Request For Proposal

for selecting

Primary System Integrator for e-Health Project

Volume 2 - Technical Specifications

eHealth Project Management Unit
Directorate of Health Services,
General Hospital Junction,
Thiruvananthapuram – 695 035

February 2014

CONTENTS

1 General System Functionalities:

The proposed solution under the scope of this specification must be agile and adaptable to change to tackle changes in processes, business rules, clinical protocols. The workflow system should be able to handle routing of documents, structured information handling, complex event processing, programmatic manipulation of information, and the ability to exchange information with web services and other external information sources.

The entire system specified in the document should be able to provide procedural automation of the existing business processes i.e. work flow activities, invocation of appropriate human and/or IT resources associated with the various activity steps. The proposed solution should be able to respond to changes of user's need.

The document has been divided in different modules for purpose of specifying different kind of business activities for ease of understanding; but each of the modules is a part of one business i.e. the providing Healthcare to citizens. The workflow system should be able to interact between different processes and data base to carry out required task. For example, to carry out Non Communicable Disease Control Programmes it is necessary for IDSP module to extract information from Medical Records to identify the Chronic Diabetes or Hypertensive Patients and combine it with demographical data of such patients derived from the Digitized family Health register and provide filtered information based on rules of Confidentiality and Privacy to the field workers for follow up and monitoring.

The effort had been made to specify such inter process interactions; however study of business process of the public healthcare domain is required by the SI agency to complete the understanding. However, Service oriented architecture is the prescribed solution for work flow implementation. SOA with its loosely coupled nature shall provide better flexibility in building applications and allow enterprise to plug in new services or upgrade existing services in a granular fashion to address the new and changing business requirements, shall bring better reusability of existing assets or investments and allow to create applications that can be built on top of new and existing applications without completely rewriting an application.

Service Oriented Architecture shall be implemented using standard set of technical specifications of Web Services to achieve a platform-neutral approach for accessing services and better interoperability. SOA should be approached based on business process as the driver and it should not be driven purely from an IT perspective (i.e., reuse only). The business process and its re-engineering would drive the abstraction of business process which in turn would drive the identification of catalog of business services, i.e. services at high granularity. Also the variables in business rules embedded in these services should be configurable and not hard-coded. The scope of integration includes establishment of Business Services following SOA principles. The solution should have a catalog of business services that are at a high level of granularity to facilitate flexibility in business processes. In addition, the solution could also have lower level

granularity of services to facilitate re- use of business functionality for the technical/IT Team. This is not mandatory but desirable.

1.1 eHealth Application shall be Cloud enabled:

The application shall be developed in a Multi-Tenant (one-to-many model) architecture where a single instance of the application software deployed on the cloud at the Data Centre shall cater to all these institutions. The application software shall be scalable and configurable for each tenant and tenant level database isolation shall also be maintained. The database shall be designed as a hybrid of SaaS maturity model 2 & 3 where various institutions are grouped and are discriminated by Tenant Identifiers. (SaaS Maturity Model 2 – Multiple database / schema for each tenant & SaaS Maturity Model 3 – Single Database for all tenants discriminated by Tenant Identifiers).

1.2 Disaster Recovery

The Entire environment at disaster recovery site is planned to be maintained as a fully working copy of Primary site.

After completion of system installation and commissioning at DR site a complete copy of database files of Primary site will be transported to the DR site in suitable Tape cartridges. This will be a onetime activity and considering the huge volume of data the same shall be copied on tapes and shall be carried to the DR site by hand rather than transporting the data communication link.

The DR site will get regular data updates from the primary site through a high bandwidth communication link so that it remains up-to-date. The methodology of replication will employ storage based replication in Asynchronous and Journal based Log Volume Shipping modes. Three way (3 Data Centers) storage-based data replication is planned to ensure zero RPO in native fashion without using any additional replication appliance.

In case of a disaster strike at primary data center, the DR site will take over and will start functioning as the primary site. The goal of disaster recovery is to restore the system operations in minimum possible time and with minimum data loss so that the business processes are not affected by the disaster.

1.2.1 RPO & RTO

Recovery Point Objective is the maximum amount of time lag between Primary and Secondary storages. eHealth PMU intends to maintain Zero RPO for all application and data at primary site. Recovery Time Objective is maximum elapsed time allowed to complete recovery of application processing at DR site. In case of a disaster, the RTO shall be measured from the time when the decision is finalized & intimated to the Agency by eHealth PMU to shift the operations to DR site. The Agency in association with eHealth PMU personnel shall ensure compliance to following RTOs –

Sl No	Application	RTO
1	Hospital Management Module	3 Hours
2	Public Health Module	6 Hours
	MIS, GIS, Maintenance Management, Asset Management, HR, Finance, General Admin Applications, FMS	24 Hours
3	Web Self service	12 Hours
4	Testing & Development system	24 Hours

The Software Application shall be compatible to the above requirements. The Primary SI Agency shall be responsible to configure the Application to conform to the above requirements during the Roll out Phase.

1.3 General Requirements:

Requirement ID	Feature	Functionality
GR.1	Vendor neutral Hardware	All the Software Applications and Modules shall be Hardware agnostic. The Applications shall be capable of being installed in industry standard vendor neutral Hardware.
GR.2	Licenses	All the Software Applications, System Software viz. OS, RDBMS, Middleware etc and COTS components if any, such as Identity and Access Management System, Mail Messaging System etc, shall have Unlimited, Perpetual, Enterprise-wide Licenses.
GR.3	Latest versions	At the time of First Rollout all the System Software viz. OS, RDBMS, Middleware etc and COTS components if any, such as Identity and Access Management System, Mail Messaging System etc, shall be the latest versions. The Primary System Integrator shall submit certificates to this effect from the OEMs for claiming the Milestone payment.
GR.4	Support for a further period of three years	At the time of handing over at the end of contract period all the System Software viz. OS, RDBMS, Middleware etc and COTS components if any such as Identity and Access Management System, Mail Messaging System etc, shall be versions with at least three more years of Technical Support by the OEMs. The Primary System Integrator shall submit certificates to this effect from the OEMs for claiming the final payment..
GR.5	Technical Support and version Upgrades	The cost of System software viz. OS, RDBMS, Middleware etc shall be inclusive of the following: 1. OEM Technical Support for the entire contract Period 2. OEM Technical Support for a further period of three years after the contract Period. 3. The Technical Support for the entire period as described above shall include cost for version upgrades. This Technical support and version upgrades include the System Software installed on various devices for the Project purpose as well.

GR.6		The licenses procured for software should ensure that in case any upgrade, patches, hot fix or a newer version of the solution is launched, it should be given to the Purchaser with no extra cost for the project period. The Supplier shall create a staging area and ensure that all the application software upgrades/releases are appropriately tested in the staging area and are applied on live instance only after such comprehensive testing. Any downtime/system outage for Application system caused by applying such patches shall be attributed to the Supplier as system downtime and shall attract penalties as per SLA

1.4 System Functionality Specifications:

Requirement ID	Feature	Functionality
SF.1	Modular Design	Applications, systems and infrastructure are to be characterized as service-oriented, component-based & reusable. The system will be modular in design, operations and implementation.
SF.2	System Architecture	The supplier is to balance the adoption of standards used by market leading vendors and products, and adherence to industry standards and open architectures. Systems are to be developed, or enhanced in such a way that business processes; application and infrastructure services and data can be shared and integrated across the Healthcare domain and with potential partners.
SF.3	Application architecture	Application architectures must be highly granular and loosely coupled. This is focused on loosely coupling systems compliant to Service Oriented Architecture to facilitate application recovery. This is to ensure that the failure of one component does not cascade to others. A tier can also be scaled to run separate applications to optimize performance.
SF.4	Web based design	All the application designed for this purpose shall be web based and the Purchaser at workstation shall be able to access through the latest available version of the web browser such as Internet Explorer, Fire Fox etc Any add-on required must be integrated with latest version released by the developer
SF.5	Business Process Requirement	Application requirements will be based on business processes and the functional requirements that derive from them. The application system should empower the Business Users in defining the business processes by process modeling.
SF.6	Data base server	The applications must be capable of running in a clustered environment as high availability configuration of database server that will run multiple workloads.

SF.7	Basic system architecture and Unified Access framework	The applications system should be built upon WS* specifications using open industry standards of Web services using XML, SOAP, WSDL and UDDI and should have the unified access framework compliant to W3C portal specifications for people, process and information by integrating the backend applications with single sign-on feature, role based, request based and hybrid user type access, searching and collaborative environment.
SF.8	Directory service	Common enterprise wide directory services shall be leveraged by all access systems and services used by all the enterprise users and adhere to commonly accepted standards such as LDAP.
SF.9	Message based interface	As per the requirement, Interfaces between separate systems (both internal and external systems) will be messaged based compliant to W3C XML standard/OPC/DDE/ODBC interface.
SF.10	Application Integration	Integration technologies must be industry proven standards. They must be scalable in capacity and provide for extensive functionality. WS* based Web Services Integration specifications shall be used for integrating disparate systems, such as : Web Services Messaging Specifications including SOAP Web Services Reliable Messaging Web Services metadata Specifications including WSDL Web Services XML Specifications Web Services Business Process Specifications including BPEL4WS Web Services Management Specifications EDIFACT and ANSI Rich Internet application
SF.11	Data Storage	Data is considered to be a DHFW wide asset and is to be shared across the Department. Data stores for transaction processing shall be kept separate from data stores for decision support.
SF.12	Data access	The applications will access data through business rules i.e. the applications must not access data directly without going through APIs managed by business rules/ validation/workflow. Data should be collected once and used many times.
SF.13	Central data storage	Data shall be stored at central data center. The Data acquisition server located at Central Data Centre will acquire the meter data at periodic interval as agreed between owner and bidder during implementation stage.

SF.14	Network environment	The application should be capable in running in a hybrid network connectivity environment i.e. Dialup, PSTN, Wireless, Leased Line, WAN environment etc. including MPLS/VPN based secured tunnel.
SF.15	Application scalability	The application portfolio and the IT infrastructure are to be vertically and horizontally scalable in size, on demand with virtualization capacity, and functionality to meet changing business and functional requirements, thereby enabling the health sector to be adaptable to change.
SF.16	Application manageability	Applications need to be designed for manageability using Enterprise Management System. This needs to encompass: scheduling, backup and recovery, application, database and network infrastructure monitoring, tuning and remote diagnostic management.
SF.17	Network option	The network will use standard, open, vendor neutral communication protocols. Considering the scale of implementation envisaged, the system will provide for various networking options between different entities. Such options would include Leased Lines, VSAT Links, Telephone Modems, through Internet, VPN etc.
SF.18	Central Administration	It will be possible to set various options and logic of the system centrally. This will ease the system administration work.
SF.19	Data Ownership	Irrespective of the Operation / Outsourcing option adopted for operation of the system, the ownership and physical possession of the data will always remain with the Department of Health and Family Welfare (DHFW). The application should provide the flexibility of system disintegration/aggregation of information and application in case of outsourcing.
SF.20	Login wise rights, groups	The system will be able to grant specific access rights to each login or group of logins, as per the business requirement and policy with unique identity across the enterprise system. System shall also permit temporary tranSFer of access rights within this group to officers for employees reporting to him.
SF.21	Data Backup	System will be required to maintain daily backups of the database on reliable backup media like DAT drives, CDs, tape etc.
SF.22	Data Archiving	The System will maintain only five years of operations data online. Operations data more than five years old would be archived and the archives maintained at the various locations.

SF.23	Interface with other system	As per the requirement, system will exist in conjunction with several other systems. It would therefore be required to interface with other systems for seamless flow of business information in Web Services or W3C XML industry format/OPC/DDE/ODBC Interface.
SF.24	Embedded control	To make the operations more efficient, the system will have the facility of incorporating embedded controls, which would force the organization to carry required tasks in the time frame specified.
SF.25	Report Generation	The system will provide a report generating tool, which can be used to generate customized reports at any level. The reports generated should be stored in various user configurable "bins". The access to bins should be configurable by having security roles in the system.
SF.26	Mail interface	The system will have the capability to interface with Open Standard mailing system to deliver the Alerts and Service Orders. The system should also be capable of interfacing with open office etc.
SF.27	Prioritizing workflow	The system will have in built priorities defined, which will be used to process the prioritized tasks first in case of system constraints (e.g. network unavailability, time constraints etc).
SF.28	Performance monitoring of system	The system should have provision for network, application, and database monitoring for performance management, tuning, remote control configuration management features with facility for SLA report generation.
SF.29	MIS Reports	The system should allow for a graphical interface to view the summary data in MIS reports. This would include trend graphs, graphs indicating how much of the target has been met etc.
SF.30	Multiple OS support/ Inter-operability.	Client End: The solution should be able to support a variety of client end Operating systems like Windows, Linux with x-windows or MAC OS. Server End: The solution should be built on open standards and interoperable platform of WS* based open specification and shall be able to interoperate with multiple operating systems like Windows, Unix and Linux.
SF.31	Multiple database support	The solution should be able to interoperate with multiple industry standard RDBMS platforms like Oracle, MS SQL, MY SQL, DB2, Informix, Sybase, Postgre or any other RDBMS confirming to ANSI/ISO SQL-200n standards and should be built on WS* based open specifications.

2 Mail / Messaging system

Introduction:

The offered messaging solution shall include the required software. The Software shall be configured in cluster mode that provides logical link between the two servers and shall ensure high availability. (Supply of Servers not in the scope of the Primary System Integrator)

Messaging Application Requirement

Requirement ID	Feature	Functionality
MMS.1	Shall support standard protocols	The mail server should support standard protocols like POP, IMAP, SMTP, HTTP, NNTP, LDAP format and communication channels like SMS / USSD.
MMS.2	Integrated calendaring feature	The mail server should have an integrated calendaring feature that is able to record meeting requests, forward meeting requests and generate alerts.
MMS.3	Should support public folders	The mail server should support public folders or discussion databases.
MMS.4	Accessible from Internet, Mobile Phones	Mail server should have an ability to be accessible from Internet and also accessible via Symbian, Pocket PC, Blackberry and Windows powered PDA's/Mobile Phones.
MMS.5	cHTML, xHTML, and HTML mobile phone browser support	Messaging Server should support cHTML, xHTML, and HTML mobile phone browser support.
MMS.6	Notifications synchronization with Pocket PC, Smart phones and other devices	It should provide with up-to-date notifications synchronization with Pocket PC, Smart phones and other devices.
MMS.7	Mail filtering functionality to separate spam	Mail server should have an internet mail filtering functionality to separate spam; the messaging server should have built-in server-side filtering and also client-side filtering.

MMS.8	Security features	The mail server should have the following security features - 1. Connection filtering 2. Sender and recipient filtering, including blank sender filtering 3. Recipient lookup 4. Real-time block list–based filtering 5. Suppression of sender display name resolution 6. Ability to restrict relaying 7. Ability to restrict distribution lists to authenticated users 8. Should support Dynamic distribution lists 9. Should support virus scanning API
MMS.9	Backup restore of open files	Should support backup restore of open files
MMS.10	Integrated authentication mechanism	Should have support for integrated authentication mechanism across operating system, messaging services
MMS.11	Replication on multiple servers	Shared folders and discussion databases should be capable of being replicated on multiple servers.
MMS.12	Disaster recovery scenarios	Should provide tools to handle disaster recovery scenarios like re-connection to the directory services user account, support for recovery of individual or group of mailboxes, support for merging or copying recovered mailboxes
MMS.13	Group collaboration, Calendaring, Scheduling	Should provide support for group collaboration, Calendaring, Scheduling
MMS.14	Support for collaborative application development, integrated workflow scenarios and Web services	Should provide support for collaborative application development and support for integrated workflow scenarios and Web services.

MMS.15	Blocking Out of Office messages	Should support Blocking Out of Office messages from distribution lists- Out of Office messages should not be sent to the entire membership of a distribution list that is listed in the To or Cc boxes.
MMS.16	Workflow applications implementation	Should support workflow applications implementation
MMS.17	Messaging Client - Webmail freeware client	Messaging solution should come along with appropriate webmail freeware client (approx 30000)
MMS.18	Messaging Client functionalities	Messaging Client suggested for working with the Server should provide for the following functionalities: 1. It should provide for rich scheduling features, including personal, group, and resource scheduling, which integrate with e mail, contacts, and tasks. 2. Sender should be able to verify which recipients have accepted, partially accepted, or declined meeting requests. 3. Users should be able to share their calendar information with others, enabling users to view multiple calendars simultaneously. 4. Recipients of meeting requests should be able to return proposals for better meeting times. The sender should be able to review all proposals before resending new meeting requests. 5. It should be possible for Contacts from the Global Address List (shared directory) to be added to personal contacts. 6. Messaging Server should provide the capability for synchronizing with Symbian, Pocket PC Client, RIM and other devices enabled with GPRS or wireless. 7. Messaging Client and Server should support Secure/ Multipurpose Internet Mail Extensions (S/MIME), enabling users to digitally sign and encrypt e-mails and attachments. 8. There should be feature for Sent messages to be recalled by the sender.

MMS.19	Directory Software	The Directory Software shall have the following functionalities 1. The Directory Server should be LDAP v3 Compliant 2. Should support partitioning into multiple LDAP Repository architectures for scalability. 3. The Directory Server should have out of the box integration with the e-mail server. Should support LDAP servers in multi master configuration 4. LDAP server should be able to replicate data between servers and support cascading replication. 5. SNMP support for flexible network monitoring and management. Support for Access Control Lists (ACLs). 6. Support for controlling access to the directory, a sub tree, entries, attributes by setting permissions for users, groups, roles and location information like IP addresses. 7. Support for user authentication through user ID/password, X.509v3 public-key certificates, or Anonymous authentication 8. Ability to keep Replicas in Synch and to enforce Replication updates 9. Should have support for open standards [LDAP v.3, XML] 10. Should have support for integrated authentication mechanism across operating system, messaging services. 11. Should support directory services integrated DNS zones for ease of management and administration/replication. 12. The directory service should support features for health monitoring and verifying replication. 13. The directory service should provide support for Group policies and software restriction policies.

MMS.20	SPAM Filter	Messaging solution should come along with appropriate SPAM filtering solution. The solution should have the following functionalities 1. Should provide at least 95% spam filtering capacity 2. should be able to block emails using both lists and preset filters 3. Should have various filtering options- a. It should have the facility to block certain specific IP addresses, certain servers, or certain email addresses (Black List) b. It should have allowing filters also (white list) depending on specific servers, IP Addresses or Email addresses. c. The solution should have dynamic list of open proxy servers and so as to block known spam senders d. Should update filtering rules automatically e. Should allow users to customize the filtering options 4. It should have customizable options to either- a. Redirect all spam mails to one mail ID b. Save spam mails to hard disk c. Delete all spam mails automatically d. Quarantine spam outside users inbox 5. Should allow the users to view blocked mail through graphics on/off 6. Administrative features a. Group policies to manage filtered mail b. Should have Automated filter delivery and deployment facilities c. Filtering customization d. Multiple quarantine choices (Email Client based quarantine, web based quarantine) e. System monitoring (examining logs, producing detailed logs etc) f. Should have Centralized Web-based administration

MMS.21	Integration with MSDG	The messaging system shall be integrated to the Govt. Infrastructure Facilities like MSDG (Mobile e-Governance Service Delivery Gateway).

3 GIS

The proposed e-health application system need to use the common infrastructure provided by the KSDI (Kerala State Spatial Data Infrastructure). KSDI shall act as the Geo-portal for the state and Data Clearing house to support Open Geospatial Consortium (OGC) compliant web services with advanced geo-processing capabilities. SI should integrate with the KSDI using OGC compliant web services and also create DSS for the health related reporting & analytics. Following are the information regarding the KSDI platform.

KSDI Infrastructure Information:

User access to KSDI will be through a web-access on a network. Users will have to register and log-in to access KSDI Metadata, Data and Application services. From a security perspective, server login identification, verification, authentication and single sign on authentication would be designed and a LDAP- active directory would be the basis for the security server, along with the security module developed for the KSDI. Security features will be compatible with LDAP (Light Directory Access Protocol) and Microsoft's Active Directory, and would enable the establishment of a single sign-on security and authentication scheme. In this architecture, KSDI web-gateway and its user interface allow a user to query distributed collections of spatial information through their metadata descriptions. This spatial information may take the form of ―data‖ or of services available to interact with spatial data on the different data server, described with complementary forms of metadata. A user interested in locating spatial information uses a search user interface, fills out a search form, specifying queries for data with certain properties.

The search request is passed to the Metadata Server, which shall search the Metadata repository on its end.

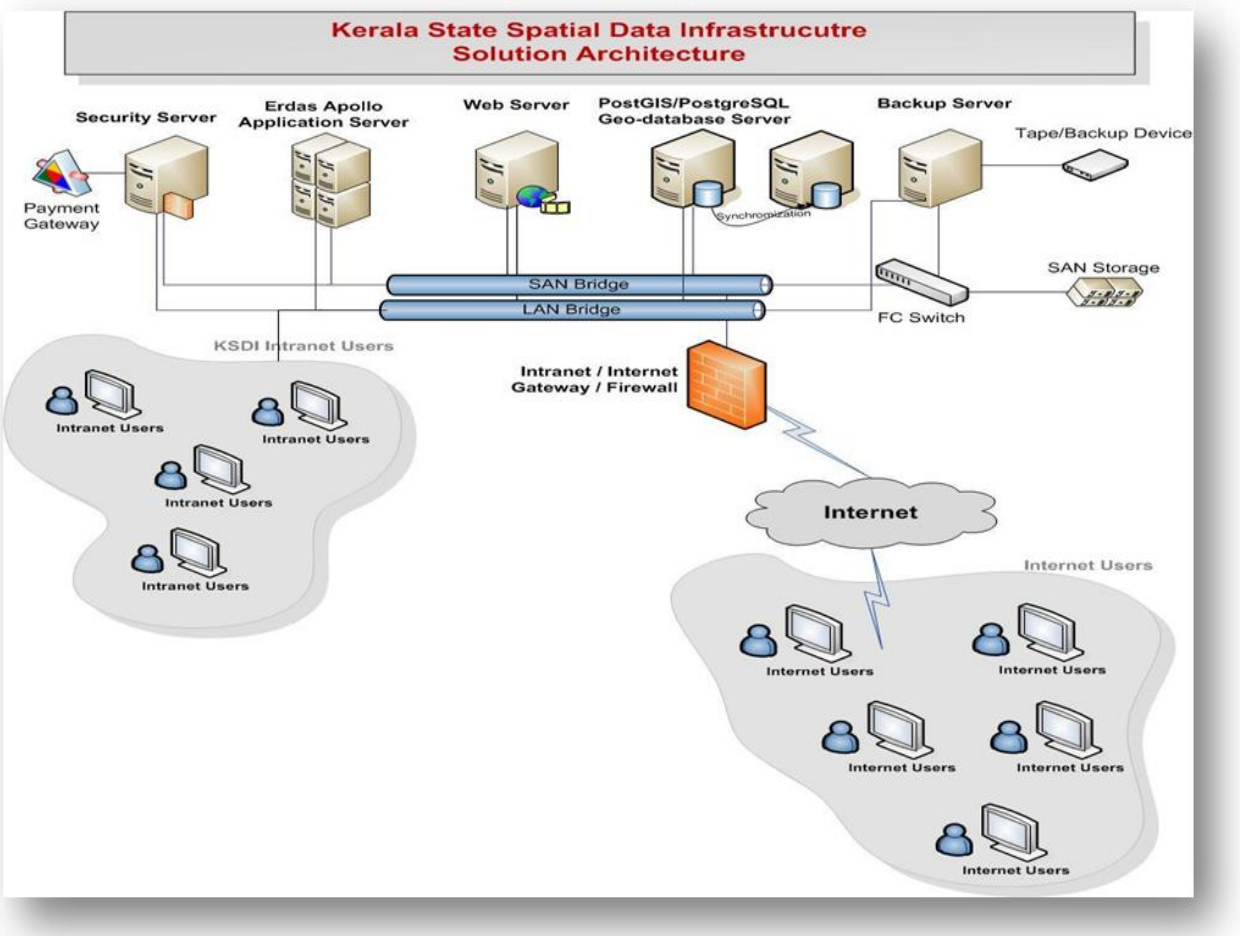
The **Web-Server** will be the main entry-point and will be a robust server behind a firewall and host the static web-pages of KSDI and also the dynamic Geo-Portal. The Web server will host the Geo-Portal application. User will connect to this application over the network. Only authorized users will have access to the Portal services.

The **Security Server** will verify and authenticate all transactions of log-in and subsequent traffic clearance so that utmost security is built in. Within KSDI, the web server would be connected to the security server and in turn to the application server. Security servers serve the purpose of keeping the data safe from intrusion/misuse/snooping and for identity management.

The **Database server** is the 3rd layer and would host the PostgreSQL RDBMS and all KSDI data as required. The spatial data stored in the Database server shall be scalable to cater to large volumes of vector data of other agencies hosted on the web in future.

The **Application server** would be housing the Erdas Apollo Enterprise and host the Geo-portal solution. The Metadata Application, DSS and any other GIS Application would be hosted on the Application Server.

KSDI Architecture Diagram:



The server components, i.e., the Geoportal server, the Application server and the Data Server, forms the KSDI server architecture, hosted on windows platform.

The GIS solution for eHealth shall display the following in a GIS Map:

1. Location of all entities covered in the Family Health Survey. The Family Health Survey is carried out using Hand Held Devices (HHD) with GPS. The longitude and latitude of all public places and house holds covered in the survey shall be captured and plotted in the GIS Map.
2. Location of Public health institutions
3. Data pertaining to each of the above entities displayed in the map shall be fetched from the database and displayed as required by the user

The following are the functionalities out of the GIS interface:

Requirement ID	Feature	Functionality
GIS 1.1	Sorting & viewing capability of any area	Sorting and viewing ward/Panchayath/District wise citizen/patient details should be possible on request.
GIS 1.2	Color Graphic Display of System Network	Color graphic displays and Color Coding: The database shall generate color graphic displays of the system components which can be zoomed in / out. This shall represent each of the elements in the healthcare institutional network with suitable differing colors for the elements. The colour coding will be based on the type of institution / Facilities available or any other chosen parameters by user.
GIS 1.3	Capability to provide customer details DT wise	Details of Customers: It shall be possible to get a view of the details of citizens/Patients attached to a particular healthcare institution in a list form using a pointing device.
GIS 1.4	Capability to provide query regarding Healthcare institution	Menu driven institution query: It shall be possible to zoom in / out on a particular Healthcare institution to obtain the desired degree of information. Menus shall be provided for viewing various combination of information related to any group of Healthcare institution. For example, it shall be possible to view only those Healthcare institution in a District which has Blood bank.
GIS 1.5	System capability of representing data of internals of any healthcare entity	The proposed system should have facility of representing data pertaining to the internal organisation of any Healthcare Institution. For example, with a click of mouse on the Healthcare Institution user should be able to see all the departments in the Institution and on taking the pointing device to a specific department, a 'pull down' menu to show user options such as List of Doctors, Other facilities, Bed strength etc to be displayed on request. The internals visible on clicking on the Healthcare Institution should be dynamic in nature and not merely static snap-shots.

4 Identity and Access Management System:

Privacy of Medical Records is of prime importance. The Identity an Access Management System shall ensure that only authorized users shall access the Medical Records. The basic principle in deciding access shall be 'need to know'. Only those users who actually have a 'need to know' the information alone shall be provided access the information. The system shall have facility to differentiate users based on functionality (such as Nurses, Doctors, Lab Technicians etc) and provide restricted access to specific data as required for performing those specific functions. For example a Nurse may not necessarily require all Medical Data as compared to information required by a Physician.

The detailed requirements of IAM Module is given below.

Requirement ID	Feature	Functionality
IAM.1	**Adapter/ connector Support**	
IAM.1.1	Solution Compatible	The proposed solution should be compatible on all the operating systems offered by the bidder in the proposed solution including client machines.
IAM.1.2	Out of box Workflow	Identity management for user provisioning should have out of the box workflow for automating approvals for user access management, self registration and self-care functionality for reducing the administrative load and manual intervention.
IAM.1.3	IDE to design Work - Flow	The solution should provide an IDE to design the workflows.
IAM.1.4	Standard for Workflow implementation	The proposed solution should support "Workflow Management Consortium (WfMC) TC-1003 Workflow Reference Model standard for workflow implementation".
IAM.1.5	Connector availability for target systems	Identity Management Solution should have Connector availability for all target systems that need to be managed.
IAM.1.6	Connector development tool	The proposed solution Should provide resource kit or an SDK to add new Resource adapters.
IAM.1.7	Agent-less Architecture	Identity Management solution should be Agent-less Architecture and use gateways where agent is required.

IAM.1.8	Certification	The Proposed solution should be certified as"Liberty Interoperable" and should be interoperable with other products / solution based on SAML 2.0 specification. A few typical profiles given below: 1. Identity Provider 2. Identity Provider Extended 3. Service Provider 4. Service Provider Complete 5. Service Provider Extended 6. ECP 7. Attribute Authority Requester 8. Attribute Authority Responder 9. Authorization Decision Authority Requester 10. Authorization Decision Authority Responder 11. Authentication Authority Requester 12. Authentication Authority Responder 13. POST Binding 14. GSA Profile
IAM.1.9	Indexing	The solution should leverage an intelligent indexing system to manage user identities and access privileges, leaving account information with the information owner and thus avoiding the time- consuming effort of building and maintaining another user repository.
IAM.1.10	Discovery and Correlation of user Account	The proposed solution should provide an automated way to discover and correlate all accounts associated with an individual to speed the account mapping process.
IAM.1.11	User Repository	The solution should use separate repository for user data and audit log information.
IAM.1.12	Open Provisioning	The solution should support open provisioning standard like SPML.
IAM.1.13	Authentication/authorization framework	The solution should allow Enterprise applications and platforms to integrate into the centralized authentication/ authorization framework seamlessly. The solution should support both thick client as well as web based applications.
IAM.1.14	Access Management	The Access Management solution should be capable of running on web servers as well as application servers.

IAM.1.15	Pluggable authentication module	The proposed solution should provide the ability for pluggable authentication module, and new auth modules should be able to be added via an SDK.
IAM.2	**Access Rights Capabilities and Access Control**	
IAM.2.1	Data Protection	Sensitive Medical Records data must be protected in accordance with guidelines that will be agreed with eHealth PMU.
IAM.2.2	Entry screens	On completion of successful logon, the following information shall be displayed : • Date and time of previous successful logon. • Details of any unsuccessful logon attempts since the previous successful logon. • Reminder of the onus of the user to bring to notice any aberration observed.
IAM.2.3	Unsuccessful logon attempts	After predefined number of consecutive unsuccessful attempts to logon to a user Id, that user id shall be disabled against further use until the same is enabled by System Administrator.
IAM.2.4	Application time out	Terminal / User Id time-out shall occur if a terminal / user ID remains logged onto a system/ application but remains inactive for a predefined time. If the terminal is dedicated to one application then timeout shall occur after predefined time inactivity. The screen shall be cleared of any information when time out occurs.
IAM.2.5	Limited application software on key systems	Software which can be used to Modify existing programs on systems /applications, e.g. editors and compilers, shall have access restricted to authorized staff only. Any such software which is not needed for operational reasons shall be removed after the modifications have been made.

IAM.2.6	Segregation of Duties	Clear segregation of duties between user groups is necessary to minimize the risk of negligent or deliberate system misuse. In particular segregation must be implemented between : 1. Clinical Management Use 2. Business use. 3. Functional Audit 4. Computer operations. 5. Network management. 6. System administration. 7. System development & maintenance. 8. Change management. 9. Security administration. 10. Security audit. Where it is operationally not possible to adhere to this policy advice shall be sought from eHealth PMU. As a minimum, when there is a combining of privileges violating the above segregation then there shall be an audit trail and an approval process by a higher authority.
IAM.2.7	Communicating usage restrictions	A prescribed warning screen shall be displayed immediately after a user successfully completes the logon sequence to any multi user system, server or database. This does not apply when logging onto a PC, which cannot be accessed via any other means, or when logging onto a network where no information is available without further logon (note: the screen should be presented after this further logon). This screen will emphasize the requirement to comply with requirements on usage of computer as laid down by the eHealth PMU. The screen will require confirmation that the user has understood these requirements prior to proceeding.
IAM.2.8	Controlling User access	The system shall provide a mechanism to authorize users to access the system, revoke users from accessing the system, and modify the security information associated with users. The system shall also be able to automatically suspend or roll back a reconfigured account that violates policy.
IAM.2.9	Restricted access to resources	The system/resources shall provide a mechanism to allow or deny specified user IDs to access the system during specified ranges of time based on time-of-day, day-of-week, and calendar date.

IAM.2.10	Console operations for privileged users	The system shall provide a mechanism to allow or deny specified user IDs to access the system based on means of access or port of entry.
IAM.2.11	Resource, access control list	For each resource, the system shall provide a mechanism to specify a list of user IDs or groups with their specific access rights to that resource (i.e. an access control list). Solution shall provide for grouping of users and assigning ACL to the group.
IAM.2.12	Group ACL vs individual ACL	Group ACL should be aggregated to individual user ACL and in case of conflict, users ACL shall govern.
IAM.2.13	Grant and deny access	System shall provide both Grant and Deny to a resource.
IAM.2.14	Individual access rights to users	The system shall have ability to assign users individual access rights and to define access rights available to users in a role upon their request and approval by a higher authority.
IAM.2.15	Job based access to information	The system shall have ability for different personnel to view different levels of information based on their job duties. For example Doctors, Nurses, Lab Technicians, Pharmacists etc shall have different access levels so that information is displayed based on a 'Need to Know' basis.
IAM.2.16	Modifications to the access list	The system shall provide a mechanism to modify the contents of a resource's access control list.
IAM.2.17	Change in Access rights	The System shall have ability to associate access-rights definition with a role within the organization and dynamically and automatically change access rights based on changes in user roles. The system shall also have ability to set designated times for changes in access rights or policies.
IAM.2.18	Rules for routing approvals	System should also use defined rules / information specific to public healthcare domain to determine routing of approvals.
IAM.2.19	Access rights change notification	The system shall be able to Compare local administrator changes against a system-of-record of account states to determine if changes comply with approved authorities and policies and shall be able to notify designated personnel of access- rights changes made outside the provisioning solution, if any.

IAM.2.20	Audits on user accounts	The solution should provide the capability to do half yearly audits on the lines of ISO 27001 for user accounts.
IAM.2.21	Resource ownership	The system shall provide a mechanism to identify all resources in the system that are owned by a specified user ID, the resources to which that user ID is allowed access and the specific access rights for each resource.
IAM.2.22	Users authority changes	System shall also be able to detect, evaluate and respond to user authority changes made directly to a resource.
IAM.2.23	Restrictive access	Each resource delivered with the system shall have the most restrictive access rights possible to permit the intended use of that resource.
IAM.2.24	Restricted access to access control information	The system shall protect all information used for resource access control decisions (e.g., access control lists, groups lists, system date and time)
IAM.2.25	Policy simulation	The system shall provide policy simulation and 'what-if' modeling of changes, i.e. simulation of effects of policy changes before they are enacted, reporting errors, or potential problems, and ability to resolve before live operations.
IAM.2.26	Monitoring of access controls	The system shall monitor the following:- 1. Successful logins and login attempts e.g. Wrong user ID /Password, and login patterns 2. Rejected access attempts because of insufficient authority 3. All usage by privilege users e.g. Powerful access to system utilities or applications 4. Use of sensitive resources e.g. Access to highly sensitive data 5. Change to access rights of resources 6. Changes to the system security configuration 7. Modification of the package software 8. Changes to user privileges.
IAM.2.27	Reporting on user roles and rights	The system shall have ability to report on roles, rights associated with roles and users associated with roles.

IAM.2.28	Flexible connection to multiple data stores	The system shall have flexible mechanisms to connect to multiple data stores containing accurate information on valid users.
IAM.2.29	Identity store information in real time	The system shall have ability to load identity store information on a scheduled bulk basis and to detect and respond to identity store changes in near real time.
IAM.2.30	Retrieval of account information	The system shall have ability to retrieve account information from target managed resources on a scheduled basis, both in bulk or in filtered subsets to preserve network bandwidth.
IAM.2.31	Real-time local administrator account maintenance	The system shall have ability to detect and report in near real- time local administrator account maintenance (creation, deletion, changes) made directly on local resources natively.
IAM.2.32	Support for prerequisite services	The system shall define services that must be granted prior to creation of the access rights. (each characteristic of an entitlement may be set to a default value, or its range can be constrained, depending on the capabilities of the entitlement to be granted)
IAM.3	**User Management**	
IAM.3.1	Creation of standard User Profile	A mechanism must exist to allow a range of User Ids to be built with a standard user profiles of multiple categories.
IAM.3.2	Dormant User	Where a user Id remains unused for a pre-specified number of consecutive days, it shall be disabled. If no authorized request For reinstatement is received within a further predefined time period, the user Id shall be deleted from active user list. The user would be informed before this happens.
IAM.3.3	Segregating user access to system	All user Ids shall be set up with privileges that limit the use of the user Id to designated areas only and to ensure that other functions cannot be performed by the user ID for which they are not authorized. Some user IDs have powerful privileges associated with them and these shall only be provided and maintained by the system administrator. To prevent the provision of user IDs with privileges associated to them, when these are not required by the user, any templates used to set up user IDs shall have no default privileges associated with them.

IAM.3.4	Unique User ID	System shall be able to create unique user IDs using a set of consistent algorithms and defined policies of the owner and not in current use or previous use by the organization and not shared with others. The system shallprovide a mechanism to associate specified information (e.g., user name and affiliation) with each user ID.
IAM.3.5	ID Conventions	Procedures for user account management should define the naming convention for user IDs and the operations practices for provisioning and removing these user Ids.
IAM.3.6	Differentiating normal and privileged Users	User Ids shall not consist of less than a predefined number of characters. The number of characters would be different for normal users and privileged users;
IAM.3.7	Single account with multiple authorities	The system shall have ability to create a single account with multiple authorities governed by different policies.
IAM.3.8	Temporarily Disabling	The system shall provide a mechanism to administratively disable user IDs and a mechanism for re-enabling or deleting a disabled user ID after a specified period of time. The use of this mechanism shall be privileged.
IAM.3.9	Active Users	The system shall internally maintain the identity of all active users.
IAM.3.10	Tracking User IDs	The system shall provide a mechanism to obtain the status of any user ID.
IAM.3.11	Grouping User IDs	The system shall provide a mechanism that allows a collection of user IDs to be referenced together as a group.
IAM.3.12	Limiting multiple log on	For those systems that have the architecture to support multiple logons per user ID, the system shall provide a mechanism that limits the number of multiple logon sessions for the same user ID. The mechanism shall allow limits for user IDs and groups to be specified. The system default shall limit each user ID to one simultaneous logon session. As per business process requirement, particular machine IDs to permit login by selected users only.

IAM.3.13	Associating IDs to processes	The system shall provide a mechanism by which the user ID associated with a process can change to a user ID that would provide any additional privileges.
IAM.3.14	Assignment of one or more roles to users	The system shall be able to assign users to one or more roles and can implicitly define subsets of access to be unavailable to a role.
IAM.4	**Self Regulation User Administration capabilities**	
IAM.4.1	Adherence to open standards	The system shall adhere to open standards.
IAM.4.2	Secure Environment	The system shall have secure environment for transmitting access changes across the Internet.
IAM.4.3	Protection of private user information	Protection of private user information through secure facilities and sound processes.
IAM.4.4	Reporting of user rights	Reports of user rights into external systems, sponsors of users and audit trails of access rights changes.
IAM.5	**Authentication**	
IAM.5.1	Authentication mechanism	The system shall provide a mechanism to authenticate the claimed identity of a user.
IAM.5.2	Single authentication procedure	The system shall perform the entire user authentication procedure even if the user ID that was entered was not valid. Error feedback shall contain no information regarding which part of the authentication information is incorrect
IAM.5.3	Modification Ability to authentication	The system shall provide a mechanism to support the initial entry or modification of authentication information.
IAM.5.4	Privileged access to authentication	The system shall require a privilege to access any internal storage of authentication data
IAM.5.5	2-Factor authentication	System should support two factor authentications (Biometrics, tokens etc.)

IAM.6	**Password Management**	
IAM.6.1	Password confidentiality	System shall be able to securely deliver User Ids and passwords to new users electronically. User Ids and passwords, when conveyed electronically shall only be visible to the person for whom they are intended e.g. after the user has logged on to the appropriate electronic system.

IAM.6.2	Password protection	All electronic information systems and applications shall have a password management system which meets the following requirements : 1. Enforces change of initial password at first logon. 2. Allows users to select and change their own passwords at any time subsequently. 3. Have ability to implement password formation rules to enforce password strength across the organization, e.g. minimum character length of password, password as a combination of numeric, alphabets & special characters 4. Have validation routines built in which, as far as possible, check that the password selected is a quality password as defined in a Policy Document to be handed over to the Purchaser at the time of implementation. 5. Have a confirmation process on changing passwords to cater for typing errors, 6. Have ability to deliver password-change success/ failure status to requestor electronically 7. Have the ability to enforce password change after every n days. if the password is not changed in the pre specified number of logins then the ID should be disabled requiring re- enabling by System Administrator. 8. Prevents reuse of passwords within a specified period/ number of times. 9. Does not echo passwords to screen or paper. 10. Stores passwords in a one- way encrypted form away from the system/ application data files in a protected password file that is access controlled such that no users can read or copy the encrypted contents. 11. Prohibit use of null passwords 12. Have ability to synchronize passwords for multiple systems to the same value to reduce the number of different passwords to be remembered by the user 13. Have a challenge-response system to authenticate a user with a forgotten password by using shared secrets
IAM.6.3	Unique passwords	The system shall provide no mechanism whereby multiple user IDs explicitly shares a single stored password entry. The system shall provide no means to facilitate the sharing of passwords by multiple users.

IAM.6.4	Clearing passwords	The system shall allow a user to choose a password that is already associated with another user ID. The system shall provide no indication that a password is already associated with another user ID.
IAM.7	**Directory Services Requirements for Enterprise -**	
IAM.7.1	LDAP and Open Standards	• The Directory Server should be LDAP v3 Compliant • LDAP server should be able to replicate data between servers and support cascading replication. • Should have support for open standards [LDAP v.3, XML]
IAM.7.2	Group Policies Management	• The directory service should provide support for Group policies and software restriction policies. • The group policies should have settings to configure various desktop or user related settings via centralized control. These settings will include items like Browser setting, desktop restrictions, program restrictions, admin controls, software deployment etc. It should allow for almost all manual functions to be automated using group policies.
IAM.7.3	Integration	• Should have support for integrated authentication mechanism across operating system, messaging services. • The Directory Server should have out of the box integration with the e-mail server. • Should provide enhanced authentication like Kerberos which support authentication across multiple Operating system like Windows and Unix/Linux. • Should be able to integrate with other Standards based Directory system for synchronizing user accounts and passwords.

IAM.7.4	Management	• SNMP support for flexible network monitoring and management. • Should support directory services integrated DNS zones for ease of management and administration/replication. • The directory service should support features for health monitoring and verifying replication. • The directory service shall provide support for modifiable and extensible schema
IAM.7.5	Access Control	• Support for Access Control Lists (ACLs). • Support for controlling access to the directory, a subtree, entries, attributes by setting permissions for users, groups, roles and location information like IP addresses. • Should provide facility to provide Rights Management Service for documents like Word, Excel etc on the built on standards like XRML.
IAM.7.6	Multi Factor Authentication	• Support for user authentication through user ID/password, X.509v3 public- key certificates, or Anonymous authentication • Should support security features, such as support for Kerberos, smart cards, public key infrastructure (PKI), and x.509 certificates
IAM.7.7	High Availability	• Should support partitioning into multiple LDAP Repository architectures for scalability. • Should support LDAP servers in multi master configuration • Ability to keep Replicas in Synch and to enforce Replication updates
IAM.7.8	Administration	• The solution should provide a comprehensive single window Admin tool locally or over internet to administer the directory services. • The Directory services should have APIs to programmatically manage each component of Directory Service. • The directory service shall provide support for modifiable and extensible schema both manually and programmatically

IAM.8	**Audit Trails & Reports**	
IAM.8.1	Time-stamped records	The system must maintain- • Time-stamped recordsof every access change request, approval/denial, justification and change to a managed resource • Time-stamped record of every administrative and policy-driven change to access rights
IAM.8.2	Audit Trail reporting	The system must provide reports on audit trails for users, systems, administrators and time periods, including workflow approvals, rejections, request statistics, policy compliance and Audit reports, User account reports, Access reports and Service reports and also any customized reports based on specific need.
IAM.8.3	Maintaining audit trails	Audit trail records shall be retained in a tamper proof environment in accordance with the Purchasers policy for a reasonable amount of time as per e-Governance Policies to allow for accountability and evidential purposes. Backup copies shall also be maintained to protect against any accidental or deliberate erasure of data.
IAM.9	**Distributed Administration**	
IAM.9.1	Defining of organizational structures	Ability to define organizational structures based on the access- granting authority
IAM.9.2	Delegation of administrative tasks	Ability to delegate each administrative task with fine- grained control at Organizational Unit Level so that the team or Dept Admins can completely perform the Administrative tasks for their Organization Unit.
IAM.9.3	Access to delegated capabilities over	Ability to access all delegated capabilities over the Web via Web Browser with a zero-footprint client.
IAM.9.4	Web access control with single sign-on environment	Ability to incorporate Web access control with single sign-on environment and to distribute provisioning components securely Over WAN and Internet environments, including crossing firewalls.

IAM.9.5	Enterprise Single Sign On products	Ability to incorporate Enterprise Single Sign On products to include the provisioning solution within the Thick client single sign-on environment.
IAM.9.6	Custom user authentication approach	Ability to incorporate custom user authentication approaches commensurate with internal security policies and to create private, filtered views of information about users and available resources.
IAM.9.7	Ability to import and export configurations	Ability to import and export configurations to enable migrations between Development, Staging and Production environment without delays.
IAM.10	**System Operations**	
IAM.10.1	interaction with target resources	Ability to interact with target resources without interfering with their performance.
IAM.10.2	Operation for temp inaccessible system	Ability to continue to operate without degradation when the managed system is temporarily inaccessible.
IAM.10.3	Function if provisioning solution unavailable	Ability for the managed resources to remain fully functional if the provisioning solution is unavailable
IAM.10.4	Users interaction with provisioning solution	Responsiveness to users interacting with the provisioning solution features for searches, reporting, approvals, self-service and auditing.
IAM.10.5	Synchronization with user information	Ability to load and maintain synchronization with user information from existing human resources and other identity systems, both statically and dynamically.

IAM.10.6	Account and authorization information from existing systems	Ability to load account and authorization information from existing operational systems without data entry
IAM.10.7	Reconcile accounts created by other adm. systems	Ability to detect and reconcile accounts created by, and/or changed by, other administrative systems (e.g., the local administration console provided with the managed resource)
IAM.10.8	Support for configuration and scalability requirements	Support for configuration and scalability requirements for large environments and high-availability operations utilizing shared communication capacity on corporate WANs.
IAM.10.9	End-to-end security	End-to-end security over account changes.
IAM.10.10	Web-based functionality	Entirely Web-based functionality to allow easy distributed administration on an unlimited scale.
IAM.10.11	Integrated functionality w/o duplicate data entry	Integrated functionality that does not require duplicate data entry or manual synchronization of information shared for multiple functions.
IAM.10.12	Server configuration for high availability operation.	Ability for serversto be inexpensively configured for high-availability operation, including disaster recovery.
IAM.10.13	Utilized data store configuration for high availability operation.	Ability for utilized data stores to be configured for high-availability operation.
IAM.10.14	Accuracy in provisioning solution	Ability for provisioning solution to maintain accuracy when local administrators maintain privileges to make changes to target resources.

IAM.10.15	Resilient Communication's design	Resilient communications design between distributed components to withstand network or target resource outages.
IAM.10.16	Multi-layered security architecture	Multilayered security architecture for operation in a demilitarized zone" ((DMZ) and for management of users and systems in untrusted environments.
IAM.10.17	Interaction with external systems	XML-based extensibility and interaction with external systems
IAM.10.18	common and de facto standards	Use of common and de facto standards for interfaces that are internal and external to the provisioning solution.
IAM.10.19	Integration of LDAP directory services	Integration of LDAP directory services as identity stores, access control system authorization stores and internal user account and policy stores.
IAM.10.20	audit trails and system recovery	Inclusion of a persistent data store or repository for audit trails and system recovery.
IAM.10.21	Quick response to user interactions	Ability to respond quickly to user interactions including report requests, access change requests, policy changes and password self- service.
IAM.11	**4.1 Security and Access control for Patient data**	
IAM.11.1	Patient Data Access Control	Patient data is confidential and is governed by privacy and confidentiality regulations. Hence a robust confidentiality and privacy framework specifically designed for the Security and Access control is required for Patient data.
IAM.11.2	Implied Consent	1. Once a patient seeks an appointment with a specific doctor it is deemed that the patient has provided a consent for that doctor to see his clinical records 2. Once a patient has been admitted to a hospital it is deemed that the patient has provided consent to the doctors, consultants and nursing staff associated with the hospital to view his records

IAM.11.3	Doctor specific Appointments	The documents on the local system can be seen only by the doctor with whom the appointment has been fixed or the patient has been routed to after due information provided to the patient. (e.g: Patient comes and asks for a gynecologist and not a specific doctor. The reception tells the available doctors and then with patient consent routes her to the patient queue of the next available doctor. In this case this shall be treated at par with implied consent at par with the patient consent to meet the specific doctor after information of availability. The patient can decline and provide his/her preference. If the patient still does not give any preference for a specific doctor, then the patient will be seen by the first doctor who becomes available for consultation and the data will be accessed by her. In some Government hospitals this facility to choose doctor is not provided. The patient has to report to the first doctor who is available for consultation as per the first-cum-first-served queue management system
IAM.11.4	Encounter specific association	The requester from the hospital requesting documents from central repository should specify the attending physician. This will create an encounter specific association with the patient authorizing the doctor to see the associated documents except for the confidential marked documents.

IAM.11.5	Confidential Records	Certain specific records shall be marked confidential by default some examples of such records include the following • HIV related • Domestic violence related • Veneral and STD related • Reproductive health related • Addiction related • Psychiatry related Additional categories can be provided at the design stage In addition to these the patient can request attending physician to mark certain document confidential. These documents can be seen in existence as a patient confidential records and an informed consent shall be received before access by the doctor after doctor's discussion with the patient The original author of the document should be able to access his authored documents for the patient, unless patient decides to revoke and mark these confidential. In this scenario we will be able to have original psychiatrist access patient's relevant records while restricting access to others.
IAM.11.6	System warnings on privacy and confidentiality	The documents requested by the local system shall be audited and provide system warnings on privacy and confidentiality related alerts

IAM.11.7	VIP records	Certain records shall be treated as VIP records and a more stringent documented consent shall be followed. o Village panchayat President or Member can be a VIP in their associated PHC. In that case the records shall be tightly controlled and restricted to the associated doctor in the PHC with the VIP patient tag o For other eminent citizens or persons holding public positions, medical record should follow a written consent for these patients and additional authentication should be imposed for doctors to see their records. These interactions on VIP records should create appropriate audit trail of transactions conducted.
IAM.11.8	Overriding confidentiality restrictions	The system shall have a facility to allow the doctor to override all these confidentiality restrictions and view the Medical records of a Patient in case of emergency. The system shall require the doctor to specify the reason for exercising this override facility. An audit trail of this shall also be maintained by the system.

5 System Security Requirement

Requirement ID	Functionality	Description
SS.1	**Audit Trails and Reports**	
SS.1.1	Tracking key system accesses	The system must be capable of generating log trails, which contain details about any read / write access to sensitive data. Details must relate activity to an identifiable person. They must be configurable, so that filters and switches can be used to lower performance overheads and focus on areas of concern. It is important that the audit trail that is generated contain enough information to support after-the- fact investigation of loss or impropriety.
SS.1.2	Time-stamp based auditing method	Where equipment uses a real- time clock to timestamp audit and other time related events, the clock should be regularly checked for synchronization with both connected systems and reference clock outside of the system, in this case the Indian Standard time. For daily reporting, this would ensure that the reports generated have some sanity given continuous data input

SS.1.3	Exception reporting	Where the security audit trail becomes unavailable for any reason, the system shall continue to operate but will trigger an alarm. Action shall be taken as soon as possible to rectify the situation
SS.1.4	Detailed system access tracking	System and application use and attempted use will be monitored to ensure that the integrity and security of the client and customer data is maintained. The documented process shall include details of: who will monitor what event and how, the frequency of monitoring, what to do when suspicious activity is noted, when to escalate and the escalation path. All events logged in the audit data shall be taken into account when deciding what to audit and the appropriate actions to take. The log must record the user or process responsible for the event, terminal ID where available, and the date and time of the event The following shall be monitored :- Enabling and disabling of the audit process Any changes to the type of events logged by the audit trail Any changes to the audit trail itself Start up parameters and any changes to them
SS.1.5	Maintaining audit trails	Audit records and journals shall be retained in a tamper proof environment in accordance with the Purchaser‟s policy for a reasonable amount of time to allow for accountability and evidential purposes. Backup copies shall also be maintained to protect against any accidental or deliberate erasure of data.
SS.1.6	Disaster recovery	A recovery options analysis shall be carried out to produce the practical options for those systems and networks, which are deemed to require recovery in the event of a disaster. The most effective option shall be chosen, taking into account the cost of recovery and the cost to the business of unavailability of the
SS.2	**System Integrity**	
SS.2.1	User process protection	The system should be able to protect the user process and local data from other user.
SS.2.2	Version consistency checks	Mechanisms should be in place to ensure that the currently installed software has remained consistent with the delivered product.
SS.2.3	Versioning	Software used on systems/ applications shall be subject to version and change control to ensure that only the current authorized software is used at all user location.
SS.2.4	Modification of the system	Modification or replacement of the software provided with the system would require special privileges
SS.2.5	System maintenance	Execution of system maintenance and repair software would require special privileges

SS.2.6	Basic checks on data input	Data input to an application shall be validated by the application to ensure that the data is correct and appropriate. As a minimum, an application shall check input data is complete. Within the required ranges, and contains no invalid characters. Procedures shall be established to deal with any input data violations.
SS.2.7	Time stamping modifications	The system should be able to track the date and time at which a resource was last modified.
SS.2.8	Integrity of data passed over a communication channel	The system should have in-built mechanisms e.g. checksums to verify the integrity of data passed over acommunication channel.
SS.2.9	Data transfer lock	Where an encryption process used for data transfer fails and cannot be automatically corrected, then the transfer should not be completed.
SS.3	**Confidentiality**	
SS.3.1	Use of encryption	The system should have the flexibility of encrypting the data stored online.
SS.3.2	Approval for cryptographic techniques	Any cryptographic techniques or encryption systems used to safeguard information shall have been approved by relevant authority on data security prior to their use.
SS.3.3	Approval for security components	Only security components which have been approved by the Purchaser shall be used to protect the Purchaser's sensitive information and processes.
SS.3.4	Documentation of encryption procedures	The procedures used to maintain confidentiality should be documented and access to them restricted.
SS.4	**Networking and Data Transfer**	
SS.4.1	Authorized data transfer	All data transfers must be documented and authorized by the owner of the donor system. They must only be authorized where the receiving system has the capability to protect the data, i.e. it has an acceptable security rating.
SS.4.2	Inter system data Transfers	Data which is to be passed between systems shall be labeled to indicate the type and sensitivity of that data. The security policy for a system will state what data may be sent to, or received from, another system and will state the translation, if any, between the labeling of the two systems. Interfaces that have been built - i.e. the data migration systems should have defined access rights. The interfaces should have a fixed enabling procedure - including the frequency with which the migration happens to and from the system, the data flow that would happen and the data items that would be frozen during such a

SS.5	Customer needs	
SS.5.1	Documentation of risks and its mitigation	System developers responsible for customization should consider and document the risks and associated mitigation in the design.
SS.5.2	Installation and configuration	Developers will document instructions on how the system is to be delivered, installed and configured in a secure manner.
SS.5.3	Startup documentation	Developers will document instructions for the secure start- up, re-start and operation of the system.
SS.5.4	Interface designing	Interface designs must include the capability to selectively deny access to certain types of data.
SS.5.5	Scope control	Vendor supplied software packages must not be modified outside of the scope recommended by the Purchaser.
SS.5.6	Software change control	A mechanism for controlling software changes during development shall be implemented. This mechanism shall as a minimum ensure that : a) The change is reviewed by appropriate groups prior to authorization, b) Changes are properly authorized prior to implementation, c) All change requests are logged. d) All associated documentation is altered along with the software change. e) Version control records are maintained.
SS.5.7	Internal data	All applications shall be designed to minimize the risk of corruption by processing errors by building in validation checks, reconciliation checks etc., where necessary.
SS.5.8	Module and product testing	All new and modified software to be used on system/application shall first be tested by expert personnel to ensure that the software have been subjected to the rigor of test and thereby - a) Does not introduce added security risks b) Functions according to design specifications c) Does not adversely affect the operation of the system d) Introduces no unauthorized system changes.

SS.6	**Security of web services**	
SS.6.1	XML based Web security schemes	As web services have certain limitations with SSL type of security scheme, the web service technology shall be used with different XML-based security schemes. Some of the XML-based securities include the following – WS-security XML digital signature XML encryption XKMS (XML Key Management specifications) SAML (Secure Assertion Markup Language) ebXML Message service The bidder shall ensure content security, message level security and secure message delivery, metadata security policy, trust management and secure public key infrastructure while implementing web services using appropriate web security mechanism, which must be W3C / OASIS compliant.