My SanteMPI Deployment

Operational Architecture Documentation

[Publish Date]

[Company]

rev.

Preface

This document template should be used to plan and document your implementation of SanteMPI. The template provides useful section headings, examples, and instructions on the use. The goal of this template is to provide implementing partners with a series of considerations that should be addressed prior to installing SanteMPI specifically (and SanteDB generally).

Scope of this Template

This document is intended to be completed by a network engineer, systems architect, or enterprise architect in charge of the physical operationalization of the SanteMPI solution. The document primarily answers the questions:

* What are the physical attributes of the operational environment?
* How do the software components in the operation environment interrelate?
* What should occur in the event of a catastrophic failure of the environment? (disaster recovery and business continuity)
* What are the service level agreements in place? What are the recovery and downtime procedures in place?
* Which stakeholders are responsible for support, escalation, backup activities, etc.?
* How and when are updates and patches applied? Who is responsible for applying them?
* How are the software components configured, and why?
* Where are the environment specific considerations for deployment?
* How is this SanteMPI/SanteDB implementation integrated with other systems in the broader enterprise?
* What data is collected, forbidden, or changed from the default SanteMPI/SanteDB implementation?
* What are the security settings of the environment? How is data backed up? How often are security audits completed?

This document is one of several that should be in place and referenced by your implementation team during the operation of the SanteMPI solution.

This differs from other types of architecture documents you may have seen such as:

* Enterprise Architecture: Your jurisdiction/organization/country may have a broader eHealth enterprise architecture document (or collection of documents). This document will make references to the broader enterprise architecture, however it specifically concerned about the SanteMPI/SanteDB solution within the context of that broader architecture. Whereas the Enterprise Architecture document brings together business units, systems, and logical roles this document focuses on technical operationalization.
* Software Architecture: SanteMPI and SanteDB provide Software Architecture Documentation[1] on the wiki. Additionally, any customizations performed by the SanteSuite team (or your in country team) should have further documentation of the custom software enhancements. This document differs from software architecture in that software architecture’s primary concern is that of describing the function, solution, and use of units within the software package. This document may reference software architecture documentation.
* Data / Information Architecture: Your country/jurisdiction/organization should have data information architecture. SanteDB provides Data and Information Architecture Documentation[2]

Using this Template

This template provides section headings and descriptions of use of each section. The process of creating an operational architecture will depend on:

* The capacity of the operational environment into which the solution is being deployed, for example:
  + Public or Private Cloud Environments
  + Centralized, On-Premises Environments
  + Shared or Leased Environments (i.e. physical servers at an external data center)
* The features which are enabled in the operational environment
* Local legislation and policy requirements of the implementation
* The use cases implemented, as well as in-country workflows.

Implementers are encouraged to work through the document in an iterative fashion with relevant stakeholders. Each section includes instructions which include hints about the types of questions which should be answered by the section.

Template instructions will appear in italics, and in the purple color. You should remove these instructions prior to publishing of the documentation.

The template provides example content describing an operational environment from the fake country Demoland. You can use the content in blue as a guide for writing, diagrams, etc. The examples use the style **Example Content** , you can remove all example content from the document by clicking on the Style manager, finding the **Example Content** style and press **Remove All**.

Table of Contents

[1 Document Information 6](#_Toc98254177)

[1.1 Revision History 6](#_Toc98254178)

[1.2 Related Documents 6](#_Toc98254179)

[1.3 Document Signoffs 6](#_Toc98254180)

[1.4 Glossary of Terms 6](#_Toc98254181)

[1.5 Document License 7](#_Toc98254182)

[1.6 Outstanding Issues / Comments 7](#_Toc98254183)

[2 Introduction 8](#_Toc98254184)

[2.1 Executive Summary 8](#_Toc98254185)

[2.2 Document Scope 8](#_Toc98254186)

[2.2.1 In Scope 9](#_Toc98254187)

[2.2.2 Out of Scope 9](#_Toc98254188)

[3 Operational Environment Specification 10](#_Toc98254189)

[3.1 General Design 10](#_Toc98254190)

[3.1.1 Software Architecture Brief 10](#_Toc98254191)

[3.1.2 Workflows & User Journeys 12](#_Toc98254192)

[3.1.3 Physical Architecture 13](#_Toc98254193)

[3.2 Network Connectivity 18](#_Toc98254194)

[3.2.1 Network Addresses 18](#_Toc98254195)

[3.2.2 Network Communication Ports 18](#_Toc98254196)

[3.2.3 Remote Access Requirements 18](#_Toc98254197)

[3.2.4 Application Firewall Rules 18](#_Toc98254198)

[3.3 Integration 19](#_Toc98254199)

[3.3.1 Hospital Systems Inc. HISPlus™ 19](#_Toc98254200)

[3.3.2 National Health Facility Registry 19](#_Toc98254201)

[3.3.3 ImmunizeYou™ IMS 19](#_Toc98254202)

[3.4 Availability 19](#_Toc98254203)

[3.4.1 Service Downtime Mitigations 19](#_Toc98254204)

[3.4.2 Component Availability Requirements 21](#_Toc98254205)

[3.4.3 Support and Service Availability 22](#_Toc98254206)

[3.4.4 Support Responsibilities 23](#_Toc98254207)

[3.5 Service Continuity 23](#_Toc98254208)

[3.5.1 Escalation & Reporting Procedure 23](#_Toc98254209)

[3.5.2 Recovery and Downtime 25](#_Toc98254210)

[3.5.3 Business Continuity Plan 26](#_Toc98254211)

[3.5.4 Backup & Data Retention 29](#_Toc98254212)

[3.6 Software and Network Updates 30](#_Toc98254213)

[3.7 Environment Capacity and Scalability 30](#_Toc98254214)

[3.8 Security Considerations 31](#_Toc98254215)

[3.8.1 User Security 31](#_Toc98254216)

[3.8.2 Device Security 32](#_Toc98254217)

[3.8.3 Authentication 32](#_Toc98254218)

[3.8.4 Data Security 33](#_Toc98254219)

[4 Data Configuration Specification 35](#_Toc98254220)

[4.1 Concept & Vocabulary Data 35](#_Toc98254221)

[4.2 Business Rules & Triggers 35](#_Toc98254222)

[4.3 Custom Extension Types 36](#_Toc98254223)

[5 Citations & References 37](#_Toc98254224)

# Document Information

## Revision History

Use the table below to capture the changes to this document over time. The revision history is useful for readers as it provides a list within the document of its lineage.

|  |  |  |  |
| --- | --- | --- | --- |
| **Authors** | **Date** | **Changes** | **Version** |
| SanteSuite Team ([info@santesuite.com](mailto:info@santesuite.com)) | 2022-01-27 | * Initial Version | 0.0 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Related Documents

This section is used to indicate other documents such as e-Health Blueprints, enterprise architecture, software architecture, licenses, policy documents, assessments, etc. which may be referenced or may provide the reader with additional context for this document.

|  |  |
| --- | --- |
| **Document Title & Link** | **Relevance** |
| SanteSuite Help Portal (<https://help.santesuite.org>) | Provides supporting information for the SanteMPI and SanteDB platform. |
| Demoland Minimum Dataset XLSX | Provides context on the restrictions of fields and data-types in the Demoland MPI. |
| Demoland Identifier Domain Worksheet | Provides a list of initial identity domains for the Demoland National MPI. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Document Signoffs

If your organization requires architecture documents to be approved, or reviewed, you can use or adapt this section of the document to indicate the representatives have seen and reviewed the document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Review Date** | **Reviewed/Approved By** | **Notes** |
| 0.0 | 2022-01-27 | Wally | Chief Engineer Review Complete |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Glossary of Terms

If your implementation uses country or context specific terms then they should be enumerated here. For example, if your document refers to a national health facility registry (NHFR) it should include this definition in the table.

This provides readers a place to “look-up” what specific terms found in the document mean.

|  |  |
| --- | --- |
| **Term** | **Definition** |
| MPI | Master Patient Index – A solution which is responsible for maintaining and cross referencing the identity of persons/patients within the authority. |
| dCDR | Disconnected Clinical Data Repository – The terms used by SanteDB to describe the offline portion (or client portion) of the clinical data repository (see: [SanteDB Architecture - SanteSuite Help Portal](https://help.santesuite.org/santedb/architecture#dcdr-clients)) |
| iCDR | Integrated Clinical Data Repository – The term used by SanteDB to describe the central, jurisdictional clinical data repository ([SanteDB Architecture - SanteSuite Help Portal](https://help.santesuite.org/santedb/architecture" \l "icdr-server)) |
| MDM (Master Data Management) | Master Data Management – A data storage pattern whereby a single golden or master record is linked and maintained from various source records. |
| EPI | Expanded Programme on Immunization |
|  |  |

## Document License

This document is based on the SanteMPI/SanteDB operational architecture documentation template originally authored and shared by SanteSuite Inc. ([www.santesuite.com](http://www.santesuite.com)). The document is licensed under the terms of the Creative Commons Attribution + Share-Alike 4.0 License ([Creative Commons — Attribution-ShareAlike 4.0 International — CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)).  
  
A picture containing text, clipart

Description automatically generated

Original Copyright © 2022, SanteSuite Inc.

## Outstanding Issues / Comments

Use this section to collect or enumerate any feedback on the document which has yet to be resolved. The outstanding issues and comments section should be used while the document is being authored, and can be removed prior to publication.

Note: This section is included in the document to provide readers with a reference point within the document (for a specific version of the document they are reading) the issues and active/outstanding issues with the content of this version of the document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Discussion / Issues** | **Resolved** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

The introduction section allows you to describe your implementation of SanteMPI or SanteDB. It helps the reader understand the overall project (reason for the document), its scope, the purpose of the project, etc.

This document seeks to describe the overall deployment, security settings, configuration, and operational environment of the SanteMPI product suite within the context of the Demoland Master Patient Index (MPI) project.

## Executive Summary

Provide a summary of the project, program, or initiative in which this operational deployment fits. The executive summary should be the “elevator pitch” of the project where the SanteMPI project is being leveraged. It may provide details such as a history of the initiative, the ministries involved, etc.

Demoland is a nation of approximately 22 million citizens (about the population of New York) living in 4 territories. In 2020, a polio outbreak in the northern region necessitated an investigation by the Ministry of Health, Equity and Social Benefits (MOHESB) to determine the root cause of this outbreak.

The MOHESB initiated an analysis of the digital health systems leveraged within the territories related to immunization services. It found that the four (4) territorial health authorities leveraged a variety of solutions for labor and delivery records and immunization – however these systems were not interoperable. This introduced a problem where health care workers in the extended programme of immunization (EPI) were not aware that children were missing from their coverage reports (as they were not in the immunization management platform used).

In 2021 the MOHESB started the Demoland Enterprise e-Health Architecture initiative to design an integration of birth and labor software solutions and the EPI software solutions. It was determined that a national scale, interoperable patient registration solution was required to necessitate the integration of these two program areas.

In 2022, MOHESB conducted a survey of available master patient index and client registry software. The requirements for this survey included standards support. Demoland General Hospital uses a proprietary hospital information system (HIS) with limited integration to those solutions via an HL7 Admission, Discharge and Transfer (ADT) interface.

MOHESB determined that SanteMPI provided the correct feature set required for the Demoland context. This solution was chosen because of its disconnected support, documentation, and standards support.

This document describes the deployment of the SanteMPI software as the basis for linking the birth and labor systems with EPI in the Demoland context. Future expansions of this technology are described in the Demoland Enterprise e-Health Architecture document.

## Document Scope

The document that you are writing cannot cover all use cases, all data points, or all information necessary for a reader to get the entire picture of the broader e-health context in which SanteMPI is being deployed. Use this section to enumerate the boundaries of this document.

### In Scope

* Physical and virtual network design of the Demoland SanteMPI deployment
* Design of the security environment, controls, and auditing/accountability
* Reference data configuration including identity domains, authority to assign
* Integration and interoperability with existing systems

### Out of Scope

* National e-Health Blueprint Architecture and Enterprise Architecture artifacts
* Business processes, software design, and information design (beyond configured restrictions)
* National Interoperability Standards Profiles

# Operational Environment Specification

## General Design

### Software Architecture Brief

The software architecture brief section should explain the overall logical blocks of functionality which are being deployed, how they relate to one another, what interfaces are used and the type of transport. Try to refrain from getting too detailed on the deployment itself (servers, clusters, failover, etc.).

For now, try to give readers an idea of how the overall SanteMPI deployment will operate and fit together with local systems in scope of the project.

The overall operational architecture of the national MPI project is illustrated in Figure 1. Because of the lack of reliable connectivity to remote hospitals and clinics, the disconnected gateway software will be configured and leveraged.

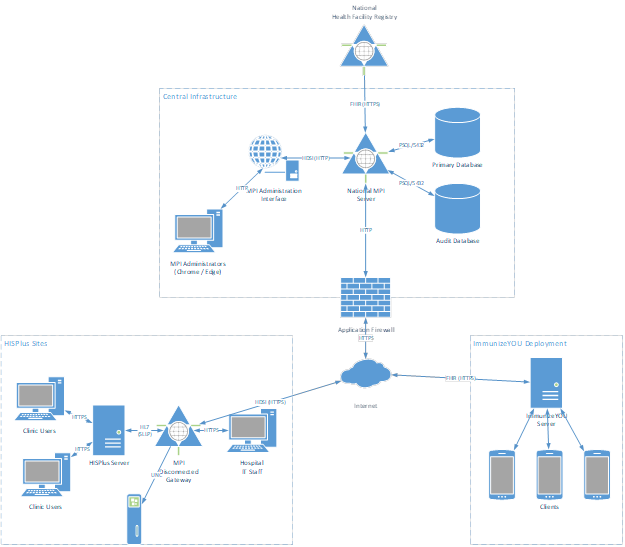


Figure 1 - Overall Software Architecture

The software solution components are enumerated in the following table:

|  |  |
| --- | --- |
| **Component** | **Description** |
| National Health Facility Registry | The Demoland national health facility registry contains a centralized list/registration of facility information for all sites (hospitals, clinics, etc.) for the entirety of Demoland. This information will be used to populate the SanteDB facility list using a periodic refresh of data.  The use of facility registration is important for the synchronization, as the offline access will rely on catchment areas established in the HFR. |
| MPI Administrative Interface | A web management platform which allows for the creation of users, roles, security users, and monitoring and correction of MPI data. |
| National MPI Server | The iCDR server configured with Master Patient Index (MPI) plugins. Responsible for management of synchronization data, and matching/merging rules as well as authentication. |
| Primary Database | The Master Patient Index primary database – where primary data is stored. |
| Audit Database | The Master Patient Index audit database – where audit trail information is kept. |
| MPI Disconnected Gateway | The dCDR server (the gateway) which is responsible for queueing messages destined for the central server while the local systems are offline.  This deployment was chosen since remote hospitals in Demoland lack reliable (and fast) internet connections. Additionally network QoS rules prefer the transfer of images over administrative traffic (like the MPI) so the use of a disconnected solution should isolate in-clinic performance issues. |
| ImmunizeYOU Server | The EPI department of the MOHESB operates a nationally scaled, in-house immunization management system (IMS). This IMS operates in a separate datacenter, and will communicate with the National MPI via HL7 FHIR over HTTPS over broadband internet. |
| HISPlus Server | HISPlus is a nationally licensed, proprietary hospital information system. HISPlus integrates with master patient index software using HL7v2 (primarily ADT^A01 and ADT^A08 messages). |
| Hospital IT Staff | Each disconnected gateway deployment at hospitals using HISPlus will have local administrative accounts created. The hospital IT staff (those in charge of HISPlus) will be given administrative access to their MPI local gateway to resolve synchronization issues, etc. |
| MPI Administrators | Central server portal clients which access the MPI for configuration purposes. |

### Workflows & User Journeys

Use this section to give readers a brief overview of how users will use this system. Do not copy/paste the entirety of the software design documents here, rather provide a brief overview of the use of the system. This is useful to establish context for readers and network operations staff to assess the potential security and privacy issues which may arise from the operation of the SanteDB software solution.

#### New Patient Registration

The new patient registration workflow can be described as:

1. The clinic user will establish the patient’s identity by asking them for their name, identifying information, etc. (see minimum data set section).
2. The clinic user will use their local system (HISPlus) to search for any existing patient records which might have already been registered within the MPI.
3. If the user does not find a candidate record, the user will create a new demographic record within the HISPlus software.
4. The HISPlus software will publish this information to the MPI software to which it is connected.
5. The clinic user will continue care as normal.

Diagram

Description automatically generated with medium confidence

#### User Journey 2

#### User Journey 3

### Physical Architecture

Use this section to describe the physical architecture of the SanteDB deployment. The physical architecture differs from the software architecture in that it is primarily concerned with the operating environment. Include in this section:

* Physical Servers which are being used
* Virtual Servers or Docker containers being used
* Network infrastructure (virtual networks, firewalls, routers, switches, etc.)
* Storage Infrastructure (SANs, NAS, etc.)
* Backup infrastructure (failover environments, backup locations, etc.)

In the example, Demoland is specifying an architecture where the SanteMPI components need to be deployed in a national system and in a clinic.

#### National Datacenter

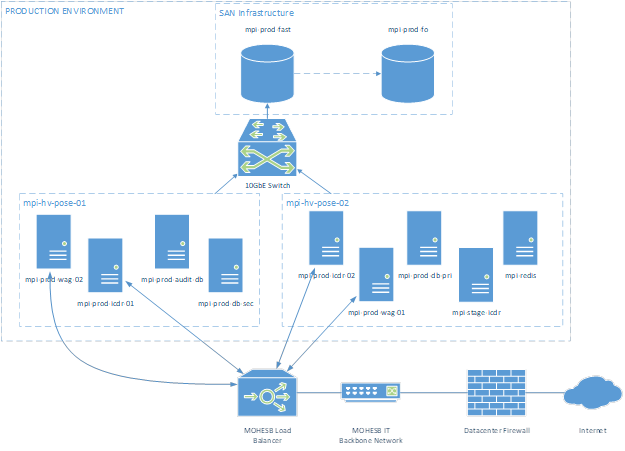
The central server in Demoland is being installed in the central datacenter in Demoland’s capital city. Here the MOHESB runs a network operations center (NOC) which has secured physical access by MOHESB IT staff.

The NOC is primarily concerned with the operation and maintenance of hardware and network infrastructure, and already has key infrastructure in place which will be used by the MPI project. Key details about the NOC are:

* A 10GbE uplink to the internet will be provided by NOC staff
* A single, publicly accessible IP address will be assigned to the entire MPI project.
* Application firewall and access rules are controlled by the NOC
* SIEM and APM monitoring software are mandatory and will be installed on the virtual machine and physical hardware provided.
* The NOC is responsible for standard equipment, the NOC will provide quotations for this spin up and hosting cost using a standard model.
* The NOC mandates that Symantec Corporate Antivirus software be installed by all virtual machine software in use in the NOC, licenses for this are procured as part of the NOC operations.
* The NOC mandates that Microsoft Windows Server 2016 Datacenter be procured for all physical hosts.

The MPI project will use a relatively simple deployment with the following characteristics:

* Two physical operating system environments (POSE) will be procured. The POSE will be procured from the preferred vendor of the NOC (Lenovo) and will be identical.
* Virtual environments will be stored on a shared storage area network array (SAN) which has a secondary replicated node for failover and recovery. The storage of the virtual disk infrastructure on the SAN permits the rapid failover between POSE executing the VMs.
* An HTTP load balancer and application firewall solution has already been installed and maintained by the MOHESB NOC. The solution requires setup and management by the NOC staff.

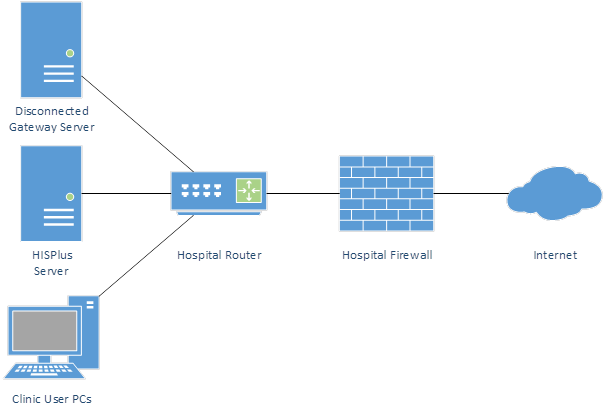


|  |  |  |  |
| --- | --- | --- | --- |
| **Server** | **Hardware** | **Software** | **Notes** |
| MPI HyperV (mpi-hv-pose-01 , mpi-hv-pose-02) POSE | 2x XEON Silver 4220  128 GB RAM  1xNVMe SSD (Operating System)  2x 10GbE NIC (1 dedicated to SAN and 1 dedicated to Network) | Microsoft Windows Server 2016 Datacenter  Symantec Corporate Antivirus  Microsoft Hyper-V Manager  Splunk APM | The physical operating system environment for the production and staging environments will be installed as 2U rack-mounted servers within the NOC rack procured for this project. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### HISPlus Sites

Hospitals in Demoland have intermittent internet connectivity to the central NOC, especially in the southern region. Hospital patient populations in Demoland rarely exceed 10,000 patient registrations per year, and there is no need of robust client side matching or merging (i.e. HISPlus already provides these types of functions).

Because of this, the Demoland MPI requires only basic store/forward/subscribe functions when interacting with the central MPI infrastructure. The SanteDB dCDR will be leveraged for this purpose.



|  |  |  |
| --- | --- | --- |
| **Server** | **Software** | **Notes** |
| dCG Laptop | * Microsoft Windows 10 * SanteDB dCDR Gateway | The dCG laptop is responsible for queueing messages meant for the central MPI and providing basic security controls within the clinic. |
|  |  |  |

## Network Connectivity

### Network Addresses

Use this section to describe the IP addresses and logical host names (maintained in either a DNS server or via host files). This is useful for other administrators to understand the network layout of the deployment. It also helps software maintainers configure and setup the services.

The network address list for the national datacenter deployment is enumerated in the table below:

|  |  |  |
| --- | --- | --- |
| **Component** | **Hostname** | **IP Address (VNET)** |
| MPI Host Server |  | 192.168.0.1 |

### Network Communication Ports

Use this section to describe how information flows between virtual or physical servers within the SanteDB deployment. This is useful for “the next guy” who will be maintaining your deployment and should provide a clear picture of which services use which ports and on which internal node.

#### National Datacenter

|  |  |  |  |
| --- | --- | --- | --- |
| **Server** | **Application** | **Service** | **Port(s)** |
| mpi-host | RDP | RDP | TCP/3389 |
| mpi-prod | SanteDB iCDR | HL7 SLLP | TCP/2100 |
|  |  |  |  |
|  |  |  |  |

#### HISPlus Sites

|  |  |  |  |
| --- | --- | --- | --- |
| **Server** | **Application** | **Service** | **Port(s)** |
| mpi-host | RDP | RDP | TCP/3389 |
| mpi-prod | SanteDB iCDR | HL7 SLLP | TCP/2100 |
|  |  |  |  |
|  |  |  |  |

### Remote Access Requirements

Use this section to describe what the requirements are for remote access to the SanteDB server infrastructure. Anytime an external service needs to be opened to the world (via the internet) where physical or software protection (like a firewall, SSH tunnel, VPN and/or multi-factor authentication mechanisms) is not used or where downstream systems may have issues with connectivity should be documented.

Be sure to be specific, use the actual host names for your deployment, the actual transports or protocols used and their ports. This is useful for network operators security and privacy reviewers to get a clear picture of the surface area for attacks.

#### National Datacenter

The national datacenter will need to be accessed externally on the following ports.

|  |  |  |  |
| --- | --- | --- | --- |
| **External Host Name** | **Internal Host** | **Transport** | **Port(s)** |
| mpi-host | RDP | RDP | TCP/3389 |
|  |  |  |  |
|  |  |  |  |

### Application Firewall Rules

Since the national datacenter is accessed using a single host name (mpi.gov.demoland.com), and because the internal infrastructure is physically secured using network firewalls, SSL termination has been configured on the load balancer. The rules for these hosts can be changed upon request, however the current configured routes.

|  |  |  |
| --- | --- | --- |
| **Source** | **Service** | **Target** |
| mm.santesuite.net:443 | MPI Portal | <http://mpi-prod:>80 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Integration

This section should be used to describe how data flows between the SanteDB system (which has a known security and privacy environment) and other systems which are connected to SanteDB. This will assist in a Privacy Impact Assessment since, anytime personal health information is disclosed between system boundaries, there is a risk to breaches in security and privacy.

## Availability

### Service Downtime Mitigations

This section is used to describe the impact of downtime of the software services and components in the deployment. Here, the writer should indicate what the impacts of a downtime would be (how they would manifest) and how the downtime can be mitigated so that business operations can continue while the server component is unavailable.

#### National Datacenter

The iCDR / central MPI server may encounter downtimes and/or data quality issues due to software defects, and/or network availability. This is not necessarily critical to the operation of the dCDR infrastructure, however may impact the onboarding of new clinics, password resets, etc.

|  |  |  |
| --- | --- | --- |
| **Component** | **Observed Impact** | **Mitigation** |
| National MPI (SanteMPI iCDR) | * Clients using HISPlus and the dCDR will observe synchronization conflicts with the error message “Remote Server Returned 503” or “Remote Server Returned 500”. * Services directly integrated with the SanteMPI service will receive 503 or 500 errors directly on their HTTP access request. * Services directly integrated with the SanteMPI server via HL7v2 will receive negative ACK responses with an ERR segment indicating unavailable host. * Timeouts may also occur if the host service or operating system is not running. | Users should report the error to the in-country partner and continue to use their instance of the dCG in offline mode. |
|  |  |  |
|  |  |  |
|  |  |  |

#### HISPlus Clinics / Disconnected Access

The following mitigations are proposed for in-clinic dCDR/dCG downtimes.

|  |  |  |
| --- | --- | --- |
| **Component** | **Observed Impact** | **Mitigation** |
| dCDR MPI Gateway | * Searches from HISPlus to the MPI will cease to function, meaning users cannot locate patients in the MPI. | Users should register the patient locally if they are not present in the local HISPlus instance. At a subsequent visit, HISPlus will resubmit the patient data during the registration/admission process. |
|  |  |  |

### Component Availability Requirements

Unfortunately computers aren’t perfect. Sometimes disks fail, networks fail, virtual machines fail, and even the software fails. This section is used to describe any foreseen issues which might arise during the operation of SanteDB operations. The table in the section should indicate a brief description of what issues might arise if certain components of the software or hardware fail.

The Demoland MPI server infrastructure runs on two physical hosts connected via SAN. This means that a catastrophic hardware failure should result in minor disruptions to the operational environment of the MPI (however service degradation may be experienced during state spin-up).

|  |  |
| --- | --- |
| **Component** | **Availability Notes** |
| MPI Application Servers (mpi-prod-icdr-01 and mpi-prod-icdr-02) | The two MPI application servers operate on one of two physical operating system environments. If one of these POSE experiences a catastrophic failure, the load-balancer should detect the condition of lost heartbeat and prevent routing of messages to the inoperable application server.  This would result in a degradation of service throughput, however would not render the MPI inoperable.  In the event of a catastrophic failure of the data-center, the application servers can be setup on a new copy of Microsoft Windows Server 2016 within 24 hrs. During this time the MPI service will be inoperable. |
| MPI Staging Application Service | The staging server is only used for training, testing and developing of new components. This means that downtimes of the application server of up to 48 hours is acceptable. |
|  |  |
|  |  |
|  |  |
|  |  |

### Support and Service Availability

Use this section to describe the support services and their availability. This section is used to clearly articulate the service level agreements in place between parties responsible for the operation of your SanteDB instance. It should include the contact name, contact information, and the hours of operation of those support contacts.

The following support services are available for the MPI Operation.

* Network support and operations support for the central infrastructure is provided by MOHESB Network Operation Center (NOC) Associates in Capital City and is available 24x7 via [noc@mohesb.gov.demoland.com](mailto:noc@mohesb.gov.demoland.com)
* End-user support for repair of equipment, password resets, provisioning, etc. is being provided by YouComp during normal business hours (Mon – Fri , 9:00 AM – 5:00 PM UTC+6:00) via [support-mpi@youcomp.com](mailto:support-mpi@youcomp.com)
* Software defect correction and end-user software issues are handled by LocalDev Inc. during normal business hours (Mon – Fri, 9:00 AM – 5:00 PM UTC+6:00) via [heldesk@localdevs.com](mailto:heldesk@localdevs.com)
* Escalated software defect issues will be provided by SanteSuite during normal business (9:00 AM – 5:00 PM UTC-5:00) via [support@santesuite.com](mailto:support@santesuite.com)
* In-Clinic network and infrastructure support is being provided by YouComp during normal business hours (Mon – Fri , 9:00 AM – 5:00 PM UTC+6:00) via [support-mpi@youcomp.com](mailto:support-mpi@youcomp.com)

### Support Responsibilities

Use this section to clearly articulate each party’s responsibility for the operation of the SanteDB software. The support responsibilities located in the table are defined as:

* **Primary Support**: Direct support to the end-user which is encountering the issue including diagnosis, log collection, and analysis to identify as best possible the cause of the issue.
* **Escalation**: Involves re-configuration, software defect correction, or enhancement by the primary support organization.

|  |  |  |
| --- | --- | --- |
| **Component** | **Primary Support** | **Escalation** |
| Central Network Infrastructure | YouComp | MOHESB NOC Associates |
| Central MPI Software UI Issues | LocalDev Inc. | SanteSuite Inc. |
| Central MPI Synchronization Issues | LocalDev Inc. | SanteSuite Inc. |
| Hospital/Clinic Network Infrastructure | Local IT Support Staff | YouComp |
| Clinic MPI Software (Gateway) | LocalDev Inc. | SanteSuite Inc. |
| HISPlus MPI Integration | Local IT Support Staff | LocalDev Inc. |

## Service Continuity

The Service Continuity section should be used to describe the procedures which are in place to ensure that, when the service is not available, that business can continue as normal.

### Escalation & Reporting Procedure

When business operations are halted due to an issue with the operational environment, it is important that the correct people be notified of the incident. Use this section to describe the procedure that users and operators should use to report an operational interruption. Include any special instructions for your environment including:

* What type of issues may occur and what the scope of those issues may be
* Which software solutions should be used to raise an issue (bug tracker, helpdesk ticketing system, etc.)
* What data should be gathered and included in the report.

Where possible, the primary support contact should attempt to diagnose and correct the issue to the best of their ability. Examples of issues where the primary support contact is best suited to correct issues:

* Network Issues – Connectivity between laptops, VMS, and clinics and the central server.
* User Interface Questions – Questions related to the user interface and its use.
* Common Synchronization Errors – Common errors will appear during the course of the MPI operation. These synchronization errors, over time, will become familiar and resolutions can be performed directly by the primary support person.

When an issue cannot be solved by the primary support contact, they should escalate it to the noted escalation point.

#### Software Defect Escalation

For software issues or low priority operations issues, a bug should be filed on MOHESB BugZilla system (<https://bugzilla.gov.demoland.com>). Bugs should:

1. Be filed under the MPI project
2. Have an appropriate component, classification, operation environment (online/offline via HISPlus or ImmunizeYOU), facility name and end user browser selected.
3. Have a descriptive summary which clearly identifies the issue
4. Include a description which identifies:
5. The steps taken prior to the issue presenting (steps to reproduce)
6. Any environmental observations (offline, slow internet, high RAM usage, etc.)
7. Whether the issue is present in more than one clinic or only in one clinic.
8. The UUID of any relevant record (Note: Do not include patient identifying details or screenshots showing patient name. Only include the UUID of the patient)
9. Include relevant log files
10. A screen capture of the System > Server Status page.

Graphical user interface, text, application, email

Description automatically generated

### Recovery and Downtime

In this section, you should describe the impact of a downtime of a component in your deployment. Additionally, you should include any relevant recovery options which could be used to restore service. The purpose of this section is to give the reader (or operator of the infrastructure) hints to possible paths of recovery.

|  |  |  |
| --- | --- | --- |
| **Component** | **Downtime Impact** | **Recovery Options** |
| Production MPI Servers | Primary MPI application server downtime will result in the central administration user interface not operating or displaying errors.  Additionally, clinics will not be able to synchronize their data. | In case of hardware failure, recovery from backup should be attempted.  If backup restoration is not possible, a fresh VM should be created and the software / configuration files re-deployed. |
|  |  |  |
|  |  |  |

### Business Continuity Plan

When the system is not available, it is important that operators understand the impact and procedures which can be used to attempt a service restoration. The table in this section is intended to express the:

* Recovery Time Objective (RTO) – The maximum amount of time that could be tolerated between unexpected failure and the resumption of normal service. (i.e. How long can clinics operate without the system?). RTO dictates the goal for recovering the service.
* Recovery Point Objective (RPO) – The maximum period of time which data might be lost if service unexpectedly fails. (i.e. How far back can you fail without disrupting business?). RPO usually dictates the frequency of backup.
* Maximum Tolerable Outage (MTO) – The maximum amount of time that the business function can tolerate complete cessation of MPI project during normal business days.

The continuity procedures column should be used to instruct administrators or users how to restore the system to an operational state and, if possible, how to continue operation of their own work during the outage.

There are various potential issues which should be covered in your procedures, and these will depend on how you are operationalizing SanteDB, however it is useful to consider the following types of failures:

* Physical / Hardware Failures – What should be done in the case of a physical failure of the infrastructure?
* Data Corruption – What should be done to recover when data is corrupted?
* Software Defects – What should be done to recover from a software defect or bug?
* Network Issues – What should be done to recover/fix a networking issue?

The table below identifies the maximum tolerable outages and defect correction times for the MOHESB Demoland MPI Pilot.

There is currently no Service Level Agreement (SLA) in place between the support organizations. The information in the table below provides a guideline to illustrate the criticality of a component within the MPI.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Component** | **RTO** | **RPO** | **MTO** | **Procedures** |
| Production MPI Servers | 24 H | 1 H | 48 H | During downtime of the primary MPI server client software should queue create/update requests for re-send when the service is available.  Catastrophic Hardware Failure of one POSE:   1. Notify users of service degradation – 1h 2. Create new VM on the remaining POSE node – 1h 3. Attach the virtual hard disk from the SAN to the new VM and start – 1h 4. Perform connection validation to the environment – 1h 5. Notify users of service restoration – 1h   Catastrophic Hardware Failure entire environment:   1. Notify users of cessation of MPI operation until replacement hardware can be ordered – 1h 2. Setup Hyper-V on the new hardware host – 8h 3. Redeploy the backups from backup storage to the new SAN – 8h 4. Re-configure the virtual networking switch – 1h 5. Re-Configure Virtual Machines – 2h 6. Notify users of service restoration – 1h   Virtual Machine Corruption / OS Issue:   1. Contact the primary support person – 4h 2. Primary support contact login to the virtual machine infrastructure and attempt to resolve the issue – 4h 3. Contact escalation point, provide analysis / relevant information – 4h 4. Escalation point resolves the issue – 4h   Application Defect / Bug:   1. Contact the in-country support (primary support) contact within – 4h 2. Primary support contact attempts to resolve the issue by analyzing logs and current state of network – 4h 3. Escalate the defect using the BugZilla portal. -1h 4. Escalation contact will attempt to resolve the issue – varies |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Backup & Data Retention

Use this section to describe the backup procedure and the retention policies for data in the operational infrastructure. These are important to understand the frequency and location of backups as well as the maximum age of data permitted.

Standard MOHSEB backup infrastructure is being used on \\moh-nas-bk01\backup\mpi . The backup strategy is using Microsoft Server Backup and Volume Shadow Copy on the schedule illustrated below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Component** | **Data Stored & Retention** | **Backup** | |
| **Schedule** | **Retention** |
| Production MPI Servers | * Log Files (30 days) * Dispatcher Queue (MSMQ) – N/A | Nightly | 1 week (hot restore on NAS)  30 days cold storage of daily backup. |
| Production Database Servers | Clinical Data is stored for 7 years after death of patient. | Nightly | 1 week (hot restore on NAS) and 10 years cold storage of first day of month backups. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Software and Network Updates

Use this section to describe any special procedures which are related to the application or impacts of Software and Network updates. This section should alert the reader of:

* What special procedures are required to update software, hardware, or operating system components?
* What are the impacts of updating software to the operation of the business?
* What are the currently configured automatic backup and maintenance windows? (i.e. have automatic updates been configured or are they scheduled? Etc.)

## Environment Capacity and Scalability

Your operational environment will grow over time. It is a prudent exercise to describe and plan for expansion of the environment as more clients, patients, and data domains come online. This section is used to enumerate the manner in which the current capacity of the operational environment can be expaneded.

|  |  |  |
| --- | --- | --- |
| **Component** | **Capacity** | **Expansion Options** |
| MPI HyperV (mpi-hv-pose-01 , mpi-hv-pose-02) POSE | * 2x XEON Silver 4220 * 128 GB RAM * 1xNVMe SSD (Operating System) * 2x 10GbE NIC (1 dedicated to SAN and 1 dedicated to Network) | RAM can be expanded up to 256 GB by procuring additional DDR4 ECC RAM.  Limited upgrade options for CPU. Storage is on SAN (upgrade separate)  Additional POSE can be procured to expand load balancing |
|  |  |  |

## Security Considerations

Use this section to describe the security environment for your operational deployment. This should include:

* What are the classes of users which use the system and what are their access levels?
* How are new users onboarded? When are they removed?
* What processes are in place to onboard new devices? How are they identified? When are they locked or removed?
* How is data encrypted? How are passwords hashed? Etc.

### User Security

Describe how new users are onboarded, how old users are removed, and which classes of users exist.

#### User Account & Session Policies

The following password policies have been set for the Demoland MPI.

* Passwords must be 8 characters in length
* Passwords must contain:
* A mix of upper- and lower-case letters
* A number
* A symbol (@, $, #, &,etc.)
* No password expiration policy has been set
* No password history policy has been set
* Session lengths have been configured to 30 minutes from time of authentication
* Sessions can be refreshed at expiry for a further 5 minutes (extend session option)
* Sliding account lockout has been set after 10 invalid login attempts.
* Session sharing between browser tabs has been disabled.

#### User Classes

Only MOHESB employees or employees of the connected clinics will be granted access to the Demoland MPI deployment.

|  |  |  |  |
| --- | --- | --- | --- |
| **User Class** | **Responsibilities** | **Onboarding Procedure** | **Retirement Procedure** |
| Administrators | Administrators are granted unrestricted administrative access and are charged with the maintenance and operation of the SanteMPI server. Administrators may create new users, groups, etc. | Administrators are added after an MOHESB IT hiring process is completed by the new user. At this time, the MOHESB supervisor will notify an administrator via Bugzilla of the creation of a new user account. The new user account is created and assigned to ADMINISRATORS group.  Administrator accounts are in the form: **xad**lastnamefirstinitial | MOHESB human resources will notify administrators via the Bugzilla portal of the request to remove the user account. |
| MDM Administrators | MDM administrators are granted permission to access clinical data, and are also granted permission to merge records, correct data, establish records of truth, etc. | MDM administrators are hired or contracted directly by the MOHESB. After completing MPI training the request to create a new user account via the Bugzilla system. | MOHESB human resources will notify administrators via the Bugzilla portal of the request to remove the user account. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Device Security

Use this section to describe how devices are authenticated, onboarded, retired and how validation of the software is performed. Typically this section will detail:

* The certification or validation process required to create a new device account (or to enable self-service creation)
* The method of authenticating the node (such as using client certificates, device secrets, etc.) and the mechanism (using MSH-8, headers, etc.)
* The process and procedures followed for de-activating the device account.
* How are devices physically secured (using access cards? Kingston locks? In cabinets? Etc.)

### Authentication

Describe the authentication policies and mechanisms that are used to validate devices, applications and users.

The following authentication mechanisms are provided in the central MPI server:

* Authentication of a dCG instance within a particular clinic is performed using OAUTH client\_credentials grant with an additional device secret passed to the server.
* Authentication of users in the administrative portal is performed using OAUTH password grants.

The authentication infrastructure generates three tokens for each session which are shared to the client once when the session is established (loss of these tokens requires re-authentication):

* A JWT identity token containing claims about the user including scope of grant (permissions), roles the user is allowed access for the current session, etc.
* A meaningless 256-bit access token whereby 128-bits are randomly generated and 128-bits are a padded HMAC256 signature of the session token.
* A meaningless 256-bit refresh token (same as the access token).

The following authentication mechanisms are provided in the dCDR:

* Authentication of OpenMRS server as a DEVICE performed using the HL7 MSH-8 security key generated by the dCG.
* This key is re-created whenever the user resets the OpenMRS configuration.
* Authentication of users using the dCG administrative user interface using a restricted OAUTH interface using password grants.
* Meaningless bearer tokens are granted for each session.
* Bearer tokens are signed using HMAC256.

### Data Security

Use this section to describe how your operational deployment handles the securing of data. Your description should include:

* How is data encrypted in transit at each contact point? (or, is the data on a physically secured network, etc.)
* How is data encrypted at rest? (i.e. is SQLCipher enabled on the dCDR, or is LUKS or BitLocker enabled on the database servers?)

#### Encryption In-Transit

The Demoland MPI is operated at the hostname mpi.gov.demoland.com and the \*.gov.demoland.com wildcard certificate is being used for this purpose. Since the internal services reside behind the MOHESB NOC firewall, and the datacenter is physically secured, SSL termination is performed at the load balancer.

#### Encryption At-Rest

The Demoland MPI primary database server, and the secondary database servers are encrypted at the file-system level using LUKS full disk encryption. Furthermore, the drives installed on the SAN infrastructure are encrypted using the provided Lenovo firmware on the SAN hardware.

#### Encryption of Backups

Backups to the MOHESB NOC NAS are encrypted using the FreeNAS option to encrypt the drives (this, in turn is tied to the TPM module on the NAS hardware). Furthermore, backups which are stored on physical media are encrypted using AES256 encryption with a passphrase configured by MOHESB NOC team.

# Data Configuration Specification

This section is used by implementers to describe the data configuration of their SanteDB product in use. This section is free-form, and will change based on your deployment. In general, useful information to include here are:

* Special restrictions of vocabulary or concepts in use in the operational context
* Custom business rules which impact the use and/or privacy/security of the solution
* Custom extensions which may be used to enforce custom business rules or behaviors in the context of the deployment
* Any special geographic or facility information which is pulled from other registry systems
* Any special data quality configuration or settings which have been implemented in the operational environment
* Special instructions or patterns used for identity domain onboarding, etc.

## Concept & Vocabulary Data

Demoland will customize the SanteMPI software solution to include our country specific concept sets and to modify the stock concept sets to remove inappropriate defaults from SanteDB.

|  |  |
| --- | --- |
| **Concept Set** | **Description** |
| OccupationType | Will be drawn from the official Demoland Ministry of Labor Statistics occupation list. |
| AdministrativeGender | Initially to be restricted to options Male and Female only, MOHESB is working on an official approved codification scheme for gender identities. |
|  |  |
|  |  |
|  |  |

## Business Rules & Triggers

MOHESB Demoland will implement custom business rules using C# for the faster performance during execution. The following table illustrates the business rules which are being implemented, their resource and the events for which the trigger event applies.

|  |  |  |
| --- | --- | --- |
| **Resource** | **Event** | **Description** |
| Patient | BeforeInsert | All patients with an occupation code of 40xxx or 50xxx (Government or Military occupations respectively) will automatically be assigned the policy **Access Sensitive Personnel Record (OID: 2.25.404039343)**. |
| Patient | BeforeInsert | All will be assigned a catchment area (primary facility) based on their official address at time of registration or update. |
| PatientMaster | BeforeInsert | All master records will have a unique, 12 digit numeric code generated automatically. This number is the national MPI temporary registration number. This number can be used to track the patient between visits until an official National Health Identifier card can be issued. |
|  |  |  |

## Custom Extension Types

Demoland national health directive requires that all patient’s carry extended information such as secrets for obtaining sensitive care (to authenticate the patient). These are to be stored in the extension registrations listed in the table below.

|  |  |  |
| --- | --- | --- |
| **Extension** | **Type** | **Use** |
| <http://demoland.com/mpi/safeword> | String | A hash of the security safety check word selected by the patient. This is the hash of the response which providers may use to authenticate the patient for care. |
|  |  |  |
|  |  |  |

# Citations & References

|  |  |
| --- | --- |
| [[1]](https://jfyfe.sharepoint.com/sites/SanteSuite/Shared Documents/1 Digital Square E1 CR RFP/0 Delivery/Documentation/Outputs/%0d%0d) | [SanteSuite Inc., "SanteSuite Software Architecture Documentation," [Online]. Available: https://help.santesuite.org/santedb/software-architecture.](https://jfyfe.sharepoint.com/sites/SanteSuite/Shared Documents/1 Digital Square E1 CR RFP/0 Delivery/Documentation/Outputs/%0d%0d) |
| [[2]](https://jfyfe.sharepoint.com/sites/SanteSuite/Shared Documents/1 Digital Square E1 CR RFP/0 Delivery/Documentation/Outputs/%0d%0d) | [SanteSuite Inc., "SanteSuite Data and Information Architecture," [Online]. Available: https://help.santesuite.org/santedb/data-and-information-architecture.](https://jfyfe.sharepoint.com/sites/SanteSuite/Shared Documents/1 Digital Square E1 CR RFP/0 Delivery/Documentation/Outputs/%0d%0d) |