Attachment G: Response to SOW
Approach to Business Operations

This project entails the implementation of the technological and operational infrastructure for the exchange of health information in Puerto Rico as an entity designated by the state to promote national interoperability and support sustainable and effective Medicaid operations. The objective of this project pursues four aspects designed by the Institute for Health Care Improvement, to focus health system improvements on the execution of a holistic approach that considers the patient experience, health outcomes, reduction of healthcare costs, care and improving staff experiences. As an added value, SecureHIT and its contractors have resources that have been in HealthIT for more than 20 years, specifically in the health sector in Puerto Rico.

Full details of the scope of this work are included in the attached documents, but in general terms this project will address all PRHIE operations to serve patients, health providers, participants, insurers, the Puerto Rico Department of Health (PRDoH) and the Puerto Rico Medicaid Program (PRMP) and the implementation of the technology necessary to carry out health information exchange (HIE) that achieves the Outcomes-Based Certification (OBC) Reporting and Support Plan certification will involve the following; governance, Service Level Agreements (SLA), policies and procedures, agreement management, customer service, quality assurance and reporting for the operational part. The technological part will include; data access, data quality, Infrastructure as a Service (IaaS) for longitudinal EHR and Enterprise Master Patient Index (EMPI), interfaces, service portals, Direct Secure Messaging, Event Notifications compliance, the State Healthcare Provider Directory, Public Health compliance by data capture and reporting, PRMP Data Service and Emergency Response Service.

Recognizing the challenges that this HIE project represents for the last years, according to the response in the document 2024-PRMP-MES-HIE-001_Vendor_QA, both the size of the databases and their quality are unknown, we suggest for approval of the PRMP that the first phase of this project, comprising the 1 year of the contract, achieve the following goals:

- Phase 1
  - 1st Quarter
    - Enable PRHIE operations
    - Creation of Master Patient Index (MPI)
    - Enable a longitudinal EHR
      - Patient Portal
      - Provider Portal
      - Participant Portal
      - Payer Portal
    - Enable interoperability capabilities that guarantee participant attestation
    - Enable filters and alerts to manage data quality
  - 2nd Quarter
    - Outreach and Adoption
    - Connect the necessary % of participants doing HIE
    - PRMP MMIS/MES HIE service
    - PRDoH data capture and reporting service
    - Assessment of existing databases
    - EMPI and Data Quality Assurance
    - Reporting
  - 3rd and 4th Quarters
    - Outreach and Adoption
    - EMPI and Data Quality Assurance
    - Reporting
    - Certify MMIS under CMS
- Phase 2 (2nd year contract)
  - 1st Quarter
    - OBC certification
  - 2nd Quarter
    - Legacy data assessment
    - Implementation assessment
    - Legacy databases migration and conversion
      - PRMP
      - Health Gorilla
      - Any other data base required by PRMP or PRDoH
    - Data Quality
      - Assessment
      - Review of the codes in the programming current operational data quality to adjust them to the newly migrated data.
      - Data stabilization and sanitization

The responses below define the work plan for the first year to address the 1st phase (12 months).

Business Operations

Governance

SecureHIT as PRHIE operator becomes a member or participant of the PRHIE Advisory Council and will assume as part of its essential functions to stay informed about the needs, experiences and objectives of the community and inform planning with operational and technical expertise. The Project Director, the subject matter expert, will be assigned to work as a liaison between the PRHIE Board of Governors, the PRMP, the PRHIE Advisory Council, and the broader healthcare community. SecureHIT ensures through the assignment of a subject matter expert, meaning the Project Director, who will be fully integrated into the collaboration with key HIE stakeholders to identify and promote

meaningful use cases for continuity of care in the Commonwealth. The Project Coordinator in coordination with the Project Director will be the herein defined role of engagement manager, as an individual to be a liaison with PRMP and participate in governance activities. It is confirmed that this function will be supported by technical, operational and financial resources as necessary to address issues that arise as the HIE progresses.

Data Governance

SecureHIT will be responsible for all business operations related to HIE services, personnel operations, customer management (i.e. data senders/participants, interested parties, etc.), subcontractors and the contracts necessary to execute the requirements of this SOW. All business operations, including policies, will be in compliance with federal and Commonwealth laws, which are applicable to HIE and protected health information (PHI). SecureHIT will implement Amazon Web Service - AWS HealthLake as the Longitudinal EHR, which has been developed for strict compliance with the requirements and laws of the ONC and CMS, refer to the link for more details; https://aws.amazon.com/about-aws/whats-new/2023/06/amazon-healthlake-interoperability-related-onc-cms-patient-access-rules/

SecureHIT takes responsibility for managing staff to achieve HIE objectives set by the Commonwealth. Refer to Attachment D - Vendor Organization and Staffing for staffing details. SecureHIT's Customer Service Division will maintain and track of the status of current participant agreements and the AWS HealthLake/Rhapsody EMPI will keep track for patient consent information in accordance with the aforementioned laws and governing body oversight as described above. Additionally, SecureHIT will maintain standard operating procedures (SOP) for all operations identified as essential to business operations. The Sensitive Data Audit report will show the number of unique users accessing sensitive data by unique patient, by facility, with confirmation of consent noted. This element requires reporting as defined in the Attachment F - Outcome Traceability Matrix and will be reported through the dashboard. A secure public website will be maintained that provides a transparent representation of PRHIE operations, including data management and sharing policies, service information, participant information, leadership contacts, support information and contacts, user consent information. patient and contacts for patients with questions. It should be defined in more detail with the PRMP to clearly establish the requirements of this request.

Policy

SecureHIT will provide and be responsible for all operational policies governing all services in this SOW. As part of the project's initial exercises, the draft Security Awareness Program will be presented for evaluation as the parent policy manual for the PRHIE and work will be done to establish final operating policies for PRMP review and approval. Among the first policies that will be reviewed and submitted for PRMP approval are the documentation policy and the policy establishing the policy as a standard procedure. Once approved by PRMP, all policies will be forwarded for final approval by the PRMP-assigned entity, as required by Commonwealth compliance, where all relevant policies (including participation agreements) will be transparently communicated to stakeholders. participants, the commonwealth, and key stakeholders. As defined in this RFP, HIE policies will be publicly available upon approval, posted on the PRHIE public website or as defined and decided by the PRMP. As required in this RFP, all participation agreements will be approved by PRMP and may represent relevant Department of Health data sharing policies. SecureHIT ensures that this will occur and will include a process to notify affected parties of relevant policy updates. The notification procedure could include training, as part of the Standard Operating Procedures (SOP) for the onboarding and continuity of improvements to the services provided by the infrastructure. Simultaneously with the development of the policies, the Service Level Agreements (SLA) will be worked on for due approval, documentation, programming in the customer service system, monitoring, and execution.

Technical Assistance and Customer Service

The Customer Service Division will help the user in its first level of help and levels 2 and 3 will be attended to in the Technical Support Division depending on their complexity, they may be passed on as a problem to the Development and Infrastructure Division to address and resolve. any situation presented by healthcare providers to connect, transition, and maintain real-time connections to the HIE by participants. Services will include initial and ongoing technical support for interfaces, data specifications and data capture, in partnership with EHR vendors, as appropriate. These 3 divisions will provide 24/7 services. Each intervention or service request will be documented, this applies to all service divisions.

The Customer Service Policy establishes the means to receive service calls, whether by telephone, email, service portal, in person, in writing or traditional mail and that all service requests must be initially submitted to the Customer Service Division. Customer. All service requests will reach the Customer Service Division for an initial level 1 evaluation where simple situations are resolved. If the situation cannot be resolved at tier 1, it is escalated to the Technical Support Division (care level 2 or 3) subject to the complexity of the request. If it is a problem that impacts a group of users and cannot be resolved in the Technical Support Division, it is raised to level 4 and must be addressed by the Development and Infrastructure Division. The Customer Service Policy also establishes service level agreements. This policy, like any other, will be approved by the PRMP and will be the metric for the provision of services. The customer service management tool will provide service quality dashboards and reports for service quality and will be presented on dashboard as scheduled. As part of the operational services, SecureHIT will subcontract Scientia for the Health Information Management Division and they will be in charge of all quality management on the Participant Onboarding, Longitudinal EHR and EMPI.

SecureHIT will provide the following;

- Technical support for resolving problems with HIE users
- Support for participants and issues from the participant's EHR provider related to maintaining connections to the HIE and its supporting infrastructure.
- Onboarding trainings
- Manual trainings
- Any teaching point to enhance the user or participant experience
- Troubleshooting support

- Complete management of service requests until the problem is resolved
- Any other action required for problem solving

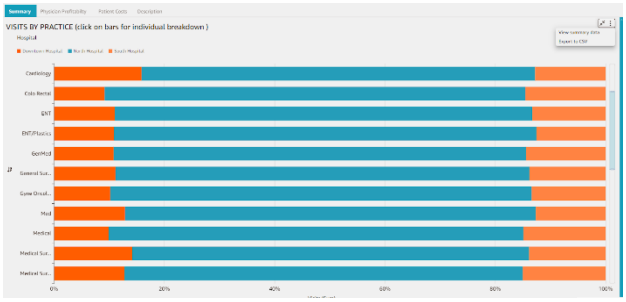
SecureHIT will respond to all customer support request in accordance with the SLAs as approved by the PRMP. SecureHIT will provide help desk statistics upon PRMP request. The SecureHIT Customer Service Division will support end users with onboarding and ongoing training in addition to any requirement as established in the training plan as approved by the PRMP. Additionally, on-demand training or support resources will be provided to help users learn how to use the portal, including, but not limited to, resources that can be accessed in emergency situations where time for training is limited and speed is needed. and task orientation. Onboarding and training statistics will be included in operational reports. Planned onboarding and training activities, including, but not limited to, personnel, policies and procedures, and measurable expectations for onboarding and training to be provided annually will be outlined and submitted for approval to the PRMP.

Operational Reporting and SLAs

SecureHIT proposes AWS HealthLake (AHL) as a longitudinal EHR solution, which is a HIPAA-eligible service that provides full access to individual and patient population health data through transactions based on FHIR (Fast Healthcare Interoperable Resources) API to store and securely transform your data into a petabyte-scale queryable format and further analyze this data using machine learning (ML) models. Using HealthLake FHIR-based APIs, SecureHIT will be able to easily import large volumes of health data, including medical reports or patient notes, from on-premises systems into a secure, compliant service. HealthLake offers integrated natural language processing (NLP) models that will allow to understand and extract meaningful medical information from a single copy of raw health data, such as medications, procedures, and diagnoses, including the characteristics that the Puerto Rico health sector has in its medical terminology. To describe the process by which data from operational reports would be collected and reported, SecureHIT, using HealthLake, will generat the necessary reports to successfully satisfy the reports requested below and allows the creation of all those required by us using the technologies included in this tool. SecureHIT will record and monitor resources in real time. To deliver customizable reports, SecureHIT will be capturing API calls and related events made by or on behalf of PRHIE. Through monthly operational reports (as a minimum communication standard), SecureHIT will clearly and consistently communicate the status of all functionalities on the exchange and the status of HIE operations relevant to the achievement of the intended results of the PRHIE. Monthly operational reports will include, among others:

Operational Report	Planned Operational Reports Delivery
Data source connections by organization type, regional locations, and MPI crossover rates.	Real Time Dashboard
Status of the entire clinical data repository and interfaces, including MPI, ongoing implementation, and remediation activities.	Real Time Dashboard
Data quality remediation efforts by data source and level of impact on the end-user community; In the initial meetings, the quality criteria of the data packages that will be received will be defined, approved by the PRMP. These criteria will be configured within HealthLake for Data Integrity and Verification.	Real Time Dashboard
Data Quality Alert capabilities: Programming will be developed to configure the necessary alerts and report to the participant the status of their package, that is, whether it was received correctly or if it does not meet the quality control criteria. This minimizes errors in the data consumed in the database, guaranteeing clean data and allows the PRHIE to certify the compliance of each participant.	Real Time Dashboard
Quality Assurance: The HIM Division will oversee this matter from the initial phase (participant adoption) and in the second phase of migration, conversion, and sanitization of existing data, as required by PRMP and PRDoH. Among the data packages to be reviewed, we will begin with the data packages required for compliance and attestation with CMS for Promoting Interoperability 3 (PI3) and any report that is required by public health (PRDoH).	Real Time Dashboard
Functionality of central systems represented as HIE technical architecture; A fully customizable dashboard will be presented at a HIE technical (as defined by PRMP) level to monitor the central architecture at the operations level.	Real Time Dashboard
Partnership activities, such as identifying new use cases, participating in state governing bodies, or contributing to community health IT activities; SecureHIT will participate in partnership activities, participate in state governing bodies, or contribute to community health IT activities where it may present or identify new use cases and present in a monthly basis executive report, by the Project Coordinator.	Monthly report, By the Project Coordinator
Status of outcomes-based services (care coordination, event notification, public health, and emergency response); In coordination with the Office of Public Health Response Preparation and Coordination (OPCRS-Bioseguridad) and all other PRDoH identified offices, the necessary data will be able to establish surveillance dashboards as required.	Real Time Dashboard
Results-based certification status; In the kickoff meetings, the criteria required to achieve certification must be established and the strengths necessary to work on the delivery methodology must be identified. Dashboard or report will be provided as required.	Real Time Dashboard or monthly report as defined by PRMP
Any other reported data and statistics indicated as performance standards associated with specific results and requirements in the RFP, as defined by the PRMP; SecureHIT has the analysis capacity using HealthLake, which will facilitate the PRHIE to query, visualize and create machine learning models from its data collected at the PRHIE in almost real time. Eliminating the need for them to execute complex data exports and transformations. Therefore, any other requested report or statistical data may be worked on for delivery within the corresponding parameters as agreed between the parties.	Real Time Dashboard or monthly report as defined by PRMP

Examples
To minimize space consumption in this document we have added live links that in will take you to different examples of dashboards that can be created HealthLake.
https://d2lzvqq4w5ulk4.cloudfront.net/?dashboardName=healthcare
https://democentral.learnquicksight.online/#Dashboard-DashboardDemo-Population-Health-Demo



Technology Architecture and Vendor Partnerships

For HIE technologies, SecureHIT is a regulated and accredited entity under the Privacy and Security standards by Direct Trust and a candidate for HiTrust accreditation, as an accreditation body. SecureHIT currently have the following technical solutions launched for ONC/CMS, which are Direct SecureHIT Messaging version 6 to perform Direct Secure Messaging and AWS HealthLake for all Commonwell, Carequality, eHealth Exchange and all FHIR transactions and Rhapsody EMPI to manage the Enterprise Master Patient Index and generate the required Unique Patient Identifier. 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 will provide the compliance for send and receive referrals, event notification service (ENS), provider directory service and other service and these services are managed by the Direct SecureHIT Messaging infrastructure. Amazon Web Service (AWS) is the Infrastructure as a service (IaaS) services for data storage, master data management, security, interface engine, machine learning and analytics. Agreement management, access management, and customer service are managed from Zoho Service Center Plus, as a help desk platform. 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.

SecureHIT will supports the requirements listed above:

- 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
- Access controls; Secure HIT confirms that all hosting services are controlled and managed for access, information exchange and identity authentication
- Use cases; can use HealthLake for the following healthcare applications - Population health management, Improving quality of care and Optimizing hospital efficiency
- Public health reporting and Medicaid operations; SecureHIT's HealthLake can accelerate data exchange and meet ONC and CMS interoperability and patient access rules

SecureHIT will comply with all established policies that guarantee systems and data management to protect the privacy and security of local patients' health information.

Business Associates Subcontractors: The following contracts are established to address the areas described above, all of them are working under agreements as business associates, as required by HIPAA:

1. Scientia Inc. for health information management (HIM) and Master Patient Index (MPI)
2. RMComm for 24/7 cybersecurity monitoring services
3. Rhapsody
4. Amazon Web Services

Approach to Technical Services

Enterprise Identity Services

1. SecureHIT will use state of the art Artificial Intelligence (AI) and machine learning to process and store meaningful Health data to contribute and promote the interoperability using federated networks like Commonwell, Carequality, DirectTrust and Qualified Health Information Network (QHIN) via FHIR API. SecureHIT proposes the use of all ONC interoperability EHR integrated tools that promote interoperability and the HIM Division will work the Quality Assurance (QA) to guarantee the quality of the data.

2. SecureHIT will provide healthcare providers with access to an integrated HIE longitudinal EHR service integrated into the provider's EHR if they have it to improve clinical decision making across care teams by providing access to real-time integrated health records through the PRHIE. Healthcare providers who do not have an EHR to integrate will be provided access to the provider portal, ensuring that providers have access to an external HIE medical records service. To generate the required reports, as part of the standardization of the data sets, the fields payer, healthcare provider/organization, and HIE participant must be required. In the data quality, a validation must be made to verify that this data is in the packet being received. The packet will be passed through NLP and ML algorithms to ensure the minimum data requirement or otherwise the transfer must be logged and rejected for correction. This should be part of a report that identifies HIE participants who are not complying with data policies and requirements to ensure compliance. Using Rhapsody EMPI technology SecureHIT will match, link, and aggregate records across disparate data sources to ensure the PRHIE provides a unique longitudinal health record for each person who receives care from PRHIE participants. With HealthLake, SecureHIT as a PRHIE operator will be able to normalize and store health data from disparate raw data sources into an FHIR data warehouse and leverage HealthLake FHIR-based APIs to create interactive applications and interoperability workflows. We will thus be responsible for transforming local patient identifiers to meet HIE specifications for interoperable exchange. This element requires reporting as defined in the Attachment F - Outcome Traceability Matrix and will be reported through the dashboard.
3. SecureHIT will provide a record location service to regional and national data sharing networks as expected by current national data sharing standards and policies using Rhapsody EMPI technology to improve PRMP beneficiaries' quality and experience of care when they receive care outside of Puerto Rico. This EMPI will improve the accuracy of patient data by linking records between systems. In addition, it will guarantee unique patient records in all Commonwell, Carequality and eHealth Exchange networks inside and outside Puerto Rico. SecureHIT uses a tool designed to be flexible enough for any patient information it contains. It is designed to facilitate real-time data exchange. With the integration of this tool, SecureHIT will help improve the physician experience, accelerate onboarding time after M&A, and help providers address specific engagement initiatives. Providing a 360° view of every person across disparate systems, a clear line between historical and site data, and optional data management help improve patient and clinician experiences. Rhapsody EMPI will carry the number of unique individuals/registrations, the number/rate of unlinked incoming registrations in the MPI monthly by incoming source, with a rolling cumulative total. Through the development of algorithms or programming, the number of merger operations per reporting (D01) period will be recorded from MPI records with addresses in Puerto Rico; MPI records by state address, center of origin, patient care overlap rate by facility (when a patient is cared for at more than one facility). By integrating this technology into HealthLake, it will be possible to bring reports or dashboards on the number of death indicators reversed per time, the number of regional and national HIE networks to which the HIE product is connected, the volume of data shared between the PR HIE and each network. (per network), as defined by the PRMP. This element requires reporting as defined in the Attachment F - Outcome Traceability Matrix and will be reported through the dashboard.
4. SecureHIT uses Rhapsody EMPI as the enterprise master patient index management tool, which is a standalone module of AWS HealthLake as the longitudinal EHR and HIE technology architecture. Rhapsody EMPI is described as a tool designed to be the best-tested Enterprise Master Persona Index (EMPI) designed to facilitate real-time data sharing. Rhapsody EMPI has the required certifications, including HealthIT ONC CEHRT. This EMPI is accessible to the overall solution and supports patient demographic queries, patient identifier cross-references, and cross-community patient discovery as required by ONC Interoperability Standards: Patient ID Sharing within and outside the community. Secure HIT will implement controls and identify consent options in databases to facilitate patient opt-out so that their health information is not exchanged with another HIE. This increases the patient's ability to control their own Health Information. Through the Patient Portal, the ability will be enabled so that the patient can section at any time whether they wish to exchange information or do not authorize it, and this interacts in real time with the databases and the authorization of the exchange of health information. This will provide the metric for the percentage of the MPI data set that is marked as an opt-out record, based on the opt-out decisions made by the patient. Through Rhapsody EMPI we will collect the number of unique patients who decide not to participate, the total unique number of patients and we will be able to represent the percentage of those who have decided not to participate. This element requires reporting as defined in the Attachment F - Outcome Traceability Matrix and will be reported through the dashboard.
5. Interface Specifications - SecureHIT will work to maintain and improve data interface specifications and control protocols that guide participating institutions in transmitting local data to the HIE. The interface specifications must be based on the required ONC standards. The SecureHIT Customer Service Division will oversee effectively communicating the data exchange specifications to participants, in addition to the PRHIE website that will allow access to enable this communication continuously. The interfaces that receive the health information packages will be configured to monitor quality criteria as required by the measures established by CMS for Promoting Interoperability and any other fields required by PRMP and PRDoH. The Health Information Management (HIM) Division will work in a timely manner and identify transmission errors. If necessary, the HIM Division (QA) and the Development and Infrastructure Division will correct transmission errors. During the implementation phases, participants will be trained based on the policies and procedures established for the HIE (as approved by the PRMP and the PRDoH) and the quality of the data to be sent. The data quality criteria, after approval by the PRMP and the PRDoH, will be configured to make data integrity evaluations on each information packet received. If the required criteria are not met, the package will be rejected. An acknowledgement message will inform the participant if their data was accepted or not so they can correct it. This programming in the system will generate a report per participant indicating the % of packages sent with significant data and how many not. It is recommended to establish a threshold for compliance by PRMP for data quality attestation. To maintain and improve the data interface specifications and control protocols that will guide participating institutions in transmitting local data to the HIE, strict use of interface specifications based on the standards required by the ONC will be in place as policy. This policy will be officially implemented as PRHIE Operator to all HIE participants as a requirement for compliance with the quality

criteria. It will be part of the review and compliance process required of each participant as a participation criterion. The “Check Sum” exercise and the quality review process of the delivered data packages will be audited both by the HIM Division and electronically programmatically and a report will be provided that identifies the participant who is below % compliance. HIE Participants who are not in compliance will be identified monthly to take corrective action measures, through education, or correct technical errors if applicable. It is suggested that as part of the quality measures, the HIE participant who is below the % compliance level be issued a report of non-compliance with the quality metrics, therefore identifying him as non-compliant for attestation with CMS.

Care Coordination Services

SecureHIT has the capacity and proposes with all its efforts in this RFP to connect 100% of the almost 65,000 health providers in Puerto Rico to enable in its simplest phase the Coordination of Health Services sending and receiving data for care management of the health of PRMP beneficiaries. By providing a SecureHIT Direct account to do DSM, the healthcare provider, including those who do not have an EHR, will be able to securely receive the ENS and implement the Closing the Referral Loop Workflow. This will be worked on during 1Q. SecureHIT will provide end users with real-time access to longitudinal medical records in the clinical data repository and MPI using the following tools;

- Providers portal
- Patient Portal
- Participants Portal
- Payers Portal
- API
- HL7 FHIR R4
- EHR integrated data access workflows and any other similar services currently provided and/or plans for the provision of these services in Puerto Rico
- Direct SecureHIT Secure Messaging (DSM)
    - Direct secure messaging portal (regardless of whether or not the provider has an EHR) the health provider will be able to send and receive service notification alerts and any direct information exchange.
    - Direct XDR API for EHR Integration
    - Direct Messaging API for EHR Integration
    - Integration into the EHR with Direct Secure Messaging, with event notifications.

All these services will be available to support care coordination in real-time clinical workflows. SecureHIT will be able to provide a report for 100% of participants with this service available, the connection is aligned with SLA 002 uptime standards. This element requires reporting as defined in the Attachment F - Outcome Traceability Matrix and will be reported through the dashboard.

Data Quality and Reporting Services

SecureHIT will provide automated support processes, meaning programming within HealthLake in each receipt of the participants' information package where it executes the validation of the quality criteria defined by CMS in Promoting Interoperability and PRMP/PRDoH. The HIM Division will manually work through quality criteria to identify and mitigate data quality issues that may impact the usability and reliability of medical records in the HIE. SecureHIT is committed to delivering a high level of data quality. The configuration of the standards and criteria that will be established suggesting the rules published by the ONC for compliance with Promoting Interoperability, thus the data integrity process for all data sources (data contributor) will guarantee compliance with these standards and the requirements defined by the PRMP and public health. At the development level, automated support processes (check sums) will be established. The HIM Division will define a manual quality review to identify and mitigate data quality issues that may impact the usability and reliability of medical records in the HIE.

To establish transparent communication of data quality standards and processes to mitigate data quality issues with the data source, SecureHIT will publish, is necessary, policies and procedures, interface documentation, official memoranda, mandates and bylaws officers as approved by the PRMP and the PRDoH by the following means;

- PRHIE official website
- Emails
- Collaborators bulletin boards
- Educational sessions such as Hospital Association, HIMSS PR, FQHC, among others.

In addition, the Customer Service Division and HIM Division will reinforce the participant, through training, participant assistance sessions and common training sessions if necessary.

CMS Promoting Interoperability 3 defines the fields required for compliance in the delivery of data packets (click the link for details). Initially all these criteria will be taken as part of quality compliance. The eCQMs also define the quality criteria in the reporting of the indicators, these will also be part of the quality programming for the packages that are received. In meetings with the PRMP and PRDoH, any other required fields must be identified to be configured in the HealthLake coding that receives the data packets and passes the first quality filter.

SecureHIT will establish the quality criteria taking into consideration the requirements of CMS, PRMP and PRDoH and develop these filters that raise alerts within the programming code. This exercise will trigger an acknowledgement message to the participant informing them that they did not pass the quality criteria, in real time, which means, the automatic checksum services will deliver a response message in case of error indicating what the error is to the participant (sender). Additionally, this exercise will allow us to have direct monitoring of the participants in their execution, measuring the number of packages sent and how many of them meet the quality criteria. With the approval of the PRMP,

thresholds will be established that outline compliance values. A report will be generated monthly where the level of compliance will be identified. It refers to training or programming participants who are in non-compliance for the corresponding action and bringing it to compliance. Description: Recording data quality issues with existing healthcare organizations participating in bi-directional data sharing connections specific to encounters, diagnosis coding, data related to clinical quality measurement. SecureHIT will maintain a record of data quality issues with existing healthcare organizations participating in two-way connections to share encounter-specific data, diagnosis coding, and data related to clinical quality measurement through the HealthLake platform and will be delivered periodically (as defined by the PRMP).

Once the data packet is received from HealthLake, the programming will check the data quality and mark the transaction as pass or fail. This generates a log of data quality problems for all bidirectional connections. These reports will be referred to the HIM Division in conjunction with the Development and Infrastructure Division to re-evaluate the content manually and identify whether it is a human management situation or a programming correction. The Customer Service Division will follow up with the participant through a service request on the customer service platform. This allows you to work on the monitoring progress in a documented manner and generate reports as required by PRMP. Results from both platforms will be delivered periodically (as defined by the PRMP); HealthLake for error reports in the electronic transaction and participant follow-up reports by the Customer Service Division to share quality results and participant behavior to the PRMP. All HIE participant data will be passed through NLP and ML algorithms to map terminology and ontology codes such as CPT, ICD10, LOINC, RXNORM to validate them according to the standards. To improve patient safety and privacy by safeguarding "sensitive" data in HIE health records, AWS HealthLake will record the number of facilities and/or providers that provide sensitive data to demonstrates that users use this feature and will provide the aggregate number of data sets/types by facility provider categorized as sensitive will demonstrates that required flagging is occurring. This element requires reports as defined in the Results Traceability Matrix in Attachment F, seeking to meet the objective that 100% of participants have this service available and will be reported through the dashboard.

SecureHIT recognize the challenge in Puerto Rico of the use of Spanish in local HL7 terminology, for these purposes, given that all HIE participating data will be passed through NLP and ML algorithms to map terminology and ontology codes such as CPT, ICD10, LOINC, RXNORM to validate them according to the standards we will also use Natural Language Processing (NLP) to work on this reality. It continues to be a challenge because the standardization of terminology is required to maintain parameters and trends, but the issue will be worked on with advances in artificial intelligence to maintain the quality of data for reporting and analysis. Using the HealthLake integrated medical natural language processing (NLP) capabilities, SecureHIT can analyze unstructured clinical text from diverse sources. HealthLake transforms unstructured data using natural language processing models and provides powerful query and search capabilities. HealthLake can be used to organize, index, and structure patient information in a way that is secure, compliant, and can be audited.

Application Programming Interface (API) Services

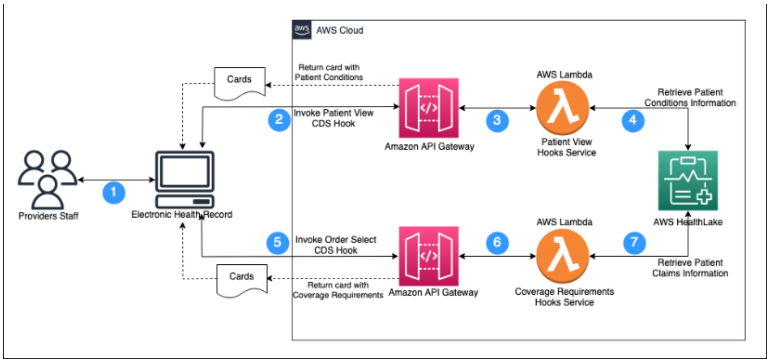
In AWS HealthLake, SecureHIT will use Fast Healthcare Interoperability Resources (FHIR) REST API operations to manage and search resources in your HealthLake data store. Through this platform you can use the FHIR REST API operations to perform create, read, update and delete (CRUD) operations on resources in a data warehouse. You can also form complex search strings using HTTP GET or POST requests. HealthLake supports a subset of FHIR-supported lookup operations. These new capabilities, combined with existing Amazon Healthlake APIs, will help EHRs, and any other systems, enable healthcare organizations to quickly create applications that conform to ONC and CMS patient access rules. https://aws.amazon.com/about-aws/whats-new/2023/06/amazon-healthlake-interoperability-related-onc-cms-patient-access-rules/

Supported operations for: Current FHIR API capabilities and FHIR API capabilities in development.

Operation	**Description**
Read	Read the current state of a resource
Update	Update a resource by its ID (or create it if it's new)
Delete	Delete a resource
Create	Create a new resource with a server-assigned ID
Search	Search the resource type based on filter criteria
Capabilities	Get a capability statement for the system

The measures of API activity will be using AWS CloudTrail integrated to HealthLake as a bulti-in component. This feature protects the PRHIE from penalties using logs to prove compliance with regulations such as SOC, PCI, and HIPAA. This tool is responsible for monitoring events and activities of the FHIR endpoint, and the API design approach will be using the HL7 FHIR Release 4 version as approved by the ONC. The technical specifications for access and use of the API will be using SMART on FHIR, providing all the authentication requirements as established in this RFP.

a. Demonstration of API functionality in production use
   i. HealthLake API Demonstration, see the graph on the right side.
   ii. Direct SecureHIT Provider Portal API demo https://api.direct.securehit.net/direct_mail/



iii. SecureHIT Viewer API demo https://api.direct.securehit.net/ccd_viewer/

b. Technical documentation for third-party API users, including security and deployment protocols, same as HealthLake Demonstration graphic.
c. Statistics related to API message volumes, will presented by report
d. The API metrics HIE operational reporting will be delivered in a dashboard

Public Health Reporting

The main objective of this proposal is to enable capable interoperability capabilities in ONC Certified EHRs as required by federal regulations and maximize the investment in Promoting Interoperability for HIEs available to facilitate adoption in Puerto Rico and all states. SecureHIT will coordinate aligned federal and local public health interoperability requirements and mandates for Medicare innovation programs and initiatives. And will support healthcare providers and the Department of Health in meeting public health management reporting obligations both at the state and federal levels and at the federal policy level through the Customer Service Division, Technical Support and HIM by continuous training, manuals (update and delivery) and monitoring. SecureHIT will use the AWS HealthLake platform to maintain existing electronic laboratory reporting (ELR) data streams for state epidemiology representatives and the COVID-19 registry. Meetings will be established with public health representatives from the Department of Health to identify the HIE method to automate the collection and aggregation of public health reporting data sets, including immunizations, syndromic surveillance, vital statistics, and other use cases evolving from community and federal partners. Once the data packages and electronic integration have been identified through FHIR API, Direct Secure Messaging, or Jason API for sending and receiving information from public health entities as a method to receive laboratory reports and surveillance information as designed and provided from the HealthLake platform we can manage the number of electronic laboratory reporting messages (ELR standard) captured in the HIE and transmitted to Public Health. In addition, the number of syndromic surveillance messages (Syndromic Surveillance Standard) captured in the HIE and transmitted to Public Health. To achieve the target of 100% of ELR/syndromic surveillance messages from providers capable of sending are provided to the Commonwealth. This element requires reporting as defined in the Attachment F - Outcome Traceability Matrix and will be reported through the dashboard.

To obtain certification of institutions regarding compliance with CMS requirements that promote interoperability and local public health reporting, SecureHIT will establish health information exchange requirements for participation within the PRHIE network synchronized with the compliance requirements and be able to carry out compliance monitoring, using all tools and configurations in accordance with the Promotion of Interoperability. We can always also attend to those systems or participants that do not meet these requirements or do not need to meet them, in those cases where it is necessary. Once they begin to send and receive using the Promoting Interoperability 3 and eCQM tools, HealthLake will be able to count the packages received satisfactorily with the quality parameters and reject them for non-compliance and generate a monitoring report for the documentation of each attestation.

By enabling the capabilities so that the PRHIE can send and receive health information using all the tools provided by the Promote Interoperability and eCQM rule, it will allow the exchange of health information to occur with minimal effort on the part of providers. SecureHIT will offer the necessary services to serve those health providers who do not yet have technologies that can respond to the requirement, providing direct assistance to those needs and access using the portal. SecureHIT will start conversations to identify the needs of PRDoH in the required divisions for compliance to address and facilitate, if necessary, the development of applications or interfaces that allow them to receive information electronically and in real time to satisfy the needs of public health. HealthLake allows to receive information from disparate sources, with structured and unstructured data, increasing the opportunity to satisfy the different PRDoH systems with their different needs. It is understood that PRIR has a system that is enabled to receive structured data. Connecting HealthLake to this system will allow PRIR to receive vaccination information as designed and intended and bring the number of Vaccination Messages (VXU) provided by the HIE to the Vaccination Registry. It is hoped to meet the target of 100% of VXU messages from capable providers being provided to the Commonwealth. This element requires reporting as defined in the Attachment F - Outcome Traceability Matrix and will be reported through the dashboard.

Medicaid Services

SecureHIT could stream structured data to a PRMP data store periodically using the HealthLake (FHIR) REST API. If necessary due to incompatibility problems with the PRMP data store, specific APIs will be developed, as necessary. Daily data updates will be provided with the possibility of near real-time updates in the future, similar to those seen in the attached link; https://democentral.learnquicksight.online/#Dashboard-DashboardDemo-Population-Health-Demo. Typical data contents will include identity, attribution relationships, clinical information, and ADT information. It will be necessary to define in meetings with PRMP the necessary data to be able to generate the requested reports, then to the extent that the corresponding data is being received. SecureHIT will maintain a data repository to provide data visualization services and accessible reports for a variety of users from PRDoH. These visualizations and/or reports, depending on the request, will respond to the needs foreseen in this RFP, but are not limited to these because HealthLake provides open capacity for the development of dashboards, visualizations and reports adjustable to the need of the service. SecureHIT will address its efforts to both healthcare providers and the Department of Health to meet public health management reporting obligations at both the state and federal policy levels. HealthLake provides open capacity for the development of dashboards, visualizations and reports adjustable to the needs of the service used. Here we share how AWS HealthLake Analytics supports Athena SQL queries on HealthLake data that enables users to analyze without needing to export the data. With Amazon QuickSight, you can create dashboards on HealthLake data to quickly explore patient trends. Here is an example of a population health dashboard created using Amazon QuickSight. You can also build, train, and deploy your own predictive analytics using machine learning models with Amazon SageMaker. Here is how to build a number of predictive chronic or

acute disease models using Amazon SageMaker with AWS HealthLake normalized data. Here is an example of building an ML-enabled cognitive search application where every clinical evidence is tagged, indexed, and structured to provide evidence-based topics on things like transmission, risk factors, therapeutics, and incubation. This functionality is tremendously valuable for clinicians or scientists, who can quickly ask questions to validate their clinical decisions or advance their research. With this SecureHIT tool you will be able to offer all the reports requested in this RFP but it is not limited to them.

Direct Secure Messaging

SecureHIT is a DirectTrust accredited HISP/HIE since 2018 and will provide secure direct messaging (Direct SecureHIT) services to make available and support local healthcare providers' technology gaps for HISP services. This exercise will quickly enable a Provider Directory at the level of all states and PR allowing compliance with the sending and receiving of referrals, Event Notifications, and the exchange of information even for those providers who do not have the technology of an EHR. This tool for the health information exchange is proposed to be for 100% of healthcare providers to guarantee the compliance within the 1st quarter a provider directory can be obtained and meet the referrer sending and receiving interoperability metrics (closing the referral loop). In the initial meetings, the PRMP/PRDoH will be requested to provide us as a Trusted Agent with the necessary information in a comma delimited file for the creation of the Direct PR Provider Directory. These files will be used to generate the accounts. Once the accounts are created, this generates an email to the provider in their regular (primary registered) email with an Onboarding package to start their Direct SecureHIT account. Once the Direct Provider Directory is created, the tutorials and standard procedure for accessing and using this directory for sending health information by Direct SecureHIT will be published to the entire health sector. Direct SecureHIT is enabled to be integrated into EHRs using FHIR API, Jason Restful API, XDR/XDM protocols and currently about 40% of hospitals in PR use Direct SecureHIT as a tool and is interoperable with any other HISP implemented in another healthcare facility. In the case of health providers that have DSM, it will be completely interoperable. Implementing SecueHIT Direct to 100% of healthcare providers will improve care coordination, in short term, between Medicaid providers and their patients by facilitating communications through a secure direct messaging (DSM) service, allowing the health information exchange through DSM even if the healthcare provider does not have an EHR in place. Direct SecureHIT will provide the availability to record the total number of DSM accounts sent by provider, the number of DSM messages sent, received and opened allowing us to achieve the goal of 100% of DSM messages being sent and received correctly to users assigned. This element requires reporting as defined in the Attachment F - Outcome Traceability Matrix and will be reported through the dashboard.

Electronic Notification Services (ENS)

SecureHIT, as operator of PRHIE, will provide the healthcare community with ENS to alert providers based on desired use cases, such as admission/discharge/transfer (ADT) encounters. Event notifications through Direct Standard® Care teams will be reported when a mutual patient experiences an event, such as an admission, discharge, or hospital transfer (ADT). https://directtrust.org/standards/event-notifications-via-direct. This service will be provided directly by SecureHIT as PRHIE operator. SecureHIT will enable ENS to include dashboard management for automated subscription delivery, consistent with the DirectTrust authorization process. SecureHIT will provide a letter to institutions to document their compliance with the certification requirements for the Merit-Based Incentive Payment System (MIPS) and interoperability rules. Having enabled Direct SecureHIT for 100% of health providers in PR, the ENS will be transparently enabled under the same portal and in compliance with the interoperability integrated into the EHR and HealthLake. The documentation for the integration of ENS will be delivered to the corresponding participants to proceed with the integration of the APIs. As soon as the hospitals are properly configured, the providers will receive the ENS regardless of whether they have an EHR or not. SecureHIT will be able to count the end users receiving admission, discharge and transfer (ADT) notifications in real time, the volumes of event notifications are reported periodically, to be able to report periodically and observe compliance with the goal which is to receive 100% of the notifications that are delivered; and notify the source of 100% of rejected messages. This element requires reporting as defined in the Attachment F - Outcome Traceability Matrix and will be reported through the dashboard.

Emergency Response Services

SecureHIT, using the AWS HealthLake platform, will provide connectors to the US government's federated networks to enforce the Department of Health in providing emergency response services. SecureHIT has a connecting connector with eHealth Exchange and other regional or national exchange providers to support data sharing in times of emergency. In meetings with PRDoH, the protocol and method for sharing the ADT information required for hospitals and patient registration with the provider that provides emergency response services to PRDoH will be defined. Once defined, APIs will be integrated to send the information. Technical support will be provided to Department of Health if necessary. SecureHIT asserts its ability to support emergency response services as described.

Interoperability Compliance

SecureHIT offers AWS HealthLake as the EHR interoperability and longitudinal solution in compliance with each of the requirements of this RFP. The FHIR API capabilities in Amazon HealthLake were developed by Amazon Web Services (AWS) to help customers accelerate data exchange and comply with ONC and CMS interoperability and patient access rules. The tool is natively developed and designed for compliance with ONC interoperability and CMS requirements.

Deliverables

D01: Monthly Status Report

1. Delivered by the Project Coordinator – Reporting
- Status against the Project Management Plan/Project Schedule (status of scope, schedule, budget)
- Key accomplishments
- Upcoming focus areas
- Key metrics
- Objectives for the next reporting period
- Key upcoming meetings
- Recovery plan for all work activities not tracking to the approved schedule and/or to the approved plan documents
- Escalated risks, issues (including schedule and budget), action items, and decisions
- Progress towards key goals including data quality tracking and remediation, expansion and maintenance of interface feeds, data use and access, pilots, public health reporting and need identification, etc.

2. Status of compliance with federal mandates
   - Delivered by RMComm – privacy controls, security assessments
   - Delivered by Project Coordinator – Conditions of MES OBC, etc.
3. Delivered as defines in Outcome Traceability Matrix
   - Status of key services areas including, but not limited to, MPI rates, data access, care coordination facilitation, ENS, public health reporting and support, and emergency response support –
   - Consent rates for people who choose to opt-out of the HIE, as tracked within the MPI – Outcome Traceability Matrix
4. Delivered by Cybersecurity Division
   - Adverse privacy audits results – Incident and Response Plan
5. Delivered by Project Coordinator/Project Director
   - Intentions to redisclose data aggregated through the HIE to third parties
6. Delivered by Customer Service Dashboard
   - Status of compliance with all SLAs
7. Delivered by Project Coordinator/Project Director
   - Status of compliance with the Outcomes Traceability Matrix (OTM)

Milestones Business Operations (Refer to the Gantt Chart for Delivery Dates)

- Kickoff meetings
- Governance
- Data Governance
- Policy and SLA
- Participant Agreement Management
- Technical Assistance Operations
- Officially Open PRHIE Operations
- Interface Deployment
- Onboarding Deployment
- Operational Reports and SLAs
- Meeting with Participants for Connectivity Activities
- OBC Support Plan

Milestones Technology Services (Refer to the Gantt Chart for Delivery Dates)

- Kickoff Meetings
- Data Quality
- Access Authentication
- Longitudinal EHR – AWS HealthLake Go Live
- Unique Patient Identifier – Rhapsody EMPI Go Live
- PRHIE Website
- Participant Portal
- Provider Portal
- Patient Portal
- Payer Portal
- Event Notification System
- Direct Secure Messaging – Direct SecureHIT
- Healthcare Provider Directory
- Public Health – Data Capture
- Public Health – Reporting
- Promoting Interoperability Program Objectives
- PRMP Interfaces
- PRMP Data Access
- Enable MCO Clinical Data Access
- MCO Data Access Pilot
- OBC Self Attestation
- CMS OBC Certification Request

Assumptions

All time estimates in this SoW assume the availability of necessary resources by the PRMP, PRDoH and stakeholders. It is assumed that the data capture sources to be integrated have the capabilities to integrate electronically through interfaces and that they have the necessary infrastructure (hardware and software). Subject to initial evaluation to validate that all necessary infrastructure (hardware and software) and administrative requirements are available to be able to execute the estimated time. It is based on the premise that all the required elements are available; If they are not available, they can negatively impact deliveries and/or their times. Additionally, any other unforeseen event or element that we are not aware of at this time is considered part of this assumption. The approval process can impact the timelines and deliverables, and is part of this assumption.