## Attachment E: Mandatory Specifications

### Submission Requirements

This RFP includes multiple sections that specify proposal submission requirements, including, but not limited to, **1.3 RFP Timeline, 3.11 Proposal Submittal and Instructions,** and **7. Attachments**. The vendor must at least meet all proposal submission requirements as part of this RFP, including, but not limited to, formatting, completeness, timeliness, and accuracy, as described in the sections. Failure to meet any of the submission requirements of this RFP may result in disqualification of a proposal, in accordance with Mandatory Requirements.

Vendors must provide a response to each of the following mandatory requirements. Vendor responses will then be verified by the PRMP to establish and maintain compliance between the PRMP and the HIE vendor. The first section requires initialing and narrative explanation. The second section does not require narrative explanation; however, the vendor must still include and initial these mandatory requirements as part of their proposal.

**Narrative Explanation Required Below According to Response Indication:**

The vendor must provide the right of access to systems, facilities, data, and documentation to the PRMP or its designee to conduct audits and inspections as is necessary.

<Response>

1. The vendor must support the PRMP’s requests for information in response to activities including, but not limited to:
	1. Compliance audits
	2. Investigations
	3. Legislative requests

<Response>

1. The vendor must provide authorization from a parent, affiliate, or subsidiary organization for the PRMP to have access to its records if such a relationship exists that impacts the vendor’s performance under the proposed contract.

<Response>

1. The vendor must help ensure that all applications inclusive of internet, intranet, and extranet associated with this contract are compliant with Section 508 of the Rehabilitation Act of 1973, as amended by 29 United States Code (U.S.C.) §794d, and 36 Code of Federal Regulation (CFR) 1194.21 and 36 CFR 1194.22.

<Response>

1. The vendor must provide increased staffing levels if requirements, timelines, quality, or other standards are not being met, based solely on the discretion of and without additional cost to the PRMP. In making this determination, the PRMP will evaluate whether the vendor is meeting service levels as defined in the contract.

<Response>

1. The vendor must provide evidence that staff have completed and signed all necessary forms prior to executing work for the contract.

<Response>

1. The vendor staff must not have the capability to access, edit, and share personal data, with unauthorized staff, including, but not limited to:
	1. Protected Health Information (PHI)
	2. Personally Identifiable Information (PII)
	3. Financial Transaction Information
	4. Federal Tax Information
	5. Social Security Administration (SSA) data including, but not limited to, family, friends, and acquaintance information

<Response>

1. The vendor must maintain a sufficient staff model to provide the services outlined in the contract while meeting or exceeding the applicable service level agreements.

<Response>

1. On a monthly basis the vendor must, at a minimum, include the standard invoice package contents for the PRMP, including, but not limited to:
	1. An authorized representative of the contracted party must sign an itemized description of services rendered for the invoice period. Additionally, the vendor must include a written certification stating that no officer or employee of the PRMP, its subsidiaries, or affiliates will derive or obtain any benefit or profit of any kind from this vendor’s contract. Invoices that do not include this certification will not be paid.
	2. Provide the PRMP with a list of all services completed within an invoice period, as well as evidence that the PRMP has accepted and approved the work.
	3. Provide the PRMP with three physical and one electronic invoice packages in support of the PRMP’s review and approval of each invoice.
		1. Invoice Package #1 – Original Signature and Hard Copy
		2. Invoice Packages #2 – #3 – Hard Copy
		3. Invoice Package #4 – Electronic

<Response>

1. The vendor must comply with federal Executive Order 11246 related to Equal Employment Opportunity Act, the Clean Air Act, and the Clean Water Act.

<Response>

1. The vendor must provide a drug-free workplace, and individuals must not engage in the unlawful manufacture, distribution, dispensation, possession, abuse, or use of a controlled substance in the performance of the contract. (Drug-Free Workplace Act of 1988)

<Response>

Table 16 details the mandatory requirements that the vendor must include and initial as part of their proposal.

**Table 16: Mandatory Requirements**

| Mandatory Requirement Item(s) | Vendor Meets Requirement? Y/N | Provide a Brief Narrative to Demonstrate Understanding and Fulfillment of Requirement \*Response should note any exceptions to meeting requirement |
| --- | --- | --- |
| The vendor must comply with current and future Puerto Rico and federal regulations as necessary to support the services outlined in this RFP |  | <Response> |
| The vendor must perform according to approved SLAs and associated metrics in the areas listed in Appendix 2: Service-Level Agreements and Performance Standards |  | <Response> |
| The vendor must perform all work associated with this contract within the continental United States (U.S.) or U.S. Territories. |  | <Response> |
| The vendor must serve as a trusted partner to the PRMP and represent the PRMP’s interests in all activities performed under the resulting contract.  |  | <Response> |
| Data Ownership: The vendor must agree that the PRMP retains ownership of all data, procedures, applications, licenses, and materials procured or developed during the contract period. |  | <Response> |
| Security: The vendor must comply with information, data, and cybersecurity requirements as applicable for contractors and vendors doing business with the Commonwealth. Reference agencies and laws include Puerto Rico Innovation and Technology Service (PRITS), the Office of the Chief Government Cybersecurity Officer (within PRITS), Law 75-2019; HIPAA; and Law 151 of June 22, 2004. |  | <Response> |
| Security: The vendor must include an independent security assessment plan aligned with the assessment guidelines in the CMS guidance document for MES certification. If a different framework is proposed for the assessment, the vendor shall ensure that the security assessment plan details how the vendor's framework is mapped to the NIST SP 800-53A framework, MARS-E, or agreed upon security controls framework.* 1. The vendor confirms use of the NIST SP 800-53A framework OR identify the framework proposed and include a mapping of the proposed framework to the NIST SP 800-53A.
	2. Vendor confirms that a security assessment plan will be submitted to be included in a contract if vendor is awarded the RFP.
	3. Vendor commits to annually comply to an independent third-party security risk assessment for the HIE's third parties that transmit, process, or store data under the HIE's contract with PRMP. The vendor shall include the cost of the annual assessment within operating cost.
 |  | <Response> |
| Security: The vendor will provide security-related reports at defined frequencies that align to NIST 800-53a security control requirements, MARS-E, or agreed upon security controls framework.* 1. The vendor confirms they can provide security-related reports. Report topics include:
		1. privileged account review
		2. audit log review
		3. continuous monitoring/security metrics report
		4. Plan Of Action & Milestones (POAM) review
		5. Vulnerability assessment
		6. system access review
		7. roles review for separation of duties
		8. contingency plan review/test
		9. incident response plan review and training
		10. risk assessment; awareness training
		11. review system security plan and update
		12. disaster recovery presentation and review
		13. system wide security assessment
		14. Internal and External Penetration test
		15. static/dynamic code analysis or peer review
		16. HIE governing board security policy review
 |  | <Response> |
| Federal Interoperability Policy Standards: All HIE services will comply with security, privacy, and interoperability policies as listed below. * 1. The vendor confirms that the following identified policies are being followed:
		1. Federal Information Security Management Act (FISMA)
		2. Health Insurance Portability and Accountability Act (HIPAA)
		3. Health Information Technology for economic and Clinical Health Act (HITECH)
		4. Patient Protection and Affordable Care Act
		5. National Security Agency (NSA) Security Recommendation Guides
		6. Office of the National Coordinator for Health Information Technology (ONC) Cures Act Final Rule on Information Blocking
		7. Centers for Medicare and Medicaid Services (CMS) Interoperability and Patient Access Final Rule
		8. Commonwealth regulations regarding privacy and security
		9. TEFCA
 |  | <Response> |
| Security – Hosting: The vendor confirms that hosting services are controlled and managed for access, information exchange, and identity authentication.* 1. The vendor confirms that:
		1. Hosting services have controls in place to prevent unauthorized access, with automated monitoring of service availability and to detect potential intrusions in the production environment
		2. Hosting Services support the exchange of SAML 2.0 (or supported version) security assertions with other systems, including eHealth Exchange and custom attributes. Vendor will use SAML attributes for logging and access control determination decisions
		3. Hosting services support:
		4. OAuth federated authentication for both web services as well as for browsers
		5. OCSP x.509 certificate revocation detection (or supported version)
		6. Other methods of x.509 certification revocation detection
	2. Hosting services will support identity federation standards (SAML, SPML, WS-Federation, etc.) to authenticate and authorize users. The NIST SP 800-63 document suite provides technical requirements for federal agencies implementing digital identity services (4-volume set)
	3. Hosting services will provide strong (multi-factor) authentication options (digital certs, tokens, biometrics, etc.) for user access in keeping with the NIST SP in cited above.
 |  | <Response> |
| Security – Encryption: The vendor confirms that Encryption Services work to ensure that all health information in transit and at rest is unusable, unreadable, or indecipherable to unauthorized individuals through use of a technology or methodology specified by the Secretary of the Federal Department of Health and Human Services in the guidance issued under section 13402 (h)(2) of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5), or any update to that guidance. |  | <Response> |
| Security – Intrusion-Detection and Firewall Protection: The vendor confirms that hosting services will have aggressive intrusion-detection and firewall protection per NIST SP 800-53A Rev 5 SI-04(01) System Monitoring, System-wide intrusion detection systems. |  | <Response> |
| Security – Legal Compliance: The vendor confirms that all HIE services will cooperate completely with the Commonwealth's Chief Information Officer in the detection of any security vulnerability of the hosting infrastructure, reporting any security breach with conformance with PR laws.* 1. The vendor confirms awareness of PR laws and PRITS (Puerto Rico Innovation & Technology Service – the central agency driving technological advancements) policies for detecting and reporting vulnerabilities, including security breaches.
 |  | <Response> |
| Security – Reporting: The vendor must demonstrate that Hosting services will issue ongoing reports regarding HIE security audits and compliance activities in a format and frequency reasonably requested by the Commonwealth. |  | <Response> |
| Security – Security Management: The vendor must demonstrate that industry-standard security management will be implemented and administered by the vendor. |  | <Response> |
| Public Health: The vendor must provide local code mapping to improve the level of accurate reporting of disease reporting to improve population health.* 1. The vendor confirms that when local institutions use their own codes for reporting diseases, which still need to be mapped to industry standards, the HIE will match the reported codes to national standards, improving the accuracy of reports and supporting data aggregation of public health disease reporting data.
 |  | <Response> |
| User Access and Management – User Account Management: The vendor confirms that they provide participants with access to IT Administrative access to manage end-user accounts, submit/edit requests for end-user accounts on their behalf, to alleviate provider burden for account management outside of password requirements.  |  | <Response> |
| User Access and Management – End-User Authentication: The vendor confirms they use Security Assertion Markup Language (SAML) Single-Sign-On (SSO) authentication whereby EHR users can access HIE services efficiently and securely from within their workflow environment.* 1. The vendor confirms support for federated identity management.
	2. The vendor confirms that integration with a variety of EHR system types is in place.
 |  | <Response> |
| User Access and Management – Provider Directory: The vendor must support for provider directory services for individuals and facilities:* 1. The vendor confirms provider Directory support for Direct Secure Messaging.
	2. The vendor confirms that Provider Directory Services associate providers with facilities and health systems.
 |  | <Response> |
| User Access and Management: The vendor must support identity and access management services.* 1. The vendor confirms that identity and access services include user profiles and contact information.
	2. The vendor confirms that identity and access services manage patient-provider attribution.
 |  | <Response> |
| User Access and Management – PRDoH Access: The vendor must confirm that PRDoH personnel will have access to the HIE through the Provider Portal. |  | <Response> |
| The MPI technology solution must be an independent module of the HIE technology architecture. PRMP expects that the PRHIE employs a best-in-class MPI that is accessible to the overall solution and supports Patient Demographic Query, Patient Identifier Cross-Reference, and Cross Community Patient Discovery. |  | <Response> |

### **Mandatory Qualifications**

The vendor must complete this section to demonstrate that it has the experience needed to meet the requirements in this RFP. Table 17 below lists each mandatory qualification. The vendor must note whether it meets the qualification and provide narrative demonstrating fulfillment of the requirement. If multiple vendors are submitting a joint proposal as a response to the RFP, the primary respondent should replicate the table and complete it for each vendor participating in the joint response.

**Table 17: Mandatory Qualifications**

| Mandatory Qualification Item(s) | Vendor Meets Qualification? Y/N | Provide A Brief Narrative to Demonstrate Fulfillment of Requirement |
| --- | --- | --- |
| The technology services described in Section 4.2.2 must be provided by vendor(s) that have experience in health information exchange(s) of similar size and scope as described in this RFP. |  | <Response> |
| The vendor must have the ability to staff the organization and contract with subcontractors to meet PRMP’s HIE program objectives and associated timelines. |  | <Response> |
| The vendor must have demonstrated experience operating and managing health system services including the direct provision of services to the provider community. |  | <Response> |
| The vendor must include at least three references from projects performed within the last two years that demonstrate the vendor’s ability to perform the scope of the work described in this RFP. The vendor must include refences from three different projects/clients that provide details on the vendor’s experience operating and managing a health information exchange or related services. |  | <Response> |
| The vendor must commit to staff and operate a place of business in the Commonwealth during any contract resulting from this procurement process and help ensure local support for outreach and onboarding, HIE participant education, representation on governance bodies, and help desk functions. Operations in Spanish and English are a part of meeting this requirement. |  | <Response> |
| The vendor must agree to meet all federal and local requirements related to the operation of a Medicaid Enterprise system and the management and distribution of private health information.  |  | <Response> |