

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>

SecureHIT, as an accredited entity under the privacy and security rules, has in place the policies and procedures that enable the audit and will 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 to comply with this requirement, in compliance with all applicable requirements.

1. The vendor must support the PRMP's requests for information in response to activities including, but not limited to:
 - a. Compliance audits
 - b. Investigations
 - c. Legislative requests

<Response>

In the event of a required information request (through oral questions, interrogatories, requests for information or documents, subpoena, civil investigation, lawsuit or similar process) that discloses any EHI, SecureHIT will provide written notification to the PRMP who, as a business associate represents a direct relationship for approval and to allow access to all information related to the PRHIE. Taking into consideration all obligations under the HIPAA rules before disclosing EHI for these purposes.

2. 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>

SecureHIT will provide written notification to the PRMP who, as a business partner and there is a direct relationship for approval and to allow any access to all information related to the PRHIE. Taking into consideration all obligations under the HIPAA rules before disclosing EHI for these purposes.

3. 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>

SecureHIT will help ensure that all applications, including the Internet, intranet, and extranet associated with this agreement, comply with Section 508 of the Rehabilitation Act of 1973, as amended by 29 United States Code (U.S.C.) §794d and the Code 36. of Federal Regulation (CFR) 1194.21 and 36 CFR 1194.22.

4. 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>

SecureHIT is committed to providing the highest levels of staffing if requirements, timelines, quality, or other standards are not met, based solely on PRMP criteria and at no additional cost.

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

<Response>

SecureHIT will provide the necessary evidence that staff have completed and signed all necessary forms prior to executing work for the contract. These forms will be requested at the operations kickoff meetings.

6. The vendor staff must not have the capability to access, edit, and share personal data, with unauthorized staff, including, but not limited to:
 - a. Protected Health Information (PHI)
 - b. Personally Identifiable Information (PII)
 - c. Financial Transaction Information

- d. Federal Tax Information
- e. Social Security Administration (SSA) data including, but not limited to, family, friends, and acquaintance information.

<Response>

SecureHIT in compliance with the privacy and security rules, is committed to grant access following the policies and procedures for Access Management approved by PRMP. The proposed policies establish the requirements to follow so that both staff and any other user have minimal access to protected information, according to the responsibilities of the position and will not have the ability to access, edit and share personal data with unauthorized personnel, including, but not limited to. others, as defined in the policies and procedures established as standard in SecureHIT, including, but not limited to:

- a. Protected Health Information (PHI)
 - b. Personally Identifiable Information (PII)
 - c. Financial Transaction Information
 - d. Federal Tax Information
 - e. Social Security Administration (SSA) data including, but not limited to, family, friends, and acquaintance information.
7. 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>

SecureHIT will maintain a sufficient staffing model to provide the services described in the contract while meeting or exceeding applicable service level agreements. Refer to Attachment D - Vendor Organization and Staffing for staffing details.

8. On a monthly basis the vendor must, at a minimum, include the standard invoice package contents for the PRMP, including, but not limited to:
- a. 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.
 - b. 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.
 - c. Provide the PRMP with three physical and one electronic invoice packages in support of the PRMP's review and approval of each invoice.
 - i. Invoice Package #1 – Original Signature and Hard Copy

- ii. Invoice Packages #2 – #3 – Hard Copy
- iii. Invoice Package #4 – Electronic

<Response>

On a monthly basis, SecureHIT will provide, at a minimum, within the standard invoice package for the PRMP, the following, among others:

- a. A detailed description of the services provided during the billing period where an authorized SecureHIT representative will sign and issue for PRMP signature. In addition, SecureHIT will include a written certification that no officer or employee of PRMP, its subsidiaries or affiliates will derive or obtain any benefit or benefit of any kind from this supplier's contract.
 - b. SecureHIT will provide the PRMP with a list of all services completed within the billing period, as well as evidence that the PRMP has accepted and approved the work.
 - c. SecureHIT will provide the PRMP with three physical and one electronic invoice package to support the PRMP's review and approval of each invoice.
 - a. Invoice Package #1: Original Signature and Printed Copy
 - b. Invoice Packages #2 – #3 – Hard Copy
 - c. Invoice package #4: electronic.
9. 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>

SecureHIT will comply with federal Executive Order 11246 related to the Equal Employment Opportunity Act, the Clean Air Act, and the Clean Water Act, as described.







10. 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>


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


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	Y 	As part of SecureHIT's functions the compliance with current and future federal and Puerto Rico regulations is required for accreditations purpose and are in please as necessary to support the services described in this RFP both for accreditation purposes and compliance with federal accreditation bodies and with the PRMP as defined is this RFP. This RFP is defined according to the federal requirements defined by the Office of the National Coordinator (ONC), which are what SecureHIT follows for its federal accreditation.
The vendor must perform according to approved SLAs and associated metrics in the areas listed in Appendix 2: Service-Level Agreements and Performance Standards	Y 	SecureHIT is committed to performing in accordance with approved SLAs and associated metrics in the areas listed in Appendix 2: Service Level Agreements and Performance Standards.
The vendor must perform all work associated with this contract within the continental United States (U.S.) or U.S. Territories.	Y 	All work associated with this contract will be performed by SecureHIT within the continental United States (U.S.) or its territories.
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.	Y 	SecureHIT accepts, to the best of its ability, to act as a trusted partner of the PRMP and to represent the interests of the PRMP in all activities carried out under the resulting contract.
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.	Y 	SecureHIT agrees and understands that PRMP retains ownership of all data, procedures, applications, licenses, and materials acquired or developed during the contract period.
Security: The vendor must comply with information, data, and cybersecurity requirements as applicable for contractors and vendors doing business with the Commonwealth. Reference	Y 	SecureHIT is committed to be in compliance with information, data, and cybersecurity requirements applicable, as requested by all reference agencies and laws include the 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.


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
<p>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.</p>		
<p>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.</p> <ul style="list-style-type: none"> a. 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. b. Vendor confirms that a security assessment plan will be submitted to be included in a contract if vendor is awarded the RFP. c. Vendor commits to annually comply to an independent third-party security risk 	<p>Y</p> 	<p>As part of the Security Awareness Plan, SecureHIT has an independent security assessment plan, delivered by RMComm Company, subcontractor, aligned with the assessment guidelines in the CMS guidance document for MES certification. The detailed security assessment plan is mapped within the supplier framework to the NIST SP 800-53A, MARS-E framework or the agreed upon security controls framework.</p> <ul style="list-style-type: none"> a. SecureHIT confirms the use of the NIST SP 800-53A framework. b. SecureHIT confirms that a security assessment plan included in the contract will be submitted to RMComm if the RFP is awarded. c. SecureHIT commits to annually complying with an independent security risk assessment for HIE third parties that transmit, process or store data under the HIE's contract with PRMP. The costs of the annual evaluation are included in the operating cost.




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
<p>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.</p>		
<p>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.</p> <p>a. The vendor confirms they can provide security-related reports. Report topics include:</p> <ul style="list-style-type: none"> i. privileged account review ii. audit log review iii. continuous monitoring/security metrics report iv. Plan Of Action & Milestones (POAM) review v. Vulnerability assessment vi. system access review vii. roles review for separation of duties viii. contingency plan review/test 	<p>Y</p> 	<p>SecureHIT will provide security-related reporting on defined frequencies that align with NIST 800-53a, MARS-E security control requirements, or agreed-upon security controls framework.</p> <p>SecureHIT confirms that it can provide security-related reports, as required in this RFP.</p>



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
<ul style="list-style-type: none"> ix. incident response plan review and training x. risk assessment; awareness training xi. review system security plan and update xii. disaster recovery presentation and review xiii. system wide security assessment xiv. Internal and External Penetration test xv. static/dynamic code analysis or peer review xvi. HIE governing board security policy review 		
<p>Federal Interoperability Policy Standards: All HIE services will comply with security, privacy, and interoperability policies as listed below.</p> <ul style="list-style-type: none"> a. The vendor confirms that the following identified policies are being followed: <ul style="list-style-type: none"> i. Federal Information Security Management Act (FISMA) ii. Health Insurance Portability and Accountability Act (HIPAA) 	<p>Y</p> 	<p>All HIE services provided by SecureHIT AWS HealthLake will comply with the security, privacy and interoperability policies detailed:</p> <ul style="list-style-type: none"> i. Federal Information Security Management Act (FISMA) ii. Health Insurance Portability and Accountability Act (HIPAA) iii. Health Information Technology for Economic and Clinical Health (HITECH) Act iv. Patient Protection and Affordable Care Act v. National Security Agency (NSA) Security Recommendations Guides saw. vi. Office of the National Coordinator's Health Information Technology Cures (ONC) Act Final Rule on Information Blocking vii. Centers for Medicare and Medicaid Services (CMS) Patient Access and Interoperability Final Rule

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
<ul style="list-style-type: none"> iii. Health Information Technology for economic and Clinical Health Act (HITECH) iv. Patient Protection and Affordable Care Act v. National Security Agency (NSA) Security Recommendation Guides vi. Office of the National Coordinator for Health Information Technology (ONC) Cures Act Final Rule on Information Blocking vii. Centers for Medicare and Medicaid Services (CMS) Interoperability and Patient Access Final Rule viii. Commonwealth regulations regarding privacy and security ix. TEFCA 		<ul style="list-style-type: none"> viii. Commonwealth Privacy and Security Regulations ix. TEFCA
<p>Security – Hosting: The vendor confirms that hosting services are controlled and managed for access, information exchange, and identity authentication.</p> <p>a. The vendor confirms that:</p>	<p style="text-align: center;">Y</p> 	<p>Secure HIT confirms that all hosting services are controlled and managed for access, information exchange and identity authentication.</p> <p>a. SecureHIT confirms that hosting services are controlled and managed for access, information exchange and identity authentication as follows:</p>



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
<ul style="list-style-type: none"> i. 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 ii. 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. iii. Hosting services support: <ul style="list-style-type: none"> i. OAuth federated authentication for both web services as well as for browsers ii. OCSP x.509 certificate revocation detection (or supported version) 		<ul style="list-style-type: none"> i. Hosting services have controls to prevent unauthorized access, with automated monitoring of service availability and to detect possible intrusions in the production environment. ii. Hosting services support the exchange of SAML 2.0 (or compatible version) security assertions with other systems, including eHealth Exchange and custom attributes. The provider will use SAML attributes for access control and logging determination decisions iii. Hosting services support: <ul style="list-style-type: none"> i. OAuth federated authentication for both web services and browsers ii. OCSP x.509 certificate revocation detection (or compatible version)


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
<p>iii. Other methods of x.509 certification revocation detection</p> <p>b. 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)</p> <p>c. 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.</p>		<p>iii. Other x.509 Certification Revocation Detection Methods</p> <p>b. Hosting services will support identity federation standards (SAML, SPML, WS-Federation, etc.) to authenticate and authorize users. NIST SP 800-63 document set provides technical requirements for federal agencies implementing digital identity services (4-volume set)</p> <p>c. Hosting services will provide strong (multi-factor) authentication options (digital certificates, tokens, biometrics, etc.) for user access in accordance with the NIST SP cited above.</p> <p>SecureHIT has in place policies and procedures, that respond to the privacy and security accreditation in compliance with these requirements.</p>
<p>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</p>	<p>Y</p> 	<p>SecureHIT confirms that encryption services are configured to ensure that all health information in transit and at rest is unusable, illegible or indecipherable to unauthorized persons through the 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 updates to that guidance.</p>




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
13402 (h)(2) of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5), or any update to that guidance.		
<p>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.</p>	<p>Y</p> 	<p>SecureHIT has an intrusion detection and firewall protection system, contracted by RMComm: therefore, it is confirmed that the hosting services will have aggressive intrusion detection and firewall protection according to NIST SP 800-53A Rev 5 SI-04(01) Monitoring of the system, system-wide intrusion detection systems.</p>
<p>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.</p> <p>a. 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.</p>	<p>Y</p> 	<p>SecureHIT confirms that all HIE services will co-operate fully with the Commonwealth Chief Information Officer in detecting any security vulnerabilities of the hosting infrastructure, reporting any security breaches in accordance with public relations laws. The Incident Response and Report Plan details the official procedure to follow and SecureHIT employees and contractors are trained for such purposes.</p> <p>a. SecureHIT staff has been trained to work in the application of all the requirements of the public relations laws and policies of the PRITS (Puerto Rico Innovation and Technology Service, the central agency that promotes technological advances) to detect and report vulnerabilities , including security breaches, and we are committed to integrating PRHIE operations under the same rules required by PRITS.</p>
<p>Security – Reporting: The vendor must demonstrate that Hosting services will issue ongoing reports regarding HIE</p>	<p>Y</p> 	<p>The security monitoring system worked by SecureHIT provides adjustable reports at the frequency required by the Commonwealth and will be delivered.</p>

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
security audits and compliance activities in a format and frequency reasonably requested by the Commonwealth.		The monitoring platform is used to analyze network traffic, operating systems Event Logs, and other security events, helping organizations improve network security and protect their customers. It solves security challenges related to device and software visibility, monitoring for anomalous events, and ensuring patch management.
<p>Security – Security Management: The vendor must demonstrate that industry-standard security management will be implemented and administered by the vendor.</p>	<p>Y</p> 	<p>SecureHIT is a Health Information Service Provider (HISP) accredited by Direct Trust under privacy and security since 2018, we are the only one with presence native in Puerto Rico. This accreditation guarantees participation within the Direct Trust Federated Directory in all States of the United States and its Territories allowing us to exchange health information. Refer to this link for accreditation registry https://accreditation.directtrust.org/accredited-organization-detail?orgid=0011O000024fNpwQAE</p> <p>DirectTrust Accredited Health Information Service Providers (HISPs) are entities that have demonstrated best practices, met HIPAA, privacy, and security compliance standards, and validated policy requirements. By becoming accredited, organizations can prove clinical data interoperability with other accredited entities, avoid one-off agreements with others, and can become part of the DirectTrust Accredited Trust Anchor Bundle to participate in the national network for Direct Secure Messaging. https://www.credly.com/org/directtrust/badge/directtrust-accredited-hisp</p> <p>Also, to maintain these accreditations, all the platforms and tools that SecureHIT uses proposed in this RFP comply with the strictest privacy and security requirements.</p>
<p>Public Health: The vendor must provide local code mapping to improve the level of accurate reporting of disease reporting to improve population health.</p>	<p>Y</p> 	<p>SecureHIT, using AWS HealthLake, will provide an engine integration tools that natively support and integrate the most common healthcare systems and standards, but we also have a development division as part of PRHIE operations that integrates developers who know the healthcare sector from Puerto Rico and with more than 15 years of experience in the local health</p>

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
<p>a. 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.</p>		<p>sector and its characteristics that can address the needs of local code mapping to improve the level of accurate notification of diseases to improve the health of the population, allowing you to choose between drag and drop creation or advanced scripting to meet your needs.</p> <p>For HIE technologies, SecureHIT is a regulated and accredited entity under the Privacy and Security standards by Direct Trust, as an accreditation body, we currently have the following technical solutions launched by the ONC/CMS, which are SecureHIT Direct Messaging version 6 to perform Direct Secure Messaging and AWS HealthLake for all Commonwell, Carequality, eHealth Exchange and all FHIR transactions. These platforms are completely managed by SecureHIT as the sole integrators of this technology and as part of the services provided to the PRHIE. It runs or resides in the Amazon Web Services (AWS) infrastructure, which has a SOC Report Type II where it guarantees the management of the privacy and security of this infrastructure. These connectors, as provided by ONC/CMS itself, meet the requirements of the different communication networks under the Qualified Health Information Network (QHIN) for the PRHIE. Direct Secure Messaging provides an event notification service (ENS) and these notifications are managed by the SecureHITDirect Messaging infrastructure. Amazon Web Service (AWS) offers infrastructure as a service (IaaS) services for data storage, master data management, security, interface engine, machine learning and analytics. Agreement management, access management, and user service are managed from Zoho Service Center Plus, a help desk platform. It is also a licensing tool that resides on SecureHIT IaaS under the same security and privacy conditions. SecureHIT will transform unstructured data using specialized machine learning (ML) models – using HealthLake that provides integrated medical natural language processing (NLP) using Amazon Comprehend Medical. Raw medical text data is transformed using specialized machine learning models. These models at HealthLake have been trained to understand and extract meaningful insights from unstructured healthcare data.</p>

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
		<p>SecureHIT will supports the requirements listed above:</p> <ul style="list-style-type: none"> • Data from disparate sources; AWS HealthLake has the ability to receive data, in different formats • Translation terminologies; SecureHIT can receive structured data and unstructured data, analyzing the data using Natural Language Processing and Ontology Mapping <p>In this way SecureHIT confirms that when local institutions use their own codes to report diseases or as defined by the Public Health agency according to local characteristics, which must still correspond to industry standards, the HIE will match the reported codes with national standards, improving reporting accuracy and supporting public health disease reporting data aggregation.</p>
<p>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.</p>	<p>Y</p> 	<p>SecureHIT confirms that it will provide relevant and security-compliant access management to participants with IT administrative access to manage end-user accounts, submit/edit end-user account requests on their behalf, to alleviate the burden of provider for external account management of password requirements within your participating organization as a Trusted Agent after having completed an Identity Verification that meets the corresponding Level of Assurance, according to the access requested.</p> <p>Secure HIT confirms that all hosting services are controlled and managed for access, information exchange and identity authentication</p>
<p>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</p>	<p>Y</p> 	<p>Security Assertion Markup Language (SAML) single sign-on (SSO) authentication will be used through which EHR users can access HIE services efficiently and securely from their integrated workflow environment. the use of the corresponding application program interface (API), whether by FHIR, Jason Restful, or as required by the Direct Trust, Commonwell or Carequality federated networks.</p> <p>Therefore;</p>


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
<p>within their workflow environment.</p> <ul style="list-style-type: none"> a. The vendor confirms support for federated identity management. b. The vendor confirms that integration with a variety of EHR system types is in place. 		<ul style="list-style-type: none"> a. SecureHIT confirms support for federated identity management. SecureHIT confirms that it will provide relevant and security-compliant access management to participants with IT administrative access to manage end-user accounts, submit/edit end-user account requests on their behalf, to alleviate the burden of provider for external account management of password requirements within your participating organization as a Trusted Agent after having completed an Identity Verification that meets the corresponding Level of Assurance, according to the access requested. b. SecureHIT confirms that there is integration using APIs with a variety of types of EHR systems.
<p>User Access and Management – Provider Directory: The vendor must support for provider directory services for individuals and facilities:</p> <ul style="list-style-type: none"> a. The vendor confirms provider Directory support for Direct Secure Messaging. b. The vendor confirms that Provider Directory Services associate providers with facilities and health systems. 	<p>Y</p> 	<p>SecureHIT within the first quarter of the project guarantees the creation of a provider directory for Direct Secure Messaging by immediately establishing the Direct Healthcare Provider Directory for both individuals and organizations that permits the HIE nationwide using DirectTrust Federated Networks and a FHIR Provider Directory inserted in the longitudinal EHR using AWS HealthLake:</p> <p>Therefore;</p> <ul style="list-style-type: none"> a. SecureHIT is an accredited HISP within the Direct Trust Directory Federated nationally in all the States of the United States and its Territories that include Puerto Rico, inserting health providers into the national information exchange within the provider directory with Direct Secure Messaging. b. SecureHIT will coordinate with PRMP the method to be used to associate providers with health facilities and systems within the Provider Directory Services and will ensure a uniform and official structure by the Puerto Rico Department of Health.



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
<p>User Access and Management: The vendor must support identity and access management services.</p> <p>a. The vendor confirms that identity and access services include user profiles and contact information.</p> <p>b. The vendor confirms that identity and access services manage patient-provider attribution.</p>	<p>Y</p> 	<p>User access and management:</p> <p>As part of the standard operations procedures established as PRHIE Operator, all user access management and their consent and validation of identity authentication will be worked in detail and documented.</p> <p>Therefore;</p> <p>a. SecureHIT confirms that as part of the PRHIE Operator's Standard Operating Procedures, identity and access services include user profiles and contact information.</p> <p>b. SecureHIT confirms that identity and access services manage patient-provider attribution.</p>
<p>User Access and Management – PRDoH Access: The vendor must confirm that PRDoH personnel will have access to the HIE through the Provider Portal.</p>	<p>Y</p> 	<p>SecureHIT will provide PRDoH access for PRDoH personnel to access the HIE through the Provider Portal, as defined by the PRMP and PRDoH, and will be documented within standard (SoP) access management procedure.</p>
<p>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.</p>	<p>Y</p> 	<p>The Rhapsody EMPI technological solution is an independent module of the HIE technological architecture and will be managed by the Health Information Management (HIM) Division defined within the SecureHIT organizational structure and following que data quality criteria. SecureHIT is committed to using a best-in-class MPI that offers the guarantees that federal accreditations offer in the provision of the service so that it is accessible as a general solution and supports patient demographic query, patient identifier cross-reference and patient discovery across communities.</p>


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
<p>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.</p>	<p>Y</p> 	<p>SecureHIT as PRHIE Operator, has more than 6 years of experience with presence in Puerto Rico accredited by Direct Trust to do Health Information Exchange, in addition to successfully participating in the beta exercise for the Trusted Network Accreditation Program (TNAP) under the Electronic Health Network Accreditation Commission now Direct Trust as one of the first 6 companies accredited as TNAP. The resources proposed in these operations have more than 15 years of experience in the health sector, as presented in Attachment C - Vendor Qualifications and Experience.</p> <p>Scientia, Inc. as a business associate subcontracted by SecureHIT to work on integrations with Meditech, the management of Health Information Management and Master Patient Index (MPI) has vast experience having worked on the implementations and integrations of more than 23 hospitals in Puerto Rico for more than 15 years. For more details, please refer to Attachment C - Vendor Qualifications and Experience.</p>

Mandatory Qualification Item(s)	Vendor Meets Qualification? Y/N	Provide A Brief Narrative to Demonstrate Fulfillment of Requirement
		<p>AWS HealthLake proposed to manage the Longitudinal EHR and Rhapsody EMPI as MPI solution has the capabilities and accreditations that guarantees being able to demonstrate compliance with this requirement.</p> <p>In addition, case studies and experiences worked in other states for this same HIE solution are presented. For more details, please refer to Attachment C - Vendor Qualifications and Experience.</p>
<p>The vendor must have the ability to staff the organization and contract with subcontractors to meet PRMP's HIE program objectives and associated timelines.</p>	<p>Y</p> 	<p>SecureHIT and Scientia and RMComm as subcontractors, have the necessary staffing capacity to meet PRMP HIE program objectives and associated timelines. As described in Attachment D - Vendor Organization and Staffing.</p>
<p>The vendor must have demonstrated experience operating and managing health system services including the direct provision of services to the provider community.</p>	<p>Y</p> 	<p>Since it began operations, SecureHIT has provided health information exchange services for more than 20 health providers in Puerto Rico, integrating this background technology for multiple systems such as Meditech, Evolution, Cerner, among other systems. This secure messaging technology and FHIR background technology using AWS HealthLake and Rhapsody EMPI, in addition to being integrated into different systems such as EHR and others, also provides a service portal to the end user. The provision of these services directly to the end user will be managed through the customer service division that</p>

Mandatory Qualification Item(s)	Vendor Meets Qualification? Y/N	Provide A Brief Narrative to Demonstrate Fulfillment of Requirement
		<p>operates 24 hours a day, 7 days a week. For more details, please refer to Attachment C - Vendor Qualifications and Experience.</p> <p>Scientia</p> <p>RMComm</p>
<p>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 references from three different projects/clients that provide details on the vendor's experience operating and managing a health information exchange or related services.</p>	<p>Y</p> 	<p>SecureHIT - three references from projects completed within the last two years that demonstrate the vendor's ability to perform the scope of work described in this RFP.</p> <p>IPPlus - Mr. Leonardo Nivar Glandalf Cay Bolivar Pagan Direct Trust Scott Stuewe - President</p> <p>One of Scientia</p> <p>SecureHIT - references from three different projects/clients that provide details on the provider's experience operating and managing a health information exchange or related services.</p> <p>Caribbean Medical Center Hospital Mr. Joel Nieves</p>

Mandatory Qualification Item(s)	Vendor Meets Qualification? Y/N	Provide A Brief Narrative to Demonstrate Fulfillment of Requirement
		<p>Damas Hospital Mr. Javier Negron</p> <p>Hato Rey Pathology Labs Mr. Santos Vega</p>
<p>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.</p>	<p>Y</p> 	<p>SecureHIT is committed to staffing and will operate a place of business in the Commonwealth during any contract resulting from this procurement process and will provide local support for outreach and onboarding, education of HIE participants, representation on governing bodies, governance and help desk functions, as described in the SoW description. Operations will be available in Spanish and English.</p>
<p>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.</p>	<p>Y</p> 	<p>SecureHIT agrees to comply with all federal and local requirements related to the operation of a Medicaid enterprise system and the management and distribution of private health information, as defined by the PRMP.</p>

