the awarded Vendor and MSDH 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. MSDH reserves the right to require onsite Vendor participation if it would be in the best interest of MSDH.

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

83. The State expects implementation with limited interruption to incumbent services and business operations. Any interruption to such operations must be approved by MSDH and conducted in a way to prevent loss of service.

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

L. Project Management Requirements

85. The Vendor shall follow industry standard best practices Project Management Institute (PMI), Project Management Body of Knowledge (PMBOK), and the specific project management processes at MSDH. These processes do not dictate how the project mut be managed but demand deliverable standards supporting review and referencing without undue burden or training.

86. The Vendor must follow an Agile Project Management approach and use Microsoft (MS) Project to manage and track project progress and implementation. Vendor shall describe the implementation and scheduling methodology.

87. The Vendor shall prepare a Project Management Plan, maintain the plan throughout the project, and utilize the plan for the comprehensive management of the project. The first draft of the PMP must be included with the proposal response. An updated PMP must be provided after Implementation.

88. The Vendor shall prepare and use a Project Workplan with timelines. The workplan makes clear the activities necessary to implement the requirements and the Vendor will use the plan to demonstrate progress toward implementation. The first draft of the workplan must be included with the proposal response. The plan is updated every two (2) weeks and presented to MSDH management.

    a. The Vendor shall manage a fully resource loaded Project Workplan and is responsible for identifying MSDH resources that are necessary to successfully execute the workplan. The workplan is fully resource loaded assigning named resources to tasks with diligent management preventing over utilization.

    b. The Vendor shall be responsible for identifying and accurately scheduling MSDH tasks and Vendor tasks on the workplan. All activities associated with creating, maintaining, and reporting from the workplan are Vendor's responsibility.

89. The Vendor shall develop Project Artifacts when appropriate in the schedule including responsibility for:

    a. Periodic Progress Reports, as defined by MSDH;

    b. Project Workplan updates every other week;

c. A key project states breakdown with criteria defining success for each;

d. All deliverables and plans described in Section E; and

e. Vendor must provide and realistic sample product Maintenance Schedule with the response to the RFP.

90. The Vendor is responsible for discovery and clarification to ensure it has a clear understanding and interpretation of the requirements, the MSDH environment, interoperability, technical infrastructure, and MSDH policies. Discovery is considered JAD sessions, validation sessions, and working sessions. The following are Vendor responsibilities:

a. Scheduling discovery meetings and sending invites;

b. Providing agendas, diagrams, handouts, prior meeting recaps, parking lot capture; and

c. Notes, JAD Notes, decisions, action items, minutes, and roll.

91. The Vendor shall prepare a Project Workplan with MSDH and Vendor tasks, timelines, MSDH and Vendor resource allocation, integration, testing, data migration, move to production, warranty period, and transition to the new system using the proposed development lifecycle processes. An example will be submitted with the proposal. It contains:

a. Activities required for the project;

b. Sequencing of activities, considering dependencies;

c. Resources assigned to the activities;

d. Durations of the activities; and

e. Timeline schedule

M. Test Plan

92. The Vendor shall produce a plan describing the testing methodology that it will use to produce a product that meets all requirements.

93. The Vendor shall describe the methods and tools used to report, triage, estimate, track, and resolve defects and change requests.

94. The Vendor shall describe the testing methodology used to conduct a holistic system test that culminates in the delivery of a product meeting all MSDH requirements and warranted to be defect free by the Vendor.

a. Provide a clear testing process for onboarding ELR/eCR providers from initial connection through all testing required to ensure proper data mapping, and approval for making the connection live in production.

95. The Vendor shall describe the testing methodology used to conduct a user acceptance test that validates to MSDH that the system meets all MSDH requirements and operates within MSDH infrastructure, meets state and federal requirements, and operates within user workflows to accomplish the IDSP mission.

a. The Vendor shall describe all environments necessary to accomplish testing.

b. The Vendor shall describe all roles and responsibilities related to testing.

c. The Vendor shall provide the following updated documents prior to system or acceptance testing: system test cases, test data sets and scripts (to include ELR and other interoperability functionality), user acceptance test cases and scripts, the execution method, a complete requirements traceability matrix, and testing exit and entrance criteria.

d. The Vendor shall provide periodic (as defined by MSDH) testing status updates designed to show progress against the baseline and evidence the testing progress is adequate to meet schedule expectations.

e. The Vendor shall plan, organize, and manage an MSDH user acceptance testing period. MSDH requires a testing period after system delivery in a pre-production environment (User Acceptance Testing).

96. MSDH plans to review system functionality, ELR workflow, converted data, inter-system interfacing, deduplication, matching and merging functionality and policy compliance within the new system prior to implementation.

97. The Vendor shall provide a holistic system demonstration after System Testing, at the start of UAT. The demonstration will show the system is fully functional, all requirements are implemented, data conversion is complete, and the system does fit state and MSDH policy, security, staff, and external user usage scenarios.

a. The Vendor shall provide a Requirements Traceability Matrix (RTM) at the completion of UAT showing each requirement, the system and UAT testing performed for each requirement, and the testing results.

N. User Training and Documentation

98. The Vendor shall describe their proposed training approach that meets MSDH requirements and achieves adequate user and administration training as per the Vendor's prior experience.

99. The Vendor shall collaborate with the project team to finalize a training plan and schedule. At a minimum, the Vendor should expect to provide specific training for each separate program (EPI, TB, STD/HIV) and the Office of Health Information Technology (OHIT).

100. The Vendor shall provide program and OHIT training to include, but not limited to: adhoc querying, reporting, exporting, data entry, forms creation, Health Level 7 (HL7) messaging, data visualization and analytics capabilities, Fast Healthcare Interoperability Resources (FHIR), and eCR (Electronic Case Reporting) and Electronic Laboratory Reporting (ELR) management, geographical, and disease management, etc.

101. The Vendor shall provide program level, OHIT, and system administrator training. This training will include instructions to, but not limited to: change business rules, user level access and security, alter drop down lists, modify diseases from data entry screens, etc. without the help of a programmer.

102. The Vendor shall provide OHIT training: staff shall be trained to support the system in off-hours or in emergencies, all areas where MSDH staff can interact, quality control, correct, and maintain the Solution when circumstances require such actions.

103. The Vendor shall develop a variety of short, program oriented, how-to sheets for MSDH staff that will encompass all training provided. A final administrator training list will be established by the Vendor with the client once all system capabilities are known.

104. The Vendor shall provide modifiable user documentation to include a user manual, electronic training guides, and training materials for Agency review and approval prior to system implementation.

105. The Vendor shall use a variety of training materials to include but not limited to Computer-Based Training (CBT) solutions, videos, Technical Administrative training, Program Administrative training, user training (train-the-trainer), update training manuals, quick reference guides, and system/version update training.

106. The Vendor shall regularly update user documentation, in a timely manner, training materials, and electronic training guides and materials to support training instruction after each system update or as required.

V. SOFTWARE ADMINISTRATION AND SECURITY

O. General

107. 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.

108. Solution must provide controlled access to features and functions by configurable, role-based permissions as defined by MSDH.

109. Solution must allow the system administrator to set rights for access to data by individual or group.

110. Solution must prevent unauthorized access to the system.

111. Solution must accommodate administrator user rights to any and all workflows and tasks as determined by MSDH.

112. Authorized MSDH staff must be able to restrict specific user groups from being able to view or print certain types of documentation.

113. Roles, security, and access rights must be easily configurable without Contractor assistance.

114. The proposed solution must adhere to all current, relevant security, and privacy standards.

115. 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.

116. Solution must auto terminate sessions after a specified time of inactivity.

117. Solution must accommodate two-factor authentication.

118. The Vendor shall provide a System Security Plan (SSP) that is based on National Institute of Standards and Technology (NIST) 800 standards. The plan must remain

current to NIST 800 changes and list the NIST 800 sections and controls covered in the SSP. The SSP is expected to support periodic audits and shall be structured and revised as necessary to accomplish that purpose. The plan also includes the following:

a. Describe security for the system, contractors, third party products, and affiliated systems;

b. Discuss the schedule, triggers, and responsibilities that ensure the SSP remains current and accurate at all times;

c. Establish the standards and best practices that ensure security for all data and messages specific to protected public health data;

d. Discuss the testing the Vendor will do to quality check the SSP, prepare for audits, and respond to issues detected during audits such as vulnerability tests, penetration tests, and other internal audits

e. Provide a sample or clearly identify the reporting methodology and content used to convey SSP execution results, both successes and failures, the period of reporting, and the reporting showing security issue resolution plans, root cause analysis and successful resolution; and

f. Discuss user security and user management for internal and external users as well as a comprehensive discussion on user account management through Azure Active Directory and the Vendor managed external user management system. This section also includes a description of the two-factor authentication process.

119. The Vendor shall develop a Software Deployment Plan outlining an approach ensuring smooth software management, maintenance, and migration from lower to higher environments such that human error is minimized, and deployment errors can be rolled back. The Vendor is expected to follow and update the standards established in the plan prior to implementation and post implementation. The plan shall include the following:

a. Describe the process used to maintain source code version control and configuration management. This includes describing versioning, finding version numbers, procedures for release notes, code changes procedures, configuration change procedures, rules changes, and workflow change procedures, etc. This includes procedures for rolling back changes to code, configuration, rules, and environments; and

b. Describe how code and configuration changes are deployed to the various environments. This identifies the deployment environment sequencing (e.g., System Test comes before User Acceptance Test), approvals necessary, MSDH involvement, and quality controls that ensure code deployment is appropriate for the environment. Particular attention is expected for production environment deployments.

P. Cloud or Offsite Hosting Requirements

120. Data Ownership: MSDH 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 MSDH User accounts, or MSDH 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 MSDH 's written request.

121. 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 MSDH information at any time. To this end, the Vendor shall safeguard the confidentiality, integrity, and availability of MSDH information and comply with the following conditions:

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

    b. At no time shall any data or processes which either belong to or are intended for the use of MSDH 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 MSDH.

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

123. Encryption

    a. The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism using MSDH approved encryption methodologies and standards which are NIST 800 data in transit encryption standards.

    b. The Vendor must submit encryption methodologies in writing annually for MSDH approval.

    c. 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:

        1. The policy shall be issued by an insurance company acceptable to MSDH and valid for the entire term of the contract, inclusive of any term extension(s).
        2. The Vendor and MSDH shall reach agreement on the level of liability insurance coverage required.
        3. 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.
        4. At a minimum, the policy shall include third party coverage for credit monitoring. notification costs to data breach victims; and regulatory penalties and fines.
        5. 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.

6. The policy shall include a provision requiring that the policy cannot be cancelled without thirty (30) days written notice.
7. The Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.
8. The coverage under the policy shall be primary and not in excess to any other insurance carried by the Vendor.
9. In the event the Vendor fails to always keep in effect the insurance coverage required by this provision, MSDH 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.

124. Breach Notification and Recovery: Unauthorized access or disclosure of non-public data is a security breach. The Vendor will provide immediate notification and all communication shall be coordinated with MSDH. 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 three (3) years, mailing costs, Website, and toll-free telephone call center services. MSDH 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 MSDH to hold a Vendor harmless. All breach and recovery measures shall be in compliance with MSDH policy.

125. Notification of Legal Requests: The Vendor shall contact MSDH 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 MSDH. The Vendor shall not respond to subpoenas, service of process, and other legal requests related to MSDH without first notifying MSDH unless prohibited by law from providing such notice.

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

   a. 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 MSDH data.

   b. 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 MSDH 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 MSDH data and shall thereafter, unless legally prohibited, dispose of all MSDH data in its systems or otherwise in its possession or under its control as specified in section 127(d) below. Within this 90-day timeframe, Vendor will continue to secure and back up MSDH data covered under the contract.

   c. Post-Termination Assistance: MSDH 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.

d. Secure Data Disposal: When requested by MSDH, the provider shall destroy all requested data in all 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 MSDH.

127. 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 MSDH's information among the Vendor's employees and agents.

128. Security Logs and Reports: The Vendor shall allow MSDH 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 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.

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

130. Sub-contractor Disclosure: The Vendor shall identify all 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.

131. 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.

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

133. Operational Metrics: The Vendor and MSDH 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

Q. Additional Requirements

134. ITS acknowledges that the specifications within this RFP are not exhaustive. Rather, they reflect the known requirements that must be met by the proposed system.

Vendors must specify, here, what additional components may be needed and are proposed to complete each configuration.

VI.   SUPPORT AND MAINTENANCE

R. Service Level Agreements

135. System Availability: All Vendors and All Components: The Vendor proposed solution, including all IDSP production instances, shall operate twenty-four (24) hours per day, and support a 99.5% uptime per month, and is subject to a $2,500.00 penalty for each 15-minute occurrence of downtime outside of the 99.5% uptime requirement. Uptime shall be calculated by the following formula:

    a. 24 hours per day x 7 days a week x 52 weeks per year = Total hours per year.

    b. Total hours per year x .005 = Allowed unscheduled downtime per year.

    c. Allowed unscheduled downtime per year / 12 = Uptime per month

    d. Unexpected Downtime Notification: The Contractor must notify MSDH within one (1) hour of any solution system access issues. The Contractor must act with due diligence to re-establish connectivity as soon as possible. Notification must include an estimate of system restoration:

136. Root Cause Report: The Vendor shall provide a Root Cause Analysis (RCA) for all system outages within five (5) business days of the resolution. The report shall describe the root cause of the incident, the actions that resolved the incident, and steps taken to avoid future similar incidents.

137. Scheduled Downtime: Agreed upon and scheduled downtime shall occur only between 1:00 a.m. and 4:00 a.m. Central Time. The Vendor shall be assessed a penalty of $5,000.00 per instance of a failure to notify MSDH in writing forty-eight (48) hours in advance of a scheduled downtime. Solution downtime outside of the allowable downtime period shall be categorized as unscheduled downtime and is subject to a monetary penalty for each occurrence, as is outlined in Item 136.

138. Interface Timeliness: Incoming electronic messages sent from outside systems are processed, stored, and entered on the system workflow/queue/screens or are otherwise ingested and made available to worker(s) or system processing based on the nature of the electronic message within one (1) second. Daily averages exceeding one (1) second shall be assessed damages of $2,500.00 per day. The Vendor shall segregate messages by type for reporting and calculation and any message type speed exceptions must be pre-authorized by MSDH.

139. Transaction Timeliness: User interface (GUI) components of all IDSP instances shall support a two (2) second or less average response time for selected processes measured daily. Averages exceeding three seconds will be considered an outage and the Vendor shall be assessed damages of $2,500.00 per day. Selected processes include:

    a. End-user login;

    b. Single patient/person query and return results; and

    c. Standard report generation (Note: Some reports, including the analytics and population health reports and queries, may take longer than the required two

(2) seconds to generate, and if so, please note in your response what reports these are, what data sets and size are typically included, and the estimated performance for generating these reports).

140. The Vendor shall host the proposed solution in a United States-based Tier 2 data center or better, with written approval from MSDH on any change in the selection of the data center, data center Vendor, and location. MSDH reserves the right to physically audit (by State or State contracted personnel) the data center the proposed solution is hosted in and the Disaster Recovery (DR) site. By the first ninety (90) days after contract execution and on every August 30th thereafter, the Vendor must provide MSDH with an annual data center report, specifying their Tier Certification of Constructed Facility rating or Technology Innovation Agency (TIA)-942 Data Center Standard Rating, specifying the Tier rating of their facility and specifying what certifications have been awarded to the facility, including but not limited to Leadership in Energy and Environmental Design (LEED), Statement on Standards for Attestation (SSAE) 16 (i.e.,. System and Organization Controls [SOC 1], HIPAA, etc. Failure to provide an annual report is subject to a penalty of $10,000 per month until the report is completed and provided to MSDH.

141. Data center-provided servers and network switching equipment used to host the proposed solution shall be no more than three (3) years old, and hardware shall be regularly scheduled for an equipment refresh every three (3) years. Failure to refresh this hardware at least every three (3) years and to notify MSDH in writing as to this refresh is subject to a penalty of $25,000.00 per month until the refresh is complete, and MSDH is notified.

142. Data center where all instances are hosted shall have system intrusion detection, firewalls and firewall policies for cloud servers, regular Operating System (OS) security patches, the most current antivirus software installed, and follow hosting/data center best practices. Upon contract execution, and every quarter thereafter, the Vendor shall provide MSDH a quarterly report detailing how the Vendor and data center are adhering to these requirements. Failure to provide a quarterly report is subject to a penalty of $10,000.00 per month until the report is completed and provided to MSDH.

143. Vendor shall have a failover process and documented Failover Plan that shall be provided to MSDH for approval upon system go-live. Failure to provide the Failover Plan may result in a penalty of $10,000.00 per month until the report is completed and provided to MSDH.

144. Vendor shall have a Disaster Recovery (DR) Plan approved by MSDH upon system go-live, including a separate DR site with a separate physical location from the primary hosting site. Upon each anniversary of contract execution, the Vendor(s) shall provide documentation that the DR environmental test has been conducted within the past year and shall provide written results to MSDH. The written results shall include any remediation and the accompanying remediation schedule necessary to correct any failures or findings that were identified because of the DR test. Failure to provide the results to MSDH on an annual basis is subject to a penalty of $10,000.00 per month until the report is completed and provided to MSDH.

145. Vendor shall execute the DR plan immediately upon notification of a Disaster (as outlined in the DR plan). Upon execution of the DR plan, the proposed solution and

data shall return to at least 70% performance status of the production status. Failure to provide at least 70% performance status of the production status is subject to a penalty of $10,000.00 per month until at least 70% performance status is complete, and documentation is provided to MSDH.

146. Vendor shall support a zero Recovery Point Objective (RPO). Failure to provide zero RPO is subject to a penalty of $10,000.00 per month until a zero RPO is completed, and documentation is provided to MSDH.

147. Vendor and all subcontractors shall adhere to the appropriate SLAs. All subcontractor non-performance and delays are the responsibility of the prime Vendor, and all penalties will be assessed to the prime Vendor.

148. Failure for any Vendor or subcontractor to meet the requirements of the Business Associate Agreement (BAA) ($2,500.00 per occurrence). An occurrence means each failure to comply with the BAA requirements, regardless of the number of persons or clinicians involved.

149. If any Vendor or subcontractor fails to notify MSDH of a breach (potential or otherwise) both in writing and by telephone within twenty-four (24) hours of discovery, the Vendor shall be assessed damages of $10,000.00 per day until MSDH is properly notified. The Vendor shall pay the costs for notification of any breach, as well as for credit monitoring for all persons whose data is breached for the term of one year.

150. Reporting Requirements: Vendor shall provide a monthly report to MSDH by the seventh (7th) business day of the following month. Failure to provide the monthly report by the seventh (7th) working day of the following month, the Vendor shall be assessed a penalty of $2,500 per day until the report is delivered, including:

    a. SLA performance metrics by instance;

    b. Internal monitoring, including metrics and tools used;

    c. Incidents and/or problems incurred per defined SLAs;

    d. Help desk statistics including contacts by users, MSDH staff and beneficiaries, tickets generated and closed by severity, who reported the issue, by instance, escalations, problem resolution rates, opt-in and opt-out requests, and those that were processed;

    e. Total ticket volume with aging by severity, tickets opened and closed during the last period, by support, maintenance, and upgrades;

    f. Monthly hardware statistics and monitoring reports; and

    g. Other metrics to be defined by MSDH in coordination with the Vendor

151. Should any Vendor have more than fifty (50) outstanding service-related Help desk tickets, the Vendor is subject to a penalty of $500.00 per calendar day.

152. Failure by any Vendor to meet mutually agreed upon deliverables and/or milestones by the due date or as otherwise required, may result in a penalty of $500.00 per instance, per calendar day that the deliverable or milestone remains late or deficient.

153. Failure by any Vendor to maintain staffing levels, including the number and qualifications of staff, and provision of key positions that are outlined in the requirements, is subject to a penalty of $2,500.00 per calendar day.

154. Any other failure of any Vendor that MSDH determines constitutes substantial non-compliance with any material term of the Contract not specifically enumerated herein, may result in a penalty of up to $5,000.00 for each failure.

155. Failure by the Vendor to obtain approval in writing by MSDH for publishing material requiring MSDH approval is subject to a penalty of up to $1,000.00 per instance.

156. Unauthorized use of MSDH's name, brand, or likeness is a violation of this contract ($1,000.00 per occurrence). An occurrence means each unauthorized use.

157. Failure of Vendor to comply with close out and turnover requirements may result in the assessment of damages of up to $25,000.00 that, if imposed, shall be deducted from the final payment to be made to Vendor.

158. Unauthorized utilization of any data is a violation of the requirements listen herein ($10,000.00 per occurrence). An occurrence means each unauthorized use, regardless of the number of persons or Trading Partners involved.

159. Failure to meet the requirements of Health Insurance Portability and Accountability Act (HIPAA) ($1,000.00 per occurrence). An occurrence means each improper use or disclosure of person information.

160. Any other failure of Vendor that MSDH determines constitutes substantial non-compliance with any material term of the contract and/or not specifically enumerated herein. (Between $1.00 and $5,000.00 for each failure).

161. The Vendor shall publish on their public Web site any actual or liquidated damages approved by MSDH within fifteen (15) business days of notice of MSDH approval and maintain the document on the site through the contract term.

162. If an SLA measurement yields an SLA credit, the Vendor shall conduct a root cause analysis (RCA). Such root cause analysis shall be provided to MSDH within five (5) business days of the SLA trigger event for MSDH review and acceptance.

163. Operational: All instances and the proposed solution shall adhere to the following table for SLAs and associated penalties (credit to MSDH):

    a. Incident/Problem Resolution Time is calculated from the time an incident/problem is reported, until the problem has been identified as resolved. It is not calculated from when it is entered into a help desk ticketing tool.

    b. The help desk must be staffed appropriately to allow incidents/problems to be entered into the tool while on call with MSDH staff and persons or if received via email within thirty (30) minutes. Each instance of a delay to incident/problem entry, MSDH may assess a $500.00 SLA credit to MSDH.

SLA Name	Definition	Resolution Time
Incident/Problem Resolution Time – Critical, Severity 1	Interruption making a critical functionality inaccessible or a complete network interruption	**98% Resolved in less than 4 hours**

SLA Name	Definition	Resolution Time
	causing a severe impact on services availability. There is no possible alternative.	
Incident/Problem Resolution Time – High, Severity 2	Critical functionality or network access interrupted, degraded or unusable, having a severe impact on services availability. No acceptable alternative is possible.	**98% Resolved in less than 24 hours**
Incident/Problem Resolution Time – Medium, Severity 3	Non-critical function or procedure, unusable or hard to use having an operational impact, but with no direct impact on services availability. A workaround is available.	**98% Resolved in less than 72 hours**
Incident/Problem Resolution Time – Low, Severity 4	Application or personal procedure unusable, where a workaround is available, or a repair is possible.	**98% Resolved in less than 72 hours**

    c. For each incident/problem that does not meet the resolution timeframes above, there shall be an SLA credit to MSDH in the amount of $8,000.00. Every incident and/or problem must be included in the monthly SLA reporting, along with any progress that has been made.

164. Disaster Recovery timeframes: In the event of a Vendor declared disaster rendering all or critical portions of the IDSP unavailable, the recovery time objective is forty-eight (48) hours. The system should be fully operational and available.

    a. The SLA Credits for this Measurement are aggregated, i.e., each lower level of failure adds the stated additional percentage (for a maximum 50% credit at the lowest level).

        1. Greater than forty-eight (48) hours: $16,000.00 SLA Credit to MSDH;
        2. Greater than seventy-two (72) hours: Additional $45,000.00 SLA Credit to MSDH; and
        3. Greater than ninety-six (96) hours: Additional $75,000.00 SLA Credit to MSDH, meaning all three figures above would be credited.
        4. The SLAs set forth herein shall be in effect beginning with the commencement of monthly services. The Vendor(s) shall be responsible for complying with all performance measurements and ensure compliance by all subcontractors.
        5. Beginning on the SLA activation date, any performance measurement not met during the monthly reporting period, the SLA credit for that individual measurement shall be applied to the monthly fees.

    b. Liquidated Damages and Corrective Action Plans

1. MSDH may require corrective action if any deliverable, report, SLA, or the like should indicate that the Vendor is not in compliance with any provision of this RFP. MSDH may also require the modification of any policies or procedures of the Vendor relating to the fulfillment of its obligations pursuant to this Contract. MSDH may issue a deficiency notice and may require a corrective action plan be filed within fifteen (15) calendar days following the date of the notice. A corrective action plan shall delineate the time and way each deficiency is to be corrected. The Corrective Action Plan (CAP) shall be subject to approval by MSDH, which may accept it as submitted, accept it with specified modifications, or reject it. MSDH may extend or reduce the time frame for corrective action depending on the nature of the deficiency and shall be entitled to exercise any other right or remedy available to it, whether it issues a deficiency notice or provides Vendor with the opportunity to take corrective action.

2. Because performance failures by the Vendor may cause MSDH to incur additional administrative costs that are difficult to compute, MSDH may assess liquidated damages against the Vendor pursuant to this section and deduct the amount of the damages from any payments due the Vendor. MSDH, at its sole discretion, may establish an installment deduction plan for any damages. The determination of the number of damages shall be at the sole discretion of MSDH, within the ranges set forth below. Self-reporting by the Vendor will be taken into consideration in determining the number of damages to be assessed. Unless specified otherwise, MSDH shall give written notice to the Vendor of the failure that might result in the assessment of damages and the proposed amount of the damages. The Vendor shall have fifteen (15) calendar days from the date of the notice in which to dispute MSDH's determination. MSDH may assess damages for specific performance failures set forth below. MSDH may assess higher liquidated damages amounts when the Vendor consistently fails to meet specific performance standards and the deficient performance has not been corrected.

3. Assessment of actual or liquidated damages does not waive any other remedies available to MSDH pursuant to this RFP or state and federal law. If liquidated damages are known to be insufficient, then MSDH has the right to pursue actual damages.

4. Failure to timely submit a MSDH approved Corrective Action Plan (CAP), MSDH may assess liquidated damages of $500.00 per business day until the CAP is submitted.

5. Failure to successfully carry out a MSDH approved CAP within the time frames outlined in the CAP, MSDH may assess $500.00 per business day until the CAP is completed.

6. In the event of repeated violations of a single SLA measure or multiple failures across SLA measures over two consecutive months, MSDH reserves the right to renegotiate SLA measures and/or escalate the applicable reductions by 50% of the stated liquidated damages after non-responsiveness. Repeated violations may be grounds for Termination for Cause.

S. Customer Support

165. The Vendor must provide a continual, around the clock, 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.

166. Vendor must provide a toll-free telephone number for MSDH staff to call 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.

167. 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.

168. Vendor must keep the appropriate MSDH management and technical support staff updated on the status of trouble resolution.

169. Vendor agrees to provide adequate training for the effective access and use of support services as requested by the State.

170. Vendor agrees to provide always-updated documentation of all support processes.

T. Issue Tracking

171. The Vendor shall use an industry standard tracking system to thoroughly document issues and requests for MSDH.

172. Describe how operational trouble issues are submitted, prioritized, tracked, and resolved.

173. Describe how software performance issues are submitted, prioritized, tracked, and resolved.

174. Describe how user support issues are requested, prioritized, tracked and resolved.

175. Detail your escalation procedures for responding to trouble tickets, software performance, and user support issues.

176. The Vendor shall provide a customer portal for MSDH to track help desk ticketing and incident resolution.

177. Details of MSDH 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.

178. The Vendor must provide a monthly issue tracking report as defined by MSDH. 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 MSDH.

179. For issue tracking, solution must be capable of on demand as well as auto-run reporting.

U. System Monitoring

180. Vendor must describe their monitoring services to cover all the provided services including but not limited to:

   a. Network connectivity (i.e., whether the network is up or down, and real-time bandwidth usage);

   b. Application monitoring;

   c. Services running on the operating systems;

   d. Performance indicators such as metrics and logs across application resources and technology stacks, database and application servers, operating system, load balancers, network latency, and queues, etc.;

   e. Utilization (e.g., memory, disk usage);

   f. Trending (for minimum of one year); and

   g. Sharing of the monitored data with MSDH through a portal.

181. Vendor must describe how it is alerted to conditions that represent a failure to meet the agreed upon SLA thresholds and how that information will be provided to the State.

V. Processes

182. The Vendor shall have mutually agreed upon processes and policies in place to support MSDH grant management and transit asset management operations.

183. Any modifications to the agreed upon policies and processes must receive prior approval from MSDH.

184. Such processes and policies must be thoroughly documented.

185. Such processes and policies must be reviewed by the Vendor and MSDH at least annually.

W. Product Updates

186. 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.

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

188. Enhancements and updates must be included with annual maintenance fees which must be included in RFP No. 4416, Section VIII Cost Information Submission.

X. Software Updates

189. 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.

190. Vendor agrees that maintenance services will also include maintaining compatibility of the solution software with any and all applicable contractor provided interfaces.

191. 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.

192. 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.

193. 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. Any and all obligations of the third party software are the responsibility of the proposing Vendor. The State will not execute any third party software agreements.

Y. Warranty/Maintenance Requirements

194. The solution must minimize requirements for in-house technical maintenance resources, specialized training, or knowledge in order to implement, configure, update, and/or maintain the system.

195. The Vendor must be capable of providing ongoing maintenance, support, upgrades, and troubleshooting.

196. Vendor must include applicable support fees to include maintenance and hosting to be included in the initial implementation costs.

197. Vendor must be able to provide warranty on the software and system operability for a minimum of one year, beginning on the date of acceptance.

VII. DELIVERABLES

198. Vendor must agree to provide the deliverables described in Table 5 below. So that the State can evaluate Vendor capabilities, proposing Vendor must submit preliminary deliverables as specified with the proposal. Preliminary deliverables should contain as much detail as possible to show compliance with the specific RFP requirements. Post award and prior to implementation, Vendor and MSDH will amend deliverables as appropriate. MSDH approval is required for all deliverables prior to implementation.

Table 5 – Deliverables

Deliverable	Due/Update
Deliverable/Milestone #1 Project Initiation - Project Schedule (JAD Schedule, Milestones, etc.) - Kickoff/Discovery and Project Methodology	Due with proposal; update as necessary;

Deliverable/Milestone #2
- Project Management Plan
  - Scope Management
  - Schedule Management
  - Quality Management
  - System Change Management
  - Configuration Management
  - Communications Management
  - Issues & Risks Management
	Preliminary plan due with proposal; update as necessary;

Deliverable/Milestone #3
- Plans Required for Implementation
  - Requirements Traceability Matrix
  - System Design Document
  - Technical Design Document
  - Web Based Provider Reporting Plan
  - Integration/Interoperability Plan
  - Training Plan
  - Testing Plan
  - GIS Plan
  - Surge Plan
  - Implementation Plan
	Due with proposal; update as necessary;

Deliverable/Milestone #4
- Implementation – Phase I
  - ELR Interface Conversion
    - All Production ELR interfaces converted to the new system
  - Data Migration/Conversion
    - All historical data, user profiles, etc. converted
  - Web Based Provider Reporting Plan
  - Training Plan (Phase 1)
  - All CDC Reporting
  - Integration (Phase 1)
    - Epic, TB Required, etc
  - Alerting/Dashboard Capabilities (Phase 1)
  - Surveys and Forms (Phase 1)
  - Message Mapping Guide Implementation (Phase 1)
  - Post Production Monitoring (Phase 1)
  - Auditing and Security
	Due with proposal; update as necessary;

Deliverable/Milestone #5 - Implementation – Phase II - eCR Capabilities/Initiation	Due upon request;

Table 5 – Deliverables

Deliverable	Due/Update
- GIS Capabilities - Integration (Phase 2) - MIIX, Vital Records, remaining required system integration(s) - Alerting/Dashboard Capabilities (Phase 2) - Surveys and Forms (Phase 2) - Message Mapping Guide Implementation (Phase 2) - New ELR and eCR On-Boarding - Post Production Monitoring (Phase 2) - Training (Phase 2)	
Deliverable/Milestone #6 On-Going Project Management - Semi-Monthly Status Reports - Monthly Office of Communicable Diseases Configuration Control Board Updates - Quarterly MSDH Executive Update - Other Project Management duties as required	Due upon request;
Deliverable/Milestone #7 System Acceptance - Approved Final Deliverable	Due upon request after implementation acceptance

    a. The Vendor shall prepare a Project Management Plan, including but not limited to the components listed below, that will assist in the comprehensive management of the project.

        1. Scope Management;
        2. Schedule Management;
        3. Quality Management;
        4. System Change Management;
        5. Configuration Management;
        6. Communications Management;
        7. Issues & Risks Management;
        8. Assumptions and Constraints;
        9. Testing;
        10. Staffing Plan;
        11. Technical Operations Plan;
        12. Data conversion/Data Import; and
        13. Training.

199. The Vendor shall provide electronic copies of draft and final documentation and deliverables. Electronic copies shall be provided in MS Office format unless otherwise specified or approved by the State.

200. Deliverable Standards: For each required deliverable or group of related deliverables, the awarded Vendor must develop a Deliverable Expectation

Document (DED) in advance of the scheduled start of any tasks or subtasks that produce the deliverable as described above.

201. Approval and Rejection of Deliverables: The awarded Vendor must submit each deliverable to the State for review, comment, and approval. The State's review period varies with the type, complexity, and volume of the deliverable. The Vendor must include adequate estimates for State review, comment, and any Vendor re-work time in the Project Schedule. For the Vendor's estimation purposes, the State's default review period shall be ten (10) business days, unless an alternative review period length is requested in writing.

202. In the event the State finds a deliverable to be unsatisfactory, the State shall notify the awarded Vendor of the reason(s) for deliverable rejection in writing. The State shall meet and confer with the Vendor to provide clarifications as requested or needed. The Vendor must then correct and resubmit the deliverable within agreed timeframes that vary with the type, complexity, and volume of the deliverable. Rejection of a deliverable by the State does not provide permission for delays in delivering subsequent deliverables unless approved by the State.