Expression of Interest (EOI)
For
Empanelment of Technology Partners with HITES
For IT/ITES Solutions

HLL INFRA TECH SERVICES LIMITED

(A CPSE under Ministry of Health and Family Welfare (MoHFW), Govt. of India)

B-14 A, Sector - 62, Noida - 201 307, Uttar Pradesh, India

Website: www.hllhites.com

EOI No. HITES/BD/EOI/2023-24/ 012 **13.02.2023**

Expression of Interest (EOI) For Empanelment of Technology Partners with HITES For IT/ITES Solutions

HLL INFRA TECH SERVICES LIMITED
(A CPSE under Ministry of Health and Family Welfare (MoHFW), Govt. of India)
B-14 A, Sector - 62, Noida - 201 307, Uttar Pradesh, India
Website: www.hllhites.com

HITES

EMPANELMENT NOTICE

EOI NO.: HITES/ BD/EOI/2023-24/012 Dated 13.02.2024

HITES, A CPSE under Ministry of Health and Family Welfare (MoHFW), Govt. of India, invites Bids against the Expression of Interest (EOI) for Empanelment of Technology Partners for IT/ITES Solutions

The last date of receipt of bids is 27.02.2024.at 15.00 PM

To download EOI document and submission of proposal, please visit https://etenders.gov.in/eprocure/app and www.hllhites.com/tenders. Any amendments / corrigendum will be published in e- tender portal and www.hllhites.com/tenders only.

Expression of Interest (EOI) for Empanelment of Technology Partners for IT/ITES Solutions

HITES, A CPSE under Ministry of Health and Family Welfare (MoHFW), Govt. of India, is one of India's leading healthcare services companies.

HITES invites Expression of Interest (EOI) from Technology Firms in the IT/ITES Solutions domain, having experience in the area of Design, development, test and supply of Cyber Security Solutions; and in the area of design and development of other IT/ITES solutions related to Health Information Management Systems (HIMS) and willing to jointly address business opportunities.

Schedule of this EOI

Schedule	Date
EOI Issue Date	13-02-2024 (10.00 am)
Submission Due Date	27-02-2024 (3.00 pm)
Technical Bid Opening at HITES.	28-02-2024 (3.30 pm)

Interested bidders shall submit Sealed Expression of Interest (EoI) with the supporting documents mentioned in Section 5 on or before the due date of submission of EoI. The bidders can also submit the bids in soft copy through email but the hard copy of the same has to reach the undersigned within 7 days of the due date of submission. Submission of response to this notice inviting EoI shall be deemed to have been done after careful study and examination of this document with full understanding of its Scope, Specifications, Terms, conditions & Implications.

1. Information for Interested party

EOI No.: HITES/BD/EOI/2023-24/012 Dated: 13.02.24

1. A Response to call for Expression of Interest (EOI) from a reputed firm at the national/ international level with prior experience in this sector in the past.

Sl. No.	Description	Details
1	EOI no.	HITES/BD/EOI/2023-24/012 dated 09.02.24
2	EOI ID	2024_HITE_185859
3	Date of issue of EOI	13th February 2024,
4	Last Date of submission of EOI	27th February 2024, 15:00 hrs.
5	Date of opening of EOI	28th February 2024, 15:30 hrs.
6	Proposals should be addressed to	The Chief Executive Officer, HITES, B-14 A, Sector-62, NOIDA, 201307
7	Proposals should be submitted at (Through online mode only)	https://etenders.gov.in/eprocure/app
8	EOI Processing fee (non-refundable)	Rs. 20,000/- Plus GST@ 18% = Rs. 23,600 (through online mode only) (as per the bank details in EOI)
9	Empanelment fee, if Qualified	₹ 50,000/- (Rupees Fifty Thousand Only) Non- refundable (through online mode only) (as per the bank details in EOI)
10	EOI Documents should be Obtained	The detailed EOI document can be viewed or downloaded from website www.hllhites.com and https://etenders.gov.in/eprocure/app
11	E-mail id	bd@hllhites.com
12	Contact Details	0120-4071500/576
13	Bid Validity (in days)	180 days

1.B Cost of bid document for on-line bid for work is shown in the schedule of submission. Tender cost (non- refundable) will be submitted online in following HITES Bank Account latest by 27.02.2024 till 15:00 hrs: -

SI. No.	Particulars	Details
1	Name of Beneficiary	HITES FD BACKED OVERDRAFT ACCOUNT
2	Name of Bank	ICICI Bank
3	Bank Branch Name	Sector-62, NOIDA Branch
4	Branch Address	Stellar IT Park, C-25, Sector-62,NOIDA, Uttar Pradesh
5	Bank A/c No.	158005003923
6	IFSC Code	ICIC0001580
7	Branch Code	152
8	MICR	110229152

2. Introduction and Project Objectives

HITES works in many aspects of the health infrastructure sector, including in hospital management and administration. The company is looking to empanel 4-5 IT/ITES solutions vendors who can fulfill the following 2 objectives -

1. To create a robust, scalable, and efficient SOC capable of 24x7 operations.
2. To create a Health Information Management System

Under these objectives there are two types of providers required:

1. Product/Solution Provider: OEM/Authorized Reseller
2. System Integrator/Implementation expert

3. Terms of EOI

3.1. Eligibility Criteria

S. No.	Criteria	Requirements
1	**PAN Card**	Interested party must have a valid PAN Card
2	**Certificate of Incorporation**	Interested party must have a valid Certificate of Incorporation
3	**Consortium – Not Allowed**	**Consortium is not allowed**

4	**Minimum Turnover**	The Bidder should have an average turnover of INR 20 **Crore in any of the three financial years out of th**e last 3 financial years (FY 20-21, FY 21-22, and FY 22-23). Exceptions will be given for 'Startup' firms recognised as such by the Department for Promotion of Industry and Internal Trade (DPIIT), Ministry of Commerce & Industry, Government of India.
5	**General Experience**	
5a	**Cyber Security Solution Provider/ Cyber Security Implementation Agency**	The interested party must have experience of providing Cyber Security solutions for Data centre/cloud or establish a Cyber Security SOC with any government / Public Sector (Central, State, Fis, etc) in India.
5b	**HIMS Solution Provider/ System Integrator for Health System**	The interested party must have experience of executing at least 3 government IT/ITES projects in the health/e-gov sector
6	**Similar Assignments**	
6a	**Cyber Security Solution Provider**	The interested party must have experience of supply, installation & support of Cyber Security solutions for Data centre/cloud with any government / Public Sector (Central, State, Fis, etc) in India as Sole Bidder/Consortium Partner/OEM
6b	**Cyber Security Implementation Agency**	The interested party must have experience of implementing Cyber Security solutions for Data centre/cloud or establish a Cyber Security SOC with any government / Public Sector (Central, State, Fis, etc) in India as Sole Bidder/Consortium Partner
6c	**HIMS Solution Provider**	The interested party must have experience of supply, installation & support of HIMS solutions for Data centre/cloud with any government / Public Sector (Central, State, Fis, etc) in India as Sole Bidder/Consortium Partner/OEM
6d	**System Integrator for Health System**	The interested party must have experience of implementing a large IT System in Health/eGovernance domain with any government / Public Sector (Central, State, Fis, etc) in India as Sole Bidder/Consortium Partner

3.2. Scope of Work

a) ***Bidders with Scope of work for Cyber Security Solution Provider will also have to fulfil the scope of work of Cyber Security Implementation Agency so that the same bidder will be responsible for both the scope of works.***

b) ***Bidder shall liable to provide new addition/ availability of any modules in future without any extra cost.***

3.2.1. Cyber Security Solution Provider

Scope of Work includes Supply, Installation, Warranty, and Support following components:

1. **Hardware**: Network security appliances, dedicated encryption devices, biometric authentication systems.
2. **Software**: Threat detection and response applications, system management software, available as perpetual licenses or SaaS.
3. **Cloud-based Infrastructure**: Scalable and flexible cloud-hosted security solutions.

The components mentioned above should be related to the following Solution Categories under comprehensive Cyber Security Solution.

- **Network Security**: Including firewalls, IDS/IPS, VPNs, NAC.
- **Endpoint Protection**: Antivirus, Anti-Malware, EDR, MDM.
- **IAM**: SSO, MFA, Identity Governance.
- **Data Security**: Encryption, DLP, Secure File Transfer.
- **SIEM**: Real-time Monitoring, Log Management, Incident Response.
- **Cloud Security**: CASB, Secure Web Gateways, Cloud Workload Protection.
- **Vulnerability Management**: Security Assessment, Patch Management, Threat Intelligence.
- **SOAR**: Automation Workflows, Response Playbooks, Threat Hunting.
- **Compliance Management Tools**: Policy Management, Compliance Reporting, Risk Assessment.
- **Threat Intelligence Platforms**: Threat Analysis, Feeds, Contextual Information.

3.2.2. Cyber Security Implementation Agency

The Scope of work is as mentioned below:

- **Design and Development:**
    - Comprehensive design of the SOC architecture, including high-level and detailed planning.
    - Periodic review and upgrading of the architecture based on evolving cybersecurity trends.
- **Implementation:**
    - Deployment of SOC components such as SIEM, threat intelligence platforms, and IT ticketing systems.
    - Integration of these components into HITES's existing IT infrastructure.
- **Testing and Go-Live:**
    - Rigorous testing of the SOC setup, including User Acceptance Testing (UAT).
    - Official commissioning of the SOC post-testing and approvals.
- **Operational Management:**
    - Ongoing 24x7 monitoring and management of cybersecurity events.
    - Regular reporting and analysis of security incidents and trends.

1. **SOC Operations: Key Design Principles**

- **Functional Principles:**
    - Effective management of security incidents to minimize business impact.
    - Continuous improvement in detection, analysis, and incident resolution capabilities.
- **Scalability Principles:**
    - Development of modular and scalable solutions.
    - Capacity to adapt to the growing and changing needs of HITES and its subsidiaries.
- **Availability Principles:**
    - Ensuring high availability of services to maintain continuous operation.
    - Designing fault-tolerant systems to prevent service disruptions.
- **Performance Principles:**
    - Ensuring SOC solutions do not adversely impact HITES and its subsidiaries existing operations.
    - Maintaining high performance and efficiency of all technology components.

2. **Deliverables**

- **Initial Deliverables:**
  - Signed contracts, NDAs, SLAs, and other legal and operational documents.
  - Comprehensive project plan outlining timelines, milestones, and responsibilities.
- **Development Deliverables:**
  - Detailed architecture diagrams and implementation plans for SOC setup.
  - Integration plans for existing systems and applications.
- **Operational Deliverables:**
  - Regular monitoring reports, incident analysis, and threat intelligence updates.
  - Quarterly and annual reviews of SOC performance and security posture.

3. **Period of Contract**

- **Contract Duration:**
  - The services are to be provided for a period of 36 months (3 years).
- **Review and Renewal:**
  - Periodic reviews for potential modifications or extensions of the contract based on performance and evolving needs.

4. **Transition and Exit Management**

- **End of Contract Procedures:**
  - Detailed plans for the handover of technologies and processes at the end of the contract or in case of early termination.
- **Future Roadmap:**
  - Recommendations for subsequent steps and potential upgrades post-contract.

5. **Evaluation and Reporting**

- **Regular Assessments:**
  - Ongoing evaluation of the SOC's performance against set benchmarks and objectives.
- **Reporting Mechanism:**
  - Regular reporting to HITES stakeholders on SOC operations and incident responses.

6. **Compliance and Standards**

- **Adherence to Standards:**
    - Compliance with national and international cybersecurity standards and best practices.
- **Data Privacy and Protection:**
    - Ensuring the confidentiality, integrity, and availability of sensitive health data.

7**. Details of Activities & Deliverables**

A. Solution Design and Development

1. **Architecture Diagrams for SOC and Solutions:**
    - Development of detailed architecture diagrams for the SOC.
    - Inclusion of all critical components and their interconnections.
2. **Implementation Plan for SOC and Solutions:**
    - Comprehensive plan detailing the steps for implementing SOC solutions.
    - Timeline and resource allocation for each phase of implementation.
3. **Integration Plan for Devices to SIEM:**
    - Strategy for integrating existing devices and applications with the SIEM system.
    - Protocols for secure and efficient data transfer and communication.
4. **Log Baseline:**
    - Establishment of a baseline for log collection and management.
    - Criteria for log prioritization and categorization.
5. **Threat Model-Based Use Case List:**
    - Development of use cases based on an in-depth threat modeling exercise.
    - Focus on scenarios most relevant to HITES's environment.
6. **BCP and DR Plans:**
    - Business Continuity Planning (BCP) and Disaster Recovery (DR) strategies.
    - Procedures for maintaining SOC operations under various scenarios.

B. Solution Implementation

1. **Implementation Closure Report:**
    - A comprehensive report marking the completion of SOC implementation.
    - Details of integration with all existing applications and devices.

2. **Activities Covered:**
    - Log Collection: Methodologies and tools for efficient log collection.
    - SIEM Use Cases and Incident Management: Implementation of SIEM for proactive incident management.
    - Reports and Dashboards: Development of custom reports and dashboards for real-time monitoring.
    - SIEM Administration: Administration protocols for SIEM management.
    - Threat Intelligence Integration: Integration of real-time threat intelligence feeds.
    - Ticketing Tool Integration: Seamless integration of ticketing tools for incident tracking and management.

C. Go-Live

1. **Live Demonstration of SOC Capabilities:**
    - Demonstrating the operational capabilities of the SOC to stakeholders.
    - Use case trigger testing to showcase real-world scenario responses.
2. **UAT Testing Report:**
    - Comprehensive report of User Acceptance Testing, covering all solutions, processes, and operations.
3. **Solution Fine-Tune Report:**
    - Analysis of the solution's performance, focusing on false positives and resource utilization.

D. Operations 24x7/365

1. **Continuous Monitoring and Threat Detection:**
    - 24x7 log monitoring and event analysis.
    - Detection of threats based on integrated log sources and predefined use cases.
2. **Analytics and Threat Hunting:**
    - IOC-based threat hunting reports.
    - Continuous analysis for proactive threat detection.
3. **Incident Response and Reporting:**
    - Investigation, forensics, and Root Cause Analysis (RCA) of security incidents.

- Submission of comprehensive reports on incidents and trends.

4. **Quarterly Briefings and Recommendations:**
    - Regular briefings on incident data, alert trends, and high-risk areas.
    - Recommendations for security improvements.
5. **Customized Reports and Dashboards:**
    - Development of both standard and custom incident dashboards and reports.
    - Focus on patterns, trends, and specific incidents like phishing campaigns and malware outbreaks.
6. **Assessment Reports:**
    - Regular SIEM health and utilization reports.
    - SLA and performance review reports.
    - Security assessment reports including API, Web Application (WASA), and Mobile Application Security Assessment (MASA).
    - Detailed Code Review, Vulnerability Assessment, and Penetration Testing Reports.

8**. Global Standards for Compliance for the SOC Provider**

The SOC provider is expected to comply with a range of international standards and frameworks to ensure the highest level of cybersecurity practices. These standards are critical for maintaining the integrity, confidentiality, and availability of information, as well as for ensuring that the SOC operates effectively and efficiently. The following are key global standards that the SOC provider should adhere to:

1. **ISO/IEC 27001: Information Security Management Systems (ISMS):**
    - A comprehensive framework for managing and protecting information assets.
    - Includes aspects such as risk management, security policy, asset management, physical and environmental security, communications security, and compliance.

2. **NIST Cybersecurity Framework:**
    - Developed by the National Institute of Standards and Technology (NIST) in the USA.
    - Provides guidelines on how to manage and reduce cybersecurity risk in a comprehensive manner.
    - Focuses on five core functions: Identify, Protect, Detect, Respond, and Recover.

3. **General Data Protection Regulation (GDPR):**
    - European Union regulation for data protection and privacy.
    - Important for SOC providers handling data of EU citizens, with strict rules on data consent, user access, and data breach notifications.

4. **PCI DSS (Payment Card Industry Data Security Standard):**
    - Essential for SOC providers involved in processing, storing, or transmitting credit card information.
    - Ensures the secure handling of cardholder information and reduces credit card fraud.

5. **SOC 2 (Service Organization Control 2):**
    - A framework for managing data security based on five "trust service principles" — security, availability, processing integrity, confidentiality, and privacy.
    - Relevant for ensuring the secure management of data within the SOC.

6. **HIPAA (Health Insurance Portability and Accountability Act):**
    - U.S. legislation providing data privacy and security provisions for safeguarding medical information.
    - Critical for SOC providers handling healthcare-related information.

7. **COBIT (Control Objectives for Information and Related Technologies):**
    - A framework for developing, implementing, monitoring, and improving IT governance and management practices.
    - Helps in aligning IT goals with business goals, while managing risks and resources effectively.

8. **ITIL (Information Technology Infrastructure Library):**
    - A set of practices for IT service management (ITSM) focusing on aligning IT services with business needs.
    - Includes aspects like service design, service strategy, service transition, and service

operation.

9. **IEC 62443: Industrial Communication Networks – Network and System Security:**
   - Series of standards focusing on the security of Industrial Automation and Control Systems (IACS).
   - Relevant for SOC providers dealing with critical infrastructure and industrial control systems.

Note: - Bidders with Scope of work for Cyber Security Solution Provider will also have to fulfil the scope of work of Cyber Security Implementation Agency so that the same bidder will be responsible for both the scope of works.

3.2.3. HIMS Solution Provider

The Scope of Work includes Supply, Installation, Customization and Support of HIMS solution that should have the following modules.

1. **Patient Registration Module**

Functional Requirements:

- Ability to perform different types of patient registrations (Normal, Special Clinic, Emergency, Self, Staff & Dependent).
- Automated assignment of a unique Central Registration Number (CRNO) and secondary UHID to each patient.
- Capture and store detailed patient demographic and government/state-issued ID information.
- Implementation of a duplicate check algorithm based on EHR 2016 guidelines to prevent multiple CRNOs per patient.
- Integration with a web-cam to capture and store patient images.

2. **Emergency Registration Module**

Functional Requirements:

- Management of Casualty Registration for ambulatory and emergency cases.
- Provision for registering and managing MLC and unknown patients.

- Storage and access to patient history, clinical summary and emergency visit details.
- Online emergency order sets for quick patient service.
- Triage management system for prioritizing patient care.

3. Appointment Module

Functional Requirements:

- Dynamic configuration of appointment slots for various services like OPD, Lab, OT.
- Automated search and scheduling for the earliest available appointments.
- Facility for rescheduling and cancellation of appointments with patient notification via email/SMS.
- Overbooking management as per hospital policy.
- Multi-appointment scheduling for a single patient across different dates.

4. Patient Enquiry Module

Functional Requirements:

- Provision to enquire about patient status, name, address, and other details using multiple search criteria.
- Information access on OPD working days, lab test availability, and bed availability.
- Integration with enquiry kiosks for self-service access to information.

5. Patient Billing Module

Functional Requirements:

- Configurable billing system for various patient categories and services.
- Facility to define and apply discounts and cancellation policies.
- Electronic claim processing for insurance and government schemes.
- Integration for digital payment methods like POS, QR Code/UP.
- Real-time tracking and updating of patient bill details.

6. Outpatient Department Module

Functional Requirements:

- Comprehensive patient profile management including history, allergies, and current conditions.
- Integration with EMR for accessing longitudinal clinical data.
- Prescription management with facility for digital prescription creation.
- Vital signs monitoring and clinical charting.
- Voice to text functionality for clinical notes.

7. **ADT (Admission, Discharge, and Transfer) / IPD Module**

Functional Requirements:

- Real-time bed management and availability status tracking.
- Automated admission, transfer, and discharge processes.
- Patient tracking from admission through discharge.
- Management of patient leaves and bed allocation.

8. **Investigation for Labs and Radio Diagnosis Module**

Functional Requirements:

- Configurable test and result entry templates for various labs.
- Barcode integration for sample tracking.
- Online access to test results for authorized personnel.
- Automated interfacing with diagnostic equipment for direct data transfer.
- Test result comparison and historical tracking.

9. **Operation Theatre Module**

Functional Requirements:

- Scheduling system for operations with department-specific configurations.
- Real-time monitoring and recording of operation details.
- Facility for pre and post-operation documentation.
- Integration with patient monitoring systems.
- Management of surgical inventory and equipment.

10. Electronic Medical Record (EMR) Module

Functional Requirements:

- Centralized storage and retrieval of electronic patient records.
- Secure access controls based on user roles and permissions.
- Integration with diagnostic and treatment modules for comprehensive data capture.
- Customizable EMR interfaces for different medical specialties.
- Compliance with healthcare data standards and privacy regulations.

11. Medical Record Department (MRD) Module

Functional Requirements:

- Digital archiving of patient case sheets and medical records.
- Indexing and retrieval system for easy access to records.
- Integration with hospital reporting systems for statistical analysis.
- Secure and compliant management of sensitive medical records.

12. Diet and Kitchen Module

Functional Requirements:

- Management of patient-specific diet orders and kitchen operations.
- Nutritional calculator for customizing patient diets.
- Integration with patient care modules for diet-related alerts.
- Automated tallying and quality control of meals prepared.

13. Blood Bank Management System Module

Functional Requirements:

- Real-time tracking of blood stock and donor registry.
- Compliance with blood bank regulations and safety protocols.
- Integration with patient care modules for timely availability of blood products.
- Donor management and tracking of transfusion-transmitted infections (TTI).

14. Pharmacy and Material Management Module

Functional Requirements:

- Inventory management for drugs and medical supplies.

- Automatic reorder alerts based on consumption and demand forecasting.
- Integration with billing and patient care modules for accurate charge capture.
- Management of drug dispensing and returns.

15. Central Sterile Supply Department (CSSD) Module

Functional Requirements:

- Tracking and management of sterilization processes.
- Quality control checks for sterilized items.
- Integration with operation theatre and other departments for supply management.
- Record-keeping for usage and maintenance of sterilization equipment.

16. Bio Medical Engineering Department (BMED) Module

Functional Requirements:

- Maintenance scheduling and tracking for medical equipment.
- Breakdown and preventative maintenance management.
- Inventory management for spare parts and maintenance supplies.
- Compliance tracking for equipment safety and performance standards.

17. Alert Management Module

Functional Requirements:

- System-wide alert generation for critical patient conditions and hospital operations.
- Customizable alert parameters for different departments.
- Integration with mobile and desktop interfaces for real-time notifications.
- Escalation protocols for unresolved alerts.

18. User Management Module

Functional Requirements:

- Role-based access control for various system functions.
- User activity tracking and audit trails.
- Integration with hospital identity management systems.
- Customizable user profiles and permissions.

19. Mobile Apps

Functional Requirements:

- Mobile access for patient registration, appointment scheduling, and report viewing.
- Integration with hospital systems for real-time information updates.
- Secure communication channels for patient-doctor interactions.
- User-friendly interface for easy navigation and accessibility.

20. Equipment Interfacing

Functional Requirements:

- Seamless integration between medical equipment and HIS for data transfer.
- Compatibility with a wide range of medical devices and equipment.
- Real-time data acquisition and processing for clinical use.

21. Integration with Third-Party Applications

Functional Requirements:

- API support for integration with external healthcare platforms like ABDM, PMJAY, IHIP etc.
- Data exchange protocols for secure and reliable information transfer.
- Compatibility checks and updates for third-party software integration.

22. Support for Standalone and Networked Health Facilities

Introduction: To accommodate diverse healthcare settings, this module ensures the HIS is adaptable for both standalone health facilities and integrated networks of hospitals, clinics, labs, and health centers.

Functional Requirements:

- Scalable architecture to support both single facility operations and a network of health facilities including large hospitals, health centers, labs, and clinics.
- Centralized data management system for integrated healthcare networks, facilitating coordinated patient care across different facilities.
- Interoperability features to enable seamless data exchange and consistent operations

across various health facilities.

- Customizable access controls and user roles for different levels of facility operations within the network.
- Real-time data synchronization and backup mechanisms to ensure data integrity and continuity across the networked facilities.

23. Support for Health-Related Compliance and Standards

Introduction: Recognizing the importance of adherence to healthcare standards and regulations, this module ensures the HIS is compliant with international and national health-related standards like HIPAA, HL7, ICD-10 & 11, and SNOMED-CT.

Functional Requirements:

- Compliance with HIPAA (Health Insurance Portability and Accountability Act) for patient data privacy and security.
- Integration with HL7 (Health Level Seven) standards for electronic data exchange in healthcare environments.
- Support for ICD-10 & ICD-11 (International Classification of Diseases) coding for diagnoses and medical procedures.
- Implementation of SNOMED-CT (Systematized Nomenclature of Medicine—Clinical Terms) for detailed clinical health information and terminology.
- Regular updates and audits to ensure ongoing compliance with evolving healthcare standards and regulations.
- Training modules and guidelines for staff to ensure adherence to compliance standards in daily operations.
- Robust data encryption and security protocols to safeguard sensitive health information.

3.2.4. System Integrator for Health System

The Scope of Work for System Integrators are as mentioned below:

1. Study

A. Activities:

- Conduct a needs assessment to understand the specific requirements of the healthcare facilities.
- Analyze existing systems and processes for integration points.
- Identify compliance requirements and standards (HIPAA, HL7, ICD-10 & 11, SNOMED-CT).
- Stakeholder interviews to gather insights and expectations.

B. Deliverables:

- Needs Assessment Report.
- System and Process Analysis Document.
- Compliance Requirements Document.
- Stakeholder Interview Summary.

2. Design

A. Activities:

- Create architectural design for a scalable, cloud-based HIS aligned to the proposed solution.
- Design/customize user interfaces and experience (UI/UX) tailored to various user roles.
- Develop a security framework for data protection and privacy.
- Prepare a detailed plan for system integrations and data migration.

B. Deliverables:

- System Architecture and Design Documents.
- UI/UX Design Prototypes.
- Security Framework Documentation.
- Integration and Data Migration Plans.

3. Development/Customization

A. Activities:

- Develop/Customize the HIS modules as per the design specifications.
- Customize modules for specific needs of each health facility in the network.
- Incorporate compliance standards into the development process.

- Develop/customize APIs for integration with third-party applications.

B. Deliverables:

- Developed HIS Modules.
- Customization Documentation.
- Compliance Standards Implementation Report.
- API and Integration Code.

4. Implementation

A. Activities:

- Deploy the HIS onto a cloud infrastructure.
- Conduct data migration and system integrations.
- Perform comprehensive system testing including load testing and user acceptance testing (UAT).
- Go-live support and initial system stabilization.

B. Deliverables:

- Cloud Deployment Documentation.
- Data Migration Completion Report.
- System Testing and UAT Reports.
- Go-Live and Stabilization Report.

5. Operation & Maintenance (O&M)

A. Activities:

- Provide ongoing technical support and system maintenance.
- Monitor system performance and conduct regular health checks.
- Apply updates and patches as needed for security and functionality.
- Manage backups and disaster recovery processes.

B. Deliverables:

- O&M Support Documentation.

- System Performance and Health Check Reports.
- Update and Patch Application Records.
- Backup and Disaster Recovery Protocols.

6. Training

A. Activities:

- Develop training materials for different user groups (administrative staff, healthcare professionals, IT support).
- Conduct training sessions on system use, data security, and compliance adherence.
- Offer continuous learning resources and update training as the system evolves.
- Collect feedback and provide post-training support.

B. Deliverables:

- Training Materials and Manuals.
- Training Session Records and Feedback.
- Continuous Learning Resources.
- Post-Training Support Documentation.
- Post Implementation Support.

3.3. Evaluation Criteria for Interested party

Note: - 3.3.A- Bidders with Scope of work for Cyber Security Solution Provider will also have to fulfil the scope of work of Cyber Security Implementation Agency so that the same bidder will be responsible for both the scope of works.

3.3.1. Cyber Security Solution Provider

I. The Bidder must be a registered company in India (Public, Private, Partnership companies) under the Companies Act 1956 having at least three years of existence. Copy of the certification of incorporation and Memorandum of Article of Association shall be submitted along with the EOI.

II. The Bidder should be an Original Equipment Manufacturer or authorized IT solution providers for above product and Solutions. The IPR of the Cybersecurity solutions should be registered in India and in the name of the bidder/OEM. The solution provider/OEM possesses all the related patents in their name.

III. Bidder should possess a valid PAN and GST number.

IV. The Bidder shall be capable of providing compliance to the Technical and Functional requirements specified by the customer. They shall also be in a position to meet any additional enhanced requirements of the customer during the course of the tender. Organization's maturity and compliance in relation to the attainment of relevant information security certifications:

   A. This should include industry-standard security certifications standards such as ISO 27001, SOC 2, and Cloud Security Alliance (CSA) or equivalent from Bidder/its OEM.

      Indicate the experience and relevant security certifications of staff members who may be assigned to this project (if applicable)

V. Minimum three years of ICT/ SOC managed services/Cyber Security experience as relevant to the requirements stated above and should provide the following:

   A. Experience and examples of how you support the collection, management and analysis of cyber security big data collected from endpoints, servers, appliances and logs deployed at customer premises
   B. Experience and examples of how you support the collection and management of Advanced Threat Intelligence
   C. Experience and examples of supporting the detection and management of cyber security breaches and incidents originating from cyber criminals, state-sponsored actors, terrorists and hacktivists
   D. Organizational experience of working on Cyber Security incidents originating from cyber criminals, state-sponsored actors, terrorists and/or hacktivists. Please specify as required
   E. Organizational experience of working with large, complex and geographically distributed organizations in Governmental and Non-

Government

NOTE: Enclose copies of Purchase Orders and Project completion certificates as much possible while providing above information.

VI. Bidders shall be ready to meet the customer tender conditions with respect to all activities like delivery, installation, integration commissioning and Annual maintenance of all items/subsystems and services as given in the customer tender on an end-to-end basis.

However, in case HITES desires to have value addition for any of the activities under the tender/purchase order, the Bidder shall be ready for the same on mutually agreeable terms and conditions. Vendor shall bear its own expenses towards certification, validation, QA inspection, delivery, etc.

VII. Customer References: Please provide at least three (3) detailed examples of customers for whom you have delivered major ICT/SOC Managed Services/ Cyber Security and/or Program Management services in the last five (5) years.

Some areas of detail to include in each example (this is a non-exhaustive list, please provide additional information that you deem relevant) are:

A. What are/were the exact products/services provided?

B. What is the average size (revenue, number of devices, volume of data collected and analyzed, etc.) and type of program?

C. How is/was the engagement structured and how did your staff engage with the customer staff?

D. Is/was the engagement successful? In what way did you measure success of the delivered products/services?

E. Is the engagement still on-going; if not, why not? Please provide supporting information for each example, along with reference contact information.

HITES reserves the right to contact these references without prior notification to the Vendor.

VIII. The Bidder shall furnish full details on the solution offered to address the tender related to above products, along with the compliances to the tender requirements and their readiness to support partnership for participating in the tender and executing any purchase order – post tender.

IX. The products and solutions should be compliant to the latest PPP-MII guidelines.

X. The empaneled bidder shall be willing to enter into a Memorandum of Understanding (MoU) with HITES valid for a minimum period of three years, extendable either based on tender requirements or on mutual consent.

3.3.2. Cyber Security Implementation Agency

I. The Bidder must be a registered company in India (Public, Private, Partnership companies) under the Companies Act 1956 having at least three years of existence. Copy of the certification of incorporation and Memorandum of Article of Association shall be submitted along with the EOI.

II. The Bidder should be an Original Equipment Manufacturer or authorized IT solution providers for above product and Solutions. The IPR of the Cybersecurity solutions should be registered in India and in the name of the bidder/OEM. The solution provider/OEM possesses all the related patents in their name.

III. Bidder should possess a valid PAN and GST number.

IV. The bidder should have experience in either of the following scenarios:

- Should have completed one project worth valued at Rs. 2 Crores atleast.

  OR

- Should have completed two projects, each valued at Rs. 1.25 Crores, in the Private/ Government/ Urban Local Body (ULB) sectors.

V. The Bidder shall be capable of providing compliance to the Technical and Functional requirements specified by the customer. They shall also be in a position to meet any additional enhanced requirements of the customer during the course of the tender. Organization’s maturity and compliance in relation to the attainment of relevant information security certifications:

A. This should include industry-standard security certifications standards such as ISO 27001, SOC 2, and Cloud Security Alliance (CSA) or equivalent from Bidder/its OEM.

Indicate the experience and relevant security certifications of staff members who may be assigned to this project (if applicable)

VI. Minimum three years of ICT/ SOC managed services/Cyber Security experience as relevant to the requirements stated above and should provide the following:

A. Experience and examples of how you support the collection, management and analysis of cyber security big data collected from endpoints, servers, appliances and logs deployed at customer premises

B. Experience and examples of how you support the collection and management of Advanced Threat Intelligence

C. Experience and examples of supporting the detection and management of cyber security breaches and incidents originating from cyber criminals, state-sponsored actors, terrorists and hacktivists

D. Organizational experience of working on Cyber Security incidents originating from cyber criminals, state-sponsored actors, terrorists and/or hacktivists. Please specify as required

E. Organizational experience of working with large, complex and geographically distributed organizations in Governmental and Non-Government

NOTE: Enclose copies of Purchase Orders and Project completion certificates as much possible while providing above information.

VII. Bidders shall be ready to meet the customer tender conditions with respect to all activities like delivery, installation, integration commissioning and Annual maintenance of all items/subsystems and services as given in the customer tender on an end-to-end basis.

However, in case HITES desires to have value addition for any of the activities under the tender/purchase order, the Bidder shall be ready for the same on mutually agreeable terms and conditions. Vendor shall bear its own expenses towards certification, validation, QA inspection, delivery, etc.

VIII. Customer References: Please provide at least three (3) detailed examples of customers for whom you have delivered major ICT/SOC Managed Services/ Cyber Security and/or Program Management services in the last five (5) years.

Some areas of detail to include in each example (this is a non-exhaustive list, please provide additional information that you deem relevant) are:

A. What are/were the exact products/services provided?
B. What is the average size (revenue, number of devices, volume of data collected and analyzed, etc.) and type of program?
C. How is/was the engagement structured and how did your staff engage with the customer staff?
D. Is/was the engagement successful? In what way did you measure success of the delivered products/services?
E. Is the engagement still on-going; if not, why not? Please provide supporting information for each example, along with reference contact information.

HITES reserves the right to contact these references without prior notification to the Vendor.

IX. The Bidder shall furnish full details on the solution offered to address the tender related to above products, along with the compliances to the tender requirements and their readiness to support partnership for participating in the tender and executing any purchase order – post tender.

X. The products and solutions should be compliant to the latest PPP-MII guidelines.

XI. The empaneled bidder shall be willing to enter into a Memorandum of Understanding (MoU) with HITES valid for a minimum period of three years, extendable either based on tender requirements or on mutual consent.

3.3.3. HIMS Solutions Provider

I. The Bidder must be a registered company in India (Public, Private, Partnership companies) under the Companies Act 2013 having at least three years of existence.

Copy of the certification of incorporation and Memorandum of Article of Association shall be submitted along with the EOI.

II. The Bidder should be an IT solution provider for the above product and Solutions. The IPR of the solutions should be registered in India and in the name of the bidder. The solution provider possesses all the related patents in their name.

III. Bidders should possess a valid PAN and GST number.

IV. The bidder should have experience in either of the following scenarios:

- Should have completed at least one project in a hospital across Private/Government/Urban Local Body (ULB) sectors with a minimum capacity of 100 beds.

  OR

- Should have completed two projects in hospitals with a cumulative capacity of 100 beds, across Private/Government/Urban Local Body (ULB) sectors.

V. The bidder shall be capable of providing compliance to the Functional requirements specified by the customer. They shall also be in a position to meet any additional enhanced requirements of the customer during the course of the tender.

VI. The bidder should have experience in developing a HIMS platform with minimum 4 *1*00000 patients registered in a year

VII. The bidder should have experience in developing HIMS solutions for one (1) 500-Bedded Hospital/one (1) 200-Bedded Government Hospital

VIII. The bidder should have experience in developing HIMS solutions for at least three (3) 100-Bedded Hospitals.

IX. The bidder should have been onboarded to provide HIMS solutions to one (1) NABH Accredited 100 Bed Hospital.

X. The bidder should have experience providing HIMS solutions to at least three (3) independent Labs.

XI. The bidder should have the following functionalities readily available –

A. Radiology PACS RIS Module

B. Pharmacy Management Module

C. Bio-Medical Waste Management Module

D. Cloud Based Multitenant system managing at least 1000 beds in the platform.

E. Multi-tier architecture with at least 4 level hierarchy – HQ, Regional Centers, Zonal Centers, and Branches.

XII. Bidders shall be ready to meet the customer tender conditions with respect to all activities like delivery, installation, integration commissioning and Annual maintenance of all items/subsystems and services as given in the customer tender on an end-to-end basis.

XIII. However, in case HITES desires to have value addition for any of the activities under the tender/purchase order, the Bidder shall be ready for the same on mutually agreeable terms and conditions. A vendor shall bear its own expenses towards certification, validation, QA inspection, delivery, etc.

XIV. Customer References: Please provide at least three (3) detailed examples of customers for whom you have delivered major IT/ITES solutions in the health/e-gov sector over the last three (3) years.

XV. Some areas of detail to include in each example (this is a non-exhaustive list, please provide additional information that you deem relevant) are:

A. What are/were the exact products/services provided?

B. What is the average size (revenue, number of devices, volume of data collected and analyzed, etc.) and type of program?

C. How is/was the engagement structured and how did your staff engage with the customer staff?

D. Is/was the engagement successful? In what way did you measure success of the delivered products/services?

E. Is the engagement still on-going; if not, why not? Please provide supporting information for each example, along with reference contact information.

F. HITES reserves the right to contact these references without prior notification to the Vendor.

XVI. The Bidder shall furnish full details on the solution offered to address the tender related to above products, along with the compliances to the tender requirements and their readiness to support partnership for participating in the tender and executing any purchase order – post tender.

XVII. The products and solutions should be compliant to the latest PPP-MII guidelines.

XVIII. The empaneled bidder shall be willing to enter into a Memorandum of Understanding (MoU) with HITES valid for a minimum period of three years, extendable either based on tender requirements or on mutual consent.

3.3.4. System Integrator for Health System

I. The Bidder must be a registered company in India (Public, Private, Partnership companies) under the Companies Act 2013 having at least three years of existence. Copy of the certification of incorporation and Memorandum of Article of Association shall be submitted along with the EOI.

II. The Bidder should be an IT solution provider for the above product and Solutions. The IPR of the solutions should be registered in India and in the name of the bidder. The solution provider possesses all the related patents in their name.

III. Bidders should possess a valid PAN and GST number.

IV. The bidder should have experience in either of the following scenarios:

- Should have completed one project valued at Rs. 1 Crore.
  OR
- Should have completed two projects, each valued at Rs. 75 Lacs, in the Private/ Government/ or Urban Local Body (ULB) sectors.

V. The bidder shall be capable of providing compliance to the Functional requirements specified by the customer. They shall also be in a position to meet any additional enhanced requirements of the customer during the course of the tender. Organization’s maturity and compliance in relation to attainment of relevant information security certifications:

VI. This should include industry standard security certifications standards such as ISO 27001, SOC 2 and Cloud Security Alliance (CSA) or equivalent

VII. Indicate the experience and relevant security certifications of staff members who may be assigned to this project (if applicable)

VIII. Minimum three years of implementing IT/ITES solutions experience as relevant to the requirements stated above and should provide the following:

IX. Experience and examples of how you support the collection, management and analysis of data collected from endpoints, servers, appliances and logs deployed at customer premises

X. Experience and examples of how you support the collection and management of end-user data

XI. Experience and examples of supporting the analysis of User Assessment reports

XII. Organizational experience of working with major ICT vendors

XIII. Organizational experience of working with large, complex and geographically distributed organizations in Governmental and Non-Government

NOTE: Enclose copies of Purchase Orders and Project completion certificates as much possible while providing above information.

XIV. Bidders shall be ready to meet the customer tender conditions with respect to all activities like delivery, installation, integration commissioning and Annual maintenance of all items/subsystems and services as given in the customer tender on an end-to-end basis.

XV. However, in case HITES desires to have value addition for any of the activities under the tender/purchase order, the Bidder shall be ready for the same on mutually agreeable terms and conditions. A vendor shall bear its own expenses towards certification, validation, QA inspection, delivery, etc.

XVI. Customer References: Please provide at least three (3) detailed examples of customers for whom you have delivered major IT/ITES solutions in the health/e-gov. sector over the last three (3) years.

XVII. Some areas of detail to include in each example (this is a non-exhaustive list, please provide additional information that you deem relevant) are:

XVIII. What are/were the exact products/services provided?

XIX. What is the average size (revenue, number of devices, volume of data collected and analyzed, etc.) and type of program?

XX. How is/was the engagement structured and how did your staff engage with the customer staff?

XXI. Is/was the engagement successful? In what way did you measure success of the delivered products/services?

XXII. Is the engagement still on-going; if not, why not? Please provide supporting information for each example, along with reference contact information.

XXIII. HITES reserves the right to contact these references without prior notification to the Vendor.

XXIV. The Bidder shall furnish full details on the solution offered to address the tender related to above products, along with the compliances to the tender requirements and their readiness to support partnership for participating in the tender and executing any purchase order – post tender.

XXV. The products and solutions should be compliant to the latest PPP-MII guidelines.

XXVI. The empaneled bidder shall be willing to enter into a Memorandum of Understanding (MoU) with HITES valid for a minimum period of three years, extendable either based on tender requirements or on mutual consent.

3.3.5 Relevant documents to be submitted for showing the work experience as per respective eligibility criteria:-

i. Copies of Agreement.

ii. Satisfactory certificates issued by client.

iii. Any relevant documents, showing the completion/ on- going work

iv. Value of work and number of beds is required in the respective criteria should be clearly mentioned

4. Instructions to the Interested party

4.1. General Guidelines

4.1.1 Completeness of Response

a) Interested parties are advised to study all instructions, forms, terms, requirements, and other information in the EOI documents carefully. Submission of EOI response will be deemed to have been done after careful study and examination of the EOI documents with full understanding of its implications.

b) The response to this EOI should be full and complete in all respects. Failure to furnish all information required by the interested party EOI documents or submission of an EOI response not substantially responsive to the EOI documents in every respect will be at the Interested party's risk.

4.1.2 EOI Response Preparation Costs

a) The interested party is responsible for all costs incurred in connection with participation in this EOI response process, including, but not limited to, costs incurred in conduct of informative and other due diligence activities, travel to and participation in meetings/discussions/presentations, preparation of EOI response, in providing any additional information required by HITES.

b) This EOI does not commit HITES to award a contract or to engage in related negotiations. Further, no reimbursable cost may be incurred in anticipation of award or for preparing this EOI response.

c) All materials submitted by the interested party become the property of HITES and may be returned completely at its sole discretion.

5. EOI Response format

The interested party must structure their response to EOI in the following Chapters:

- **Chapter 1:** Company Profile. Following information to be shared:

Details of the Organization			
Name			
Nature of the legal status in India			
Nature of business in India			
Date of Incorporation			
Date of Commencement of Business			
Address of the Headquarters			
Address of the Registered Office in India			
Name and mobile number of the Contact Person			
Turnover (in rupees Crores). Auditors certificate showing turnover for the last three (3) years (FY 20- 21, 21-22, 22-23).	FY 20 – 21	FY 21-22	FY 22-23
Other Relevant Information			

- **Chapter 2:** Interested firm's understanding of the Project.
- **Chapter 3:** Overall Approach and Methodology and timelines for completion of

Project.

- **Chapter 4:** Recommendations to HITES, if any for improvement on the overall project scope and delivery.
- **Chapter 5:** Credentials of the firm as mentioned in section 4, pertaining to handling assignments of similar nature.
- **Chapter 6:** Team that shall be deployed on the project and the Subject Matter Experts (SME)
- **Annexure:** Any information, which the interested party wishes to share, can be attached in annexure

After receiving response from interested party on EOI, the Request for Proposal (RFP) will be floated only to the empaneled agencies

Annexure 1

Functional Requirements Specifications for HIMS Solutions Provider

1. Patient Registration Module

Functional Requirements:

- Ability to perform different types of patient registrations (Normal, Special Clinic, Emergency, Self, Staff & Dependent).
- Automated assignment of a unique Central Registration Number (CRNO) and secondary UHID to each patient.
- Capture and store detailed patient demographic and government/state-issued ID information.
- Implementation of a duplicate check algorithm based on EHR 2016 guidelines to prevent multiple CRNOs per patient.
- Integration with a web-cam to capture and store patient images.

2. Emergency Registration Module

Functional Requirements:

- Management of Casualty Registration for ambulatory and emergency cases.
- Provision for registering and managing MLC and unknown patients.
- Storage and access to patient history, clinical summary, and emergency visit

details.

- Online emergency order sets for quick patient service.
- Triage management system for prioritizing patient care.

3. Appointment Module

Functional Requirements:

- Dynamic configuration of appointment slots for various services like OPD, Lab, OT.
- Automated search and scheduling for the earliest available appointments.
- Facility for rescheduling and cancellation of appointments with patient notification via email/SMS.
- Overbooking management as per hospital policy.
- Multi-appointment scheduling for a single patient across different dates.

4. Patient Enquiry Module

Functional Requirements:

- Provision to enquire about patient status, name, address, and other details using multiple search criteria.
- Information access on OPD working days, lab test availability, and bed availability.
- Integration with enquiry kiosks for self-service access to information.

5. Patient Billing Module

Functional Requirements:

- Configurable billing system for various patient categories and services.
- Facility to define and apply discounts and cancellation policies.
- Electronic claim processing for insurance and government schemes.
- Integration for digital payment methods like POS, QR Code/UP.
- Real-time tracking and updating of patient bill details.

6. Outpatient Department Module

Functional Requirements:

- Comprehensive patient profile management including history, allergies, and current conditions.
- Integration with EMR for accessing longitudinal clinical data.
- Prescription management with facility for digital prescription creation.
- Vital signs monitoring and clinical charting.
- Voice to text functionality for clinical notes.

7. ADT (Admission, Discharge, and Transfer) / IPD Module

Functional Requirements:

- Real-time bed management and availability status tracking.
- Automated admission, transfer, and discharge processes.
- Patient tracking from admission through discharge.
- Management of patient leaves and bed allocation.

8. Investigation for Labs and Radio Diagnosis Module

Functional Requirements:

- Configurable test and result entry templates for various labs.
- Barcode integration for sample tracking.
- Online access to test results for authorized personnel.
- Automated interfacing with diagnostic equipment for direct data transfer.
- Test result comparison and historical tracking.

9. Operation Theatre Module

Functional Requirements:

- Scheduling system for operations with department-specific configurations.
- Real-time monitoring and recording of operation details.
- Facility for pre and post-operation documentation.

- Integration with patient monitoring systems.
- Management of surgical inventory and equipment.

10. Electronic Medical Record (EMR) Module

Functional Requirements:

- Centralized storage and retrieval of electronic patient records.
- Secure access controls based on user roles and permissions.
- Integration with diagnostic and treatment modules for comprehensive data capture.
- Customizable EMR interfaces for different medical specialties.
- Compliance with healthcare data standards and privacy regulations.

11. Medical Record Department (MRD) Module

Functional Requirements:

- Digital archiving of patient case sheets and medical records.
- Indexing and retrieval system for easy access to records.
- Integration with hospital reporting systems for statistical analysis.
- Secure and compliant management of sensitive medical records.

12. Diet and Kitchen Module

Functional Requirements:

- Management of patient-specific diet orders and kitchen operations.
- Nutritional calculator for customizing patient diets.
- Integration with patient care modules for diet-related alerts.
- Automated tallying and quality control of meals prepared.

13. Blood Bank Management System Module

Functional Requirements:

- Real-time tracking of blood stock and donor registry.
- Compliance with blood bank regulations and safety protocols.
- Integration with patient care modules for timely availability of blood

products.

- Donor management and tracking of transfusion-transmitted infections (TTI).

14. Pharmacy and Material Management Module

Functional Requirements:

- Inventory management for drugs and medical supplies.
- Automatic reorder alerts based on consumption and demand forecasting.
- Integration with billing and patient care modules for accurate charge capture.
- Management of drug dispensing and returns.

15. Central Sterile Supply Department (CSSD) Module

Functional Requirements:

- Tracking and management of sterilization processes.
- Quality control checks for sterilized items.
- Integration with operation theatre and other departments for supply management.
- Record-keeping for usage and maintenance of sterilization equipment.

16. Bio Medical Engineering Department (BMED) Module

Functional Requirements:

- Maintenance scheduling and tracking for medical equipment.
- Breakdown and preventative maintenance management.
- Inventory management for spare parts and maintenance supplies.
- Compliance tracking for equipment safety and performance standards.

17. Alert Management Module

Functional Requirements:

- System-wide alert generation for critical patient conditions and hospital operations.

- Customizable alert parameters for different departments.
- Integration with mobile and desktop interfaces for real-time notifications.
- Escalation protocols for unresolved alerts.

18. User Management Module

Functional Requirements:

- Role-based access control for various system functions.
- User activity tracking and audit trails.
- Integration with hospital identity management systems.
- Customizable user profiles and permissions.

19. Mobile Apps

Functional Requirements:

- Mobile access for patient registration, appointment scheduling, and report viewing.
- Integration with hospital systems for real-time information updates.
- Secure communication channels for patient-doctor interactions.
- User-friendly interface for easy navigation and accessibility.

20. Equipment Interfacing

Functional Requirements:

- Seamless integration between medical equipment and HIS for data transfer.
- Compatibility with a wide range of medical devices and equipment.
- Real-time data acquisition and processing for clinical use.

21. Integration with Third-Party Applications

Functional Requirements:

- API support for integration with external healthcare platforms like ABDM, PMJAY, IHIP etc.
- Data exchange protocols for secure and reliable information transfer.

- Compatibility checks and updates for third-party software integration.

22. Support for Standalone and Networked Health Facilities

Introduction: To accommodate diverse healthcare settings, this module ensures the HIS is adaptable for both standalone health facilities and integrated networks of hospitals, clinics, labs, and health centers.

Functional Requirements:

- Scalable architecture to support both single facility operations and a network of health facilities including large hospitals, health centers, labs, and clinics.
- Centralized data management system for integrated healthcare networks, facilitating coordinated patient care across different facilities.
- Interoperability features to enable seamless data exchange and consistent operations across various health facilities.
- Customizable access controls and user roles for different levels of facility operations within the network.
- Real-time data synchronization and backup mechanisms to ensure data integrity and continuity across the networked facilities.

23. Support for Health-Related Compliance and Standards

Introduction: Recognizing the importance of adherence to healthcare standards and regulations, this module ensures the HIS is compliant with international and national health-related standards like HIPAA, HL7, ICD-10 & 11, and SNOMED-CT.

Functional Requirements:

- Compliance with HIPAA (Health Insurance Portability and Accountability Act) for patient data privacy and security.
- Integration with HL7 (Health Level Seven) standards for electronic data exchange in healthcare environments.
- Support for ICD-10 & ICD-11 (International Classification of Diseases)

coding for diagnoses and medical procedures.

- Implementation of SNOMED-CT (Systematized Nomenclature of Medicine—Clinical Terms) for detailed clinical health information and terminology.
- Regular updates and audits to ensure ongoing compliance with evolving healthcare standards and regulations.
- Training modules and guidelines for staff to ensure adherence to compliance standards in daily operations.
- Robust data encryption and security protocols to safeguard sensitive health information.