National Utilization Management Integration (NUMI)

Systems Management Guide

Version 1.1.16.0

Department of Veterans Affairs

February 2024

Revision History

Date of Revision	Description of Change	Author Information
07/01/2013	Initial baseline – per project closeout	REDACTED
08/01/2013	NUMI version numbers and document dates updated. References to Fee Based items removed from sections 3.5 and 7.2.1. SSRS and replicated database servers added to section 3.1 and CPU and memory requirements added to all servers listed in section 3.1. Our interpretation of "security relevant events" added to section 8.3.2. Brief description of the InfoLog table added to section 11, Troubleshooting.	REDACTED
04/16/2015	Changed the version number from 1.1.14.1 to 1.1.14.2	REDACTED
07/14/2015	Changed the version number from 1.1.14.2 to 1.1.14.3	REDACTED
9/13/2016	Changed the version number from 1.1.14.3 to 1.1.14.4. Updated reporting link changes to Enhanced Reports in NUMI 14.4 release.	REDACTED
9/19/2016	Updated document with feedback received from HPS team review	REDACTED
9/30/2016	Changed Remedy to CA/SDM and updated other support groups to reflect current support system for NUMI application in CA/SDM.	REDACTED
10/01/2016	Updates for MDWS–VIA Migration (version 15.0)	REDACTED
03/01/2017	Updates for IAM SSO integration (version 15.2)	REDACTED
04/05/2017	Updates due to HPS review	REDACTED
04/12/2017	Added Hospitalization Admission review Type values	REDACTED
05/25/2017	Document updated and reviewed	REDACTED
11/14/2017	Updated version number and Contract information (version 15.4)	REDACTED
11/27/2017	Updated document as per HPS feedback.	REDACTED
01/10/2018	Updated document to include NUMI configuration change	REDACTED
04/24/2018	Update version number(15.5) and Login Information	REDACTED
9/17/2018	Updated version number (15.6)	REDACTED
3/15/019	Updated version number (15.7)	REDACTED
6/27/2019	Added 11.4.3: After Hours Management for SA audience	REDACTED
8/24/2019	Updated version number (15.8)	REDACTED
12/27/2019	Updated version to 15.9 and added system architect figure	REDACTED
12/3/2020	Updated version to 15.9.1 in title and footer. Footer month and year have been updated.	REDACTED
8/19/2021	Updated System Achitecture Overview diagram (Figure 1)	REDACTED
11/15/2021	Updated version to 15.10	REDACTED
1/9/2023	Updated version to 15.11	REDACTED
11/1/2023	Updated version to 15.13	REDACTED

Date of Revision	Description of Change	Author Information
01/24/2024	Updated version to 15.14	REDACTED
02/23/2024	Updated NUMI to use VDIF instead of VIA, version 16.0	REDACTED

Table of Contents

Table of Tables

Table of Figures

1 Orientation

Not applicable. There are no software or audience-specific notations or directions (e.g., symbols used to indicate terminal dialogues or user responses) for National Utilization Management Integration (NUMI).

2 Introduction

NUMI is a web-based application that supports field Utilization Management (UM) staff in performing reviews of clinical care activities. NUMI automates the documentation of clinical features relevant to each patient's condition and the associated clinical services provided as part of Veterans Health Administration's (VHA's) medical benefits package.

2.1 Purpose

The NUMI Systems Management Guide gives a technical description of NUMI for supporting and maintaining the application.

2.2 Scope

This guide provides technical personnel with information on the interactions between the components that are part of the NUMI architecture, to enable them to support and maintain the system.

2.3 Target Audience

The intended target audience of this guide includes Developers, Systems Administrators, Information Resource Management (IRM), and Product Support.

2.4 Document Overview

Table 1 lists the chapters in this guide.

Table 1: System Management Guide Document Sections

Chapter	Chapter Name	Chapter Includes
1	Orientation	Not Applicable
2	Introduction	Purpose, Scope, Target Audience, and Document Overview
3	System Requirements	Overview of the NUMI system
4	Parameters	Description of NUMI system parameters
5	Remote Procedure Calls (RPC)	RPCs being utilized for NUMI
6	Database Information	Database tables
7	Exported Groups and/or Options and Menus	NUMI menu descriptions;(Exported Groups and/or Options are Not Applicable)
8	Security Keys and/or Roles	Security keys, roles and other related information
9	Java Components	Not Applicable
10	Setup and Configuration	Setup and configuration information
11	Troubleshooting	Troubleshooting information for NUMI exceptions

Chapter	Chapter Name	Chapter Includes
Appendix A	Acronyms and Terms	A list of acronyms and terms used in this guide and their descriptors
Appendix B	Dependencies	Information about NUMI dependencies
Appendix C	Interfacing	Information about NUMI interfaces
Appendix D	References and Official Policies	References and policies relevant to the NUMI project
Appendix E	Section 508 Compliance	Information about Section 508 compliance guidelines
Appendix F	NUMI Development Tools	A description of the tools used to develop NUMI
Appendix G	NUMI Workflow Example	An example of the NUMI application workflow from a UM user's perspective
Appendix H	Free Text Search Criteria	A listing of tables/columns checked during Free Text searches from UM Review Listing and Search Patient pages
Appendix I	NUMI Database Servers	Database Server names

3 System Requirements

NUMI will be utilized at all Veterans Integrated Services Networks (VISNs), to provide a standard way of capturing and evaluating patient conditions at all the VA medical facilities. NUMI provides a centralized Web application and database for all VISNs and Veterans Administration Medical Centers. The NUMI application is dependent on the functional operation of the Veterans Data Integration and Federation (VDIF), Internet Information Server (IIS) application servers, Veterans Information Systems and Technology Architecture (VistA), and the Care Enhance Review Management Enterprise (CERMe) commercial off the shelf (COTS) product, the Stay Synchronizer and the Structured Query Language (SQL) Server Database.

3.1 Physical Architecture

In a traditional three-tiered approach to software development, the middle tier, or business object layer is the layer of architecture that models and enforces the business rules and/or data of an organization. NUMI interacts with VistA through the VDIF services (See Section 3.4.4). The interaction with the CERMe COTS product is through Extensible Markup Language (XML) and JavaScript.

The NUMI target configuration is a three machine cluster, consisting of the NUMI/CERMe Web Server, NUMI Exchange Web Server and NUMI Database Server. The NUMI/CERMe Web server runs the web applications for NUMI and CERMe, while the NUMI Exchange Web server runs the NUMI Exchange web service.

The NUMI and the CERMe databases reside on the NUMI Database server. The NUMI database stores information on patient movements. The CERMe database stores the Change Healthcare InterQual® criteria, which is used by the UM reviewers to determine patients' level of care and to manage Stay information. The minimum server and workstation software dependencies required to support the NUMI architecture are:

NUMI/CERMe Web Server (Application Server): 16GB RAM, 2.4GHz Xeon, Windows 2019 Server; Internet Information Services (IIS) v8.0; Microsoft (MS).NET 4.6.2 Framework; CERMe application; and NUMI Application.

NUMI Exchange Web Server: 4GB RAM, 2.4GHz Xeon, Windows 2019 Server; Internet Information Services (IIS) v8.0; MS.NET 4.6.2 Framework; and Web Services Enhancements 3.0.

NUMI Database Server: 64GB RAM, 2.8GHz Xeon, Windows 2019 Server; MS SQL Server 2019; Stay Synchronizer; NUMI Database; and CERMe Database.

NUMI SQL Server Reports Server (SSRS): 8GB RAM, 2.8GHz Xeon, Windows 2019 Server; MS SQL Server 2019; MS SQL Server Reporting Services 2019.NUMI Replicated Database Server: 16GB RAM, 2.8GHz Xeon, Windows 2008 Server; MS SQL Server 2019; NUMI Database.

NUMI Workstation: Minimum specifications: 2GB RAM, 2GHz Pentium 4; Operating System (O/S): Microsoft Windows 10 Enterprise (standard VA configuration for desktops); Microsoft Edge in IE Mode; JavaScript; and Adobe Acrobat Reader.

3.2 System Architecture

All servers have dual quad-core processors, large RAID arrays, and are running on a Windows 2019 server. The 64-bit servers are set up with a 146GB RAID -one array and a 410GB RAID - 5 (with one 'hot spare' in each server). The database servers additionally have dual Host Bus Adapter cards in them to make the required Storage Area Network (SAN) connections.

Primary Site: Two web servers, connected to a hardware load balancer; two web-services servers; and a database server connected to the SAN.

Below is an image that replicates the system architecture in the production environment.

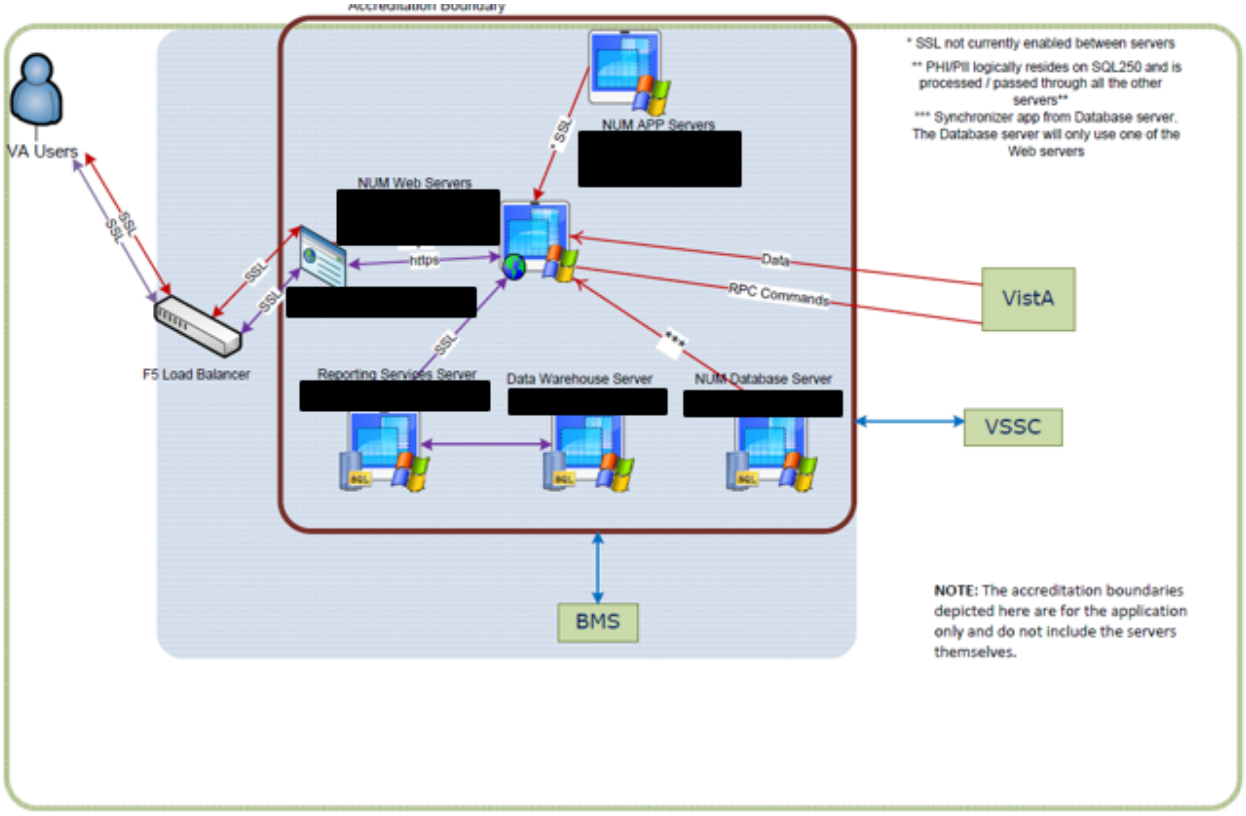

Figure 1: System Architecture Overview

3.2.1 Application Server Components

NUMI was built on the MS.NET 4.7.2 framework. The application server runs on an Internet Information Services (IIS) Application Server v8.0. The application requires MS ASP .NET 2.0 Ajax Extensions 1.0 and Web Services Enhancements 3.0 to enable the interactions with the Web Services. NUMI utilizes the VDIF service to access patient information from VistA.

The NUMI application server is installed on 2 web servers, configured for fail over. This ensures that requests are being submitted to the application server. A load balancer directs the requests to the server with the least load, giving the user an improved response time.

3.2.2 Load Balancer

The load balancer at the primary production site will be configured to distribute requests evenly between the two web application servers.

3.3 NUMI Web Application

The NUMI web application consists of services that interact with the Controller layer and, subsequently, VDIF services to retrieve patient information from VistA. The NUMI web application makes JavaScript calls to the CERMe application to retrieve Change Healthcare InterQual® information. Together, this information enables the users to determine what is needed to provide the appropriate level of care to the patients. The NUMI web application interacts with the NUMI.

GUI (graphical user interface) components and the NUMI front end, which is viewed by the UM users.

3.4 Controller Layer

The Controller layer manages the interactions between the NUMI web application, the VDIF services and the NUMI database. Components of the controller include the Business Logic Layer, Business Object Layer, and the Data Access Layer (DAL). To facilitate interactions with the NUMI web application, calls are made to the VDIF NUMIService (see Table 2 for the list of NUMIService operations), and managed by the Controller layer.

3.4.1 Stay Synchronizer

The Stay Synchronizer is a Windows service which retrieves admission, transfer and discharge data from the VistA systems across the VA. Reminders will be updated by the Synchronizer when it detects that a stay has changed. This includes stays that have been dismissed or that have had continuing stay reminders set by the reviewer.

The Synchronizer consists of an hourly and daily import of admission, transfer, and discharge records from VistA. The daily synchronization occurs at midnight local time for each VistA system. The Synchronizer can also be configured to retry missed daily synchronizations. For example, if the Synchronizer stops working on the first of the month and is restarted on the second, it will attempt to synchronize the admission, transfer, and discharge records it missed on the first.

Data flows from VistA to NUMI. NUMI does not send anything back to VistA. If information changes in VistA, the corresponding information in NUMI will be overwritten in the next Synchronizer feed. However, if a patient stay is deleted in VistA it is not automatically deleted in NUMI. To address that situation, NUMI Administrators will be able to manually inactivate the stay in NUMI.

3.4.2 Data Access Layer (DAL)

The NUMI DAL is a component of the Controller layer. It facilitates access to the NUMI database,

the data source used to store the patient review data, using a data access object solution strategy. This data is consolidated from the data retrieved from VistA and the criteria retrieved from CERMe, establishing a patient review history for use by the NUMI application.

3.4.3 NUMI Exchange

The NUMI Exchange web service will provide interoperability to different VA applications and systems by exposing NUMI data from the NUMI database. Only applications with valid authentication and privileges will be allowed to execute the published web service methods; all requests are logged. Future implementations and enhancements will allow for creation and updating of database records. NUMI Exchange should be secured with a valid Secure Socket Layer certificate.

NUMI Exchange is implemented through a web method named GetLevelOfCareBySite at Inpatient.asmx. It has the following input parameters:

AuthenticationID (guid/uniqueidentifier) SiteCodeList (string/varchar (2000))

The SiteCodeList can be a SiteCode from a single site (which will result in returned data from one site), a comma-separated list of several SiteCodes (which will return data from multiple sites), or an empty string. An empty string parameter will return data from all sites. GetLevelOfCareBySite has the following parameters:

Message (string) - Used to display error messages Array of...

SITE_CODE (string/varchar (10)) PATIENT_SSN (string/varchar (15)) LEVEL_OF_CARE (byte/bit)

ASSIGNMENT_DATE (DateTime/smalldatetime)

3.4.4 Veterans Data Integration and Federation Enterprise Platform (VDIF-EP)

VDIF is a suite of web services that exposes medical domain data and functionality by accessing legacy systems where data resides. VDIF exposes this healthcare data by means of web services constructed with modular and extensible architecture. The VDIF system is standards-based and designed to support existing data and performance requirements while anticipating growth in the exposure of new data domains through web service interfaces. This provides a single enterprise application executing in a particular site, which can be scaled to support the anticipated growth of usage by the user community and the current demands for healthcare data.

The VDIF product modularizes the services exposed to external applications and encapsulates the internal service execution logic to enable rapid change through the use of dependency injection and other techniques for developing loosely coupled, maintainable architectures. Dependency injection is a software engineering pattern that helps alleviate the need for hardcoding components, such as RPC identifiers and specific service modules.

VDIF web services provide synchronous access to data retrieved from multiple data sources, primarily VistA. A single service call may invoke other services in a federated fashion. This is done by executing the calls to data access services in separate threads maintained by a managed thread pool. At the completion of the data retrieval requests, the data is aggregated and combined to provide

the response to the client system that initiated the service request.

Table 2 contains the list of VDIF NUMIService operations used by the NUMI web application. NUMI communicates to VDIF and VDIF communicates to VistA.

The NUMI web application is configured to receive a maximum of 10,000 records per VDIF service call. This value is configured in the NumiServiceImplService WSDL implementation by changing the MaxOccurs as shown in the example below:

```
<xs:sequence>
   <xs:element minOccurs="0" maxOccurs="10000" form="unqualified" name="taggedText" type="tns:taggedText" />
</xs:sequence>
```

Table 2: NUMIService Operations

Method	Summary
inpatientStayTO	**getStayMovements** (QueryBean queryBean) Get patient movement records associated with a checkin ID.
taggedInpatientStayArrays	**getStayMovementsByDateRange** (QueryBean queryBean) Gets patient movement records falling within given start and end dateTime.
taggedInpatientStayArrays	**getStayMovementsByPatient** (QueryBean queryBean) Gets all selected patient movement records.
regionArray	**getVHA** (QueryBean queryBean) Get all VHA sites.
taggedTextArray	**issueConfidentialityBulletin** (QueryBean queryBean) Get patient confidentiality from all connected sites.
taggedPatientArray	**MatchVDIF** (QueryBean queryBean) Match patients at logged-in site using the target received.
patientTO	**Select** (QueryBean queryBean) Select a patient at logged-in site.
taggedUserArrays	**userLookup** (QueryBean queryBean) Checks if the user is authenticated in VistA with an active account.

3.4.5 Care Enhance Review Management Enterprise (CERMe)

CERMe is a COTS web application developed by the Change Healthcare Corporation. During the documentation of the clinical features relevant to the patient's condition, CERMe is used by the Utilization Management staff to review the patient information against the InterQual® criteria, thus establishing the appropriate level of care. The CERMe web application is deployed to the same server as NUMI, though the web application runs in a separate web container. The CERMe database is on the same database server as the NUMI database.

3.5 NUMI UserInterface (UI) Components

The NUMI UI is developed as Active Server Pages (ASP).net pages. Known officially as "web forms"(files with the extension ASPX); the ASP.net pages are the main building block for application development. These Web forms contain static (X) HTML markup, as well as markup defining server-side Web Controls and User Controls where the developers place all the required static and dynamic content for the web page. The NUMI web forms interact with the VDIF service through the Controller layer. Table 3 describes the major web forms developed for the NUMI application.

Table 3: NUMI UI Components

File Name	Description
AdminQuery.aspx	NUMI administrators can query the NUMI database through the interface on this page.
AdminSites.aspx	Site Admin page. This page allows authorized users to add VistA users to Primary Reviewer, Physician Reviewer, Site Administrator, Report Only panels, and remove them from the panels.
Authenticated/Default.aspx	Select NUMI configuration values can be updated by NUMI administrators on this page.
CERME.aspx	CERMe page. This is the NUMI page that facilitates access to Change Healthcare's CERMe InterQual® criteria.
DeceasedWarning.aspx	NUMI splash screen. This page displays a warning prior to displaying a deceased patient's record.
DismissalAdmin.aspx	Site administrators can configure treating specialties as Reviewable or Not Reviewable.
History.aspx	NUMI History Page. This page allows an authorized user to view the patient stay history. The user can review current or previous stays by selecting items from Movement and Review tables.
Home.aspx/Default.aspx	Select VISN, then Site (NUMI home. This page enables an authorized user to login to NUMI.
Login.aspx	This is an intermediate page that handles authentication headers passed in by the Identity and Access Management (IAM) Single Sign On (SSO) login page. This page immediately redirects to Default.aspx after the headers are read and a forms authentication ticket has been created.
Logout.aspx	NUMI Logout page. his page is accessed from the Tools menu and is where users will logout of NUMI.
NumiUserEdit.aspx	NUMI New User/Privileges page. This page includes functionality for editing user privileges and is accessed from the Admin menu. The page allows authorized users to add and edit NUMI users, and deactivate user site access.
NumiUserList.aspx	NUMI User List page. This page is accessed from the Admin menu and allows authorized users to retrieve a list of NUMI users by VistA, or by site.
PAReview.aspx	NUMI Physician Reviewer Review page. This page allows a Physician Reviewer to perform a patient review.
PatientDetails.aspx	Report #7 - Patient Details Report. This report is accessed from the Reports menu and allows users to see all reviews saved for a specific patient for a selected time period.
PatientLevelMetNotMet.aspx	Report #5 - Patient Level Met/Not Met Report. This report is accessed from the Reports menu and allows users to see a basic patient level report.
PatientLevelMetNotMetCustom.aspx	Report #6 – Patient Level Met/Not Met Custom Report. This report shows the same information that Report #5 does, except it includes information that was typed into the Custom field on the Primary Review screen.
PatientSelection.aspx	NUMI Patient Selection/Worklist Page. This page is accessed from the Tools menu and allows an authorized user to select a patient based on patient selection methods, and other criteria.

PatientSelectionDismissed.aspx	NUMI Dismissed Patient Stays page This page is accessed from the Tools menu and allows users to see the list of patient stays dismissed from an earlier review.
PatientSelectionSearch.aspx	Free Text Patient Search page. This page is accessed from the Tools menu and allows users to search for patients using various filters and text entry options.
PatientStayAdmin.aspx	Patient Stay Administration page. This page is accessed from the Tools menu and allows users to search for stays that are on NUMI but have been removed from VistA.
PatientWorksheet.aspx	Patient Worksheet page. This page displays after a button is selected on the History page. Users can print a hardcopy out and take it with them on rounds.
PhysicianAdvisor.aspx	Decommissioned page in NUMI 14.4. Replaced by external NUMI Enhanced reports. https://vaww.rtp.portal.va.gov/OQSV/10A4B/NUMI/enhanced/SitePages/Home.aspx
PhysicianUMAdvisorResponse.aspx	Decommissioned page in NUMI 14.4. Replaced by external NUMI Enhanced reports. https://vaww.rtp.portal.va.gov/OQSV/10A4B/NUMI/enhanced/SitePages/Home.aspx
PortraitReport.aspx	After reports have been generated and a print preview button is selected, the output will display in a PortraitReport.aspx window.
PrimaryReview.aspx	NUMI Primary Review page. This page allows users to perform a primary review (and indicate whether a Physician Reviewer review is required if criteria is not met).
ReasonsCSReviews.aspx	https://vaww.rtp.portal.va.gov/OQSV/10A4B/NUMI/enhanced/SitePages/Home.aspx
ReasonsforAdmReviews.aspx	Decommissioned page in NUMI 14.4. Replaced by external NUMI Enhanced reports. https://vaww.rtp.portal.va.gov/OQSV/10A4B/NUMI/enhanced/SitePages/Home.aspx
Review.aspx	Review Summary page. This page allows users to look at Primary Review, Physician Reviewer summary information for patients, as well as view only CERMe Review text.
ReviewSelection.aspx	NUMI Patient Reviews page. This page is accessed from the Tools menu and allows users to work with reviews that have been saved for later review or locked to the database. Authorized users can unlock primary review and physician reviewer reviews and delete reviews from this page.
SensitiveWarning.aspx	NUMI splash screen. This page displays a warning prior to displaying a restricted patient's record. This ensures that users are aware prior to retrieving a Sensitive record and that the record is protected by the Privacy Act of 1974.
ServerReconnect.aspx	Blank web page used by JavaScript to re-establish connection between the client side and server side; this keeps the user logged in after screen mouse movements, clicks, and key presses.
ServerRecycled.aspx	This page displays a message to inform the user that their web session has terminated unexpectedly. This is different than a timeout due to idleness.

SummaryMetNotMet.aspx	Decommissioned page in NUMI 14.4. Replaced by external NUMI Enhanced reports. https://vaww.rtp.portal.va.gov/OQSV/10A4B/NUMI/enhanced/SitePages/Home.aspx
SummaryRLOCReason.aspx	Decommissioned page in NUMI 14.4. Replaced by external NUMI Enhanced reports. https://vaww.rtp.portal.va.gov/OQSV/10A4B/NUMI/enhanced/SitePages/Home.aspx
SyncOnDemand.aspx	NUMI Sync on Demand page. This page is accessed from the Tools menu and allows an authorized user to synchronize the patient stays with the information in VistA.
TimeOut.aspx	This page displays a message to the user informing them that they were automatically logged out from the system due to idleness.
Unscheduled30DayReadmit.aspx	Decommissioned page in NUMI 14.4. Replaced by external NUMI Enhanced reports. https://vaww.rtp.portal.va.gov/OQSV/10A4B/NUMI/enhanced/SitePages/Home.aspx
Welcome.aspx	This page will be used in future versions of NUMI; currently it will simply redirect the user to their home page.

4 Parameters

This chapter provides an overview of NUMI application parameters.

4.1 Timeout Parameter

The NUMI application times out after twenty (20) minutes of inactivity by the user. Users may experience shorter timeouts if their browser timeout is less than 20 minutes. After a timeout, users will need to reinitiate the normal login procedures

4.2 Lockout Parameters

VistA will initiate a login restriction to NUMI for 20 minutes after a pre-determined number of unsuccessful login attempts. The precise number of permitted attempts varies by VistA, and lockout is according to local VistA policy. An error message will display to the user and, after 20 minutes have elapsed, VistA will automatically clear the login restriction and the user can try to login again. Users may request their local IRM to reset the login attempt count on their VistA profile to avoid the 20 minute delay.

4.3 Date Format Parameters

The NUMI application uses a consistent date format on the GUI – mm/dd/yyyy. This is the same way it is displayed in VistA.

4.3.1 Date Value Parameters

- Valid values for ‘Month’ are 1 thru 12
- Valid values for ‘Day’ are 1 thru 31

4.3.2 Day Being Reviewed Date Parameters

- In the "Day Being Reviewed Date" field on the Primary Review screen, the calendar will only permit users to select a date between the Admission and Discharge dates. If they manually type in a date, it must be within that range. If a date outside that range is provided, a message similar to this will display: "Please select a review date between <*admit date*> and <*discharge date*>".

4.3.3 Start Date and End Date Parameters

- When selecting "Start Date" and "End Date" values in NUMI, the End Date must be after the Start Date or the user will get an error message. Start Date and End Date fields in NUMI are located in:
- The "Reminder Date" filter on the Patient Selection/Worklist screen
- The "Date" filter on the Patient Reviews screen
- All Report filter screens

4.4 Text Entry Field Parameters

- The system imposes restrictions on how many characters can be entered into certain text entry fields.
- The system imposes a maximum limit of 100 text entry characters in the Custom text entry field on the Primary Review screen
- The system imposes a maximum limit of 4,000 text entry characters in the Comments field on the Physician Advisor Review screen

5 Remote Procedure Calls (RPCs)

RPCs for NUMI are handled by VDIF. VDIF interacts directly with VistA. NUMI does not.

6 Database Information

The NUMI database stores information on patient movements. NUMI does not modify, update or delete data on the VistA system. A Data Access Objects (DAO) solution strategy was utilized for the database architecture. The DAO avoids the need to create a shared data source, thus eliminating the need to collate the information dynamically. This gives the application the ability to access data from multiple data sources, encapsulating the data through the application programming interface (API), presenting it in the appropriate form for each database. The NUMI DAO architecture model is depicted in Figure 2 and the VDIF DAO architecture model is depicted in Figure 3.

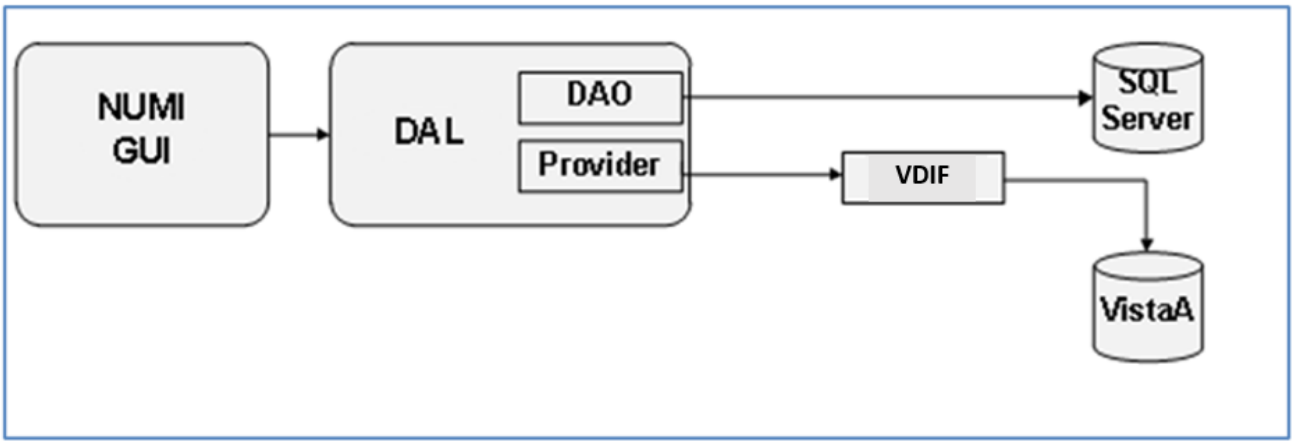

Figure 2: NUMI DAO Architecture Model

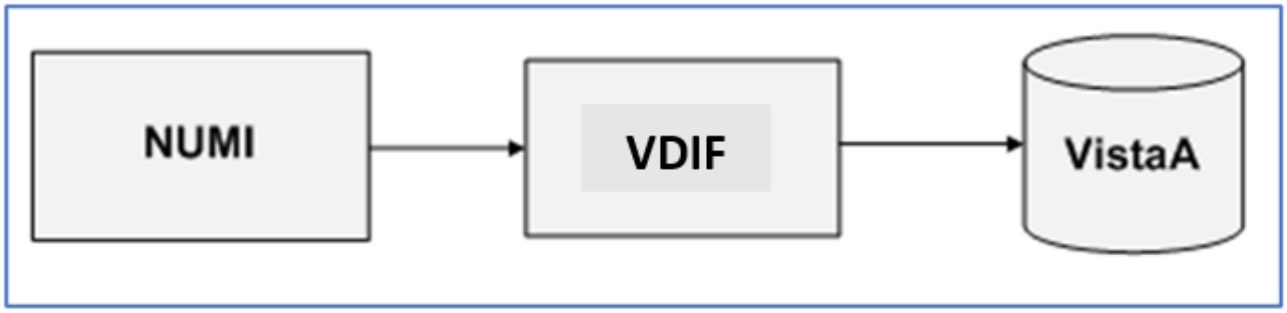

Figure 3: VDIF DAO Architecture Model

The DAO manages the connection with the data source to obtain and store data. As for the validation being done prior to storing the data in the NUMI database and what happens if the validation fails, schema-level validation as well as valid data checks depend on the operation. In fully automated operations, an event is stored in the database. This can be checked by Tier 3 support. In user-interactive operations, the system will prompt the user for the correct input.

By implementing the access mechanism required to work with the data source, the business component that relies on the DAO is able to use the simpler API exposed by the DAO for its clients. This interface does not change when the underlying data source implementation changes, thus allowing the DAO to adapt to different storage schemes without affecting its clients or business components. This middle tier translates the requests into the relevant SQL and provides the results in an array of objects that the GUI can interpret.

The DAO does not directly access any database. It sends requests in the format accepted by the target database management system, to retrieve or modify data on the target system.

When talking to a SQL database backend, the DAOs use SQL stored procedures to select, update, and delete database information. Information from VistA is retrieved by NUMI, talking to VDIF using Web Services.

6.1 Relational Tables

Information about the NUMI tables and how they inter-relate is managed by the Tier 3 Development Team.

6.2 Schema

Not Applicable. Schemas are not called in the SQL server like they are in the Oracle database.

6.3 Database Users

Table 4 identifies the authorized NUMI database users. The name of the database is NUMI.

Table 4: Authorized NUMI Database Users

User	Description
NUMI_OWNER	• Owns the NUMI database only. • Can perform all Data Definition Language activities including: altering, creating and deleting tables, indices, views, stored procedures, etc. • Cannot perform any Administrator activities.
NUMI_USER	• This user only has Data Manipulation Language roles. • Can insert, update and select tables and call stored procedures and functions.

6.4 Database Tables

The UM patient review data is stored in the NUMI database. The NUMI data model is defined based on the Entity-Relationship Model and is managed by the Tier 3 Development Team. The data model depicts the elements and fields that support the NUMI infrastructure and the database structure must be able to support data coming from multiple data sources. Subsections 6.4.1 thru 6.4.43 describe the database tables for NUMI and list the data elements, associated data types and File Number/Field Number from VistA (where applicable).

NOTE: The "Internal Entry Number" (IEN) is for a VistA file. The acronym IEN appears in some tables.

6.4.1 Table: AdminLogging

Table 5: AdminLogging

Element Name	Data Type	Indexed	Primary Key	Foreign Key
AdminLoggingID	int	Yes	Yes	No
ConnectionString	varchar(50)	No	No	No
DomainUser	varchar(50)	No	No	No
Query	nvarchar(max)	No	No	No
DateCreated	datetime	No	No	No

6.4.2 Table: AdmissionReviewType

Table 6: AdmissionReviewType

Element Name	Data Type	Indexed	Primary Key	Foreign Key
AdmissionReviewTypeID	tinyint	Yes	Yes	No
AdmissionReviewTypeDesc	nvarchar(50)	No	No	No
DateInactive	smalldatetime	No	No	No
Inactive	bit	No	No	No
ColumnOrder	tinyint	No	No	No
AdmissionReviewMask	bit	No	No	No

6.4.3 Table: AdmissionSource

Table 7: AdmissionSource

Element Name	Data Type	Indexed	Primary Key	Foreign Key
AdmissionSourceID	int	Yes	Yes	No
AdmissionSourceDesc	nvarchar(50)	Yes	No	No
DateInactive	smalldatetime	No	No	No
ColumnOrder	int	No	No	No

6.4.4 Table: CareLevel

Table 8: CareLevel

Element Name	Data Type	Indexed	Primary Key	Foreign Key
CareLevelID	tinyint	Yes	Yes	No
Identification number for a Level of Care				
CareLevelType	tinyint	No	No	No
Care level that is associated with a patient				
CreatedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
ModifiedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
CareLevelDesc	varchar(250)	Yes	No	No
Description of the level of care being given to a patient				
Version	varchar(10)	No	No	No
Version associated with CareLevel				
DateCreated	datetime	No	No	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Date that the record was created				
DateModified	datetime	No	No	No
Date that the record was modified				
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
CLOC	bit	No	No	No
Indicator to identify if care level is applicable for Current Level of Care (CLOC) when the value is 1. A value of 0 means it is not CLOC.				
RLOC	bit	No	No	No
Indicator to identify if care level is applicable for Recommended Level of Care (RLOC) when the value is 1. A value of 0 means it is not RLOC.				

6.4.5 Table: CareType

Table 9: CareType

Element Name	Data Type	Indexed	Primary Key	Foreign Key
CareTypeID	int	Yes	Yes	No
CareTypeDesc	varchar(50)	No	No	No
DateInactive	smalldatetime	No	No	No
Inactive	bit	No	No	No

6.4.6 Table: CERMeReviewXML

Table 10: CERMeReviewXML

Element Name	Data Type	Indexed	Primary Key	Foreign Key
CermeReviewXMLID	bigint	Yes	Yes	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
PatientReviewID	bigint	Yes	No	Yes
CERMEXML	varchar(max)	No	No	No
Extended Markup Language required to analyze fields from Change Healthcare CERMe				
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				

6.4.7 Table: CriteriaMetDetailedOutcome

Table 11: CriteriaMetDetailedOutcome

Element Name	Data Type	Indexed	Primary Key	Foreign Key
criteriaMetDetailedOutcomeID	tinyint	Yes	Yes	No
Identification number for a criteria met detailed outcome				
detailedOutcome	varchar(50)	No	No	No
Detailed description of a criteria met detailed outcome				
criteriaMet	bit	No	No	No
Value for critieria met in previous versions of CERMe, used to map new values to old reports				
dateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				

6.4.8 Table: DismissStayReason

Table 12: DismissStayReason

Element Name	Data Type	Indexed	Primary Key	Foreign Key
ColumnOrder	tinyint	No	No	No
Order in which Facility Treating Specialty values are displayed on application screens				
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
DismissStayReasonDesc	varchar(50)	No	No	No
Description of the reason for a patient stay dismissal				
DismissStayReasonID	tinyint	Yes	Yes	No
Identification number for a Dismissed stay Reason				
Inactive	bit	No	No	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				

6.4.9 Table: ExchangeAuthentication

Table 13: ExchangeAuthentication

Element Name	Data Type	Indexed	Primary Key	Foreign Key
AuthenticationID	uniqueidentifier	Yes	Yes	No
TeamName	varchar(50)	No	No	No
TeamContact	varchar(50)	No	No	No
ContactEmail	varchar(50)	No	No	No
ContactPhone	varchar(10)	No	No	No
DateCreated	datetime	No	No	No
DateModified	datetime	No	No	No
DateInactive	datetime	No	No	No
Inactive	bit	No	No	No

6.4.10 Table: ExchangeAuthenticationPermissions

Table 14: ExchangeAuthenticationPermissions

Element Name	Data Type	Indexed	Primary Key	Foreign Key
PermissionID	int	Yes	Yes	No
AuthenticationID	uniqueidentifier	No	No	Yes
RoleID	int	No	No	Yes
CanSelect	bit	No	No	No
CanCreate	bit	No	No	No
CanUpdate	bit	No	No	No
CanDelete	bit	No	No	No
DateCreated	datetime	No	No	No
DateModified	datetime	No	No	No
DateInactive	datetime	No	No	No
Inactive	bit	No	No	No

6.4.11 Table: ExchangeAuthenticationRoles

Table 15: ExchangeAuthenticationRoles

Element Name	Data Type	Indexed	Primary Key	Foreign Key
RoleID	int	Yes	Yes	No
RoleDescription	varchar(50)	No	No	No
DateInactive	datetime	No	No	No
Inactive	bit	No	No	No

6.4.12 Table: ExchangeLog

Table 16: ExchangeLog

Element Name	Data Type	Indexed	Primary Key	Foreign Key
ExchangeLogID	int	Yes	Yes	No
AuthenticationID	uniqueidentifier	No	No	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
RemoteAddress	varchar(50)	No	No	No
MethodName	varchar(50)	No	No	No
MethodParameters	varchar(max)	No	No	No
DateCreated	datetime	No	No	No

6.4.13 Table: FacilityTreatingSpecialty

Table 17: FacilityTreatingSpecialty

Element Name	Data Type	Indexed	Primary Key	Foreign Key
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
FacilityTreatingSpecialtyDesc	varchar(100)	No	No	No
Description of a Facility Treating Specialty	VistA File / Field 45.7 / .01			
FacilityTreatingSpecialtyID	smallint	Yes	No	No
Identification number for a Facility Treating Specialty				
FacilityTreatingSpecialtyIEN	varchar(50)	Yes	Yes	No
VistA identifier for a Facility Treating Specialty	VistA File / Field 45.7/.01			
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
ServiceSectionID	smallint	Yes	No	Yes
Identification number for a Service Section	VistA File / Field 45.7 / 1			
SiteID	smallint	Yes	Yes	Yes
Identification number for a Site				
SpecialtyID	smallint	Yes	No	No
Identification number for a Treating Specialty that can be associated with ANY Facility or Ward	VistA File / Field 45.7 / 1			
TreatingSpecialtyDismissalTypeID	int	No	No	Yes
Dismissal Type associated with Facility Treating Specialty				
CreatedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
DateCreated	datetime	No	No	No
Date that the record was created				
DateModified	datetime	No	No	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Date that the record was modified				
ModifiedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				

6.4.14 Table: ExchangeState

Table 18: ExchangeState

Element Name	Data Type	Indexed	Primary Key	Foreign Key
ExchangeStateID	int	Yes	Yes	No
Description	varchar(50)	No	No	No
DateInactive	datetime	No	No	No
Inactive	bit	No	No	No

6.4.15 Table: MASMovementTransactionType

Table 19: MASMovementTransactionType

Element Name	Data Type	Indexed	Primary Key	Foreign Key
DateInactive	smalldatetime	No	No	**No**
Date that the record was inactivated				
Inactive	bit	No	No	**No**
Indicator that the record is inactive; a value of 0 means the record is ACTIVE, a value of 1 means that the record is inactive				
MASMovementTransactionTypeDesc	varchar(100)	No	No	**No**
Description of a Medical Administration Service Movement Transaction Type	VistA File / Field 405.2 / .01			
MASMovementTransactionTypeID	tinyint	Yes	Yes	**No**
Identification number for a Medical Administration Service Movement Transaction Type				
MASMovementTransactionTypeIEN	varchar(50)	No	No	**No**
VistA identifier for a Medical Administration Service Movement Transaction Type	**VistA File / Field 405 / .18 405.2 / IEN**			

6.4.16 Table: InfoLog

Table 20: InfoLog

Element Name	Data Type	Indexed	Primary Key	Foreign Key
InfoLogID	bigint	Yes	Yes	No
Log Record ID number				
Info	nvarchar(200)	No	No	No
Error Message				
Error	bit	No	No	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Indicator of error				
StartTime	datetime	No	No	No
Start time that error was logged				
EndTime	datetime	No	No	No
End Time that error was logged				
UserName	nvarchar(50)	No	No	No
Identity of Logged on Vista User				
UserID	nvarchar(50)	No	No	No
Vista User ID				
ProcessId	int	No	No	No
Identity of Process				
ThreadId	int	No	No	No
Identity of Thread				
ProcessName	nvarchar(50)	No	No	No
Name of Process				
ClassName	nvarchar(200)	No	No	No
Name of Class				
MethodName	nvarchar(50)	No	No	No
Name of Method				
Date Created	datetime	No	No	No
Created Date				

6.4.17 Table: MASMovementType

Table 21: MASMovementType

Element Name	Data Type	Indexed	Primary Key	Foreign Key
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
MASMovementName	varchar(100)	Yes	No	No
Description of a Medical Administration Service Movement	VistA File / Field 405.2 / .01			
MASMovementTypeID	smallint	Yes	No	No
Identification number for a Medical Administration Service Movement Type				
MASMovementTypeIEN	varchar(50)	Yes	Yes	No
VistA identifier for a Medical Administration Service Movement Type	VistA File / Field 405 / .18 405.2 / IEN			
SiteID	smallint	Yes	Yes	Yes
Identification number for a Site				

6.4.18 Table: NumiConfig

Table 22: NumiConfig

Element Name	Data Type	Indexed	Primary Key	Foreign Key
NumiConfigID	int	Yes	Yes	**No**
SiteID	smallint	No	No	No
ConfigSetting	varchar(100)	No	No	**No**
ConfigValue	varchar(max)	No	No	**No**
CreatedByNumiUserID	int	No	No	**No**
ModifiedByNumiUserID	int	No	No	**No**
DateCreated	datetime	No	No	**No**
DateModified	datetime	No	No	**No**
DateInactive	datetime	No	No	**No**
Inactive	**bit**	**No**	**No**	**No**

6.4.19 Table: NumiUser

Table 23: NumiUser

Element Name	Data Type	Indexed	Primary Key	Foreign Key
CreatedByNumiUserID	int	No	No	**No**
Identification number for a NUMI user				
DateCreated	datetime	No	No	**No**
Date that the record was created				
DateInactive	smalldatetime	No	No	**No**
Date that the record was inactivated				
DateModified	datetime	No	No	**No**
Date that the record was modified				
DUZ	bigint	Yes	Yes	**No**
Vista identifier for a User	VistA File / Field 200 / IEN			
Inactive	bit	No	No	**No**
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
IsSuperUser	bit	No	No	**No**
Indicator that the User is a SuperUser within the NUMI application; a value of 0 means that the User is NOT a SuperUser, a value of 1 means that the user IS a SuperUser				
ModifiedByNumiUserID	int	No	No	**No**
Identification number for a NUMI user				
networkCredential	varchar(40)	No	No	**No**
Windows Active Directory identifier associated with the User				
NumiUserID	int	Yes	No	**No**
Identification number for a User				

Element Name	Data Type	Indexed	Primary Key	Foreign Key
SiteID	smallint	Yes	Yes	**Yes**
Identification number for a Site				
VISTAName	varchar(80)	No	No	**No**
Name that the VistA system associates with a user	VistA File / Field200 / .01			
IncludeObservation	**bit**	**No**	**No**	**No**

6.4.20 Table: NumiUserSiteActivityBitmask

Table 24: NumiUserSiteActivityBitmask

Element Name	Data Type	Indexed	Primary Key	Foreign Key
ActivityBitmask	binary(32)	Yes	No	**No**
CreatedByNumiUserID	int	No	No	**Yes**
Identification number for a NUMI user				
DateCreated	datetime	No	No	**No**
Date that the record was created				
DateInactive	smalldatetime	No	No	**No**
Date that the record was inactivated				
DateModified	datetime	No	No	**No**
Date that the record was modified				
Inactive	bit	No	No	**No**
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
ModifiedByNumiUserID	int	No	No	**Yes**
Identification number for a NUMI user				
NumiUserID	int	Yes	Yes	**Yes**
Identification number for a NUMI user				
NumiUserSiteActivityBitmaskID	bigint	Yes	No	**No**
Reason	varchar(2000)	No	No	**No**
SiteID	smallint	Yes	Yes	**Yes**
Identification number for a Site				

6.4.21 Table: Patient

Table 25: Patient

Element Name	Data Type	Indexed	Primary Key	Foreign Key
ConfirmedVistaTestPatient	bit	Yes	No	**No**
DateInactive	smalldatetime	No	No	**No**
Date that the record was inactivated				
DeceasedDate	smalldatetime	Yes	No	**No**
Date a patient was deceased	VistA File / Field 2 / .351			
DFN	Bigint	Yes	Yes	**No**

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Identification of a patient Data File Number	VistA File / Field 2 / IEN			
ICN	Bigint	No	No	**No**
	VistA File / Field 2 / 991.01			
Inactive	Bit	No	No	**No**
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
MergeToDfn	Bigint	No	No	**No**
PatientID	int	Yes	No	**No**
Identification number for a patient				
PatientName	varchar(100)	Yes	No	**No**
Name that the NUMI system associates with a patient	VistA File / Field 2 / .01			
PseudoSSN	bit	No	No	**No**
Fake Social Security Number associated with a patient to protect the patient's identity	VistA File / Field 2 / .09			
SensitivityLevel	varchar(1)	Yes	No	**No**
Indicator that a patient is either Sensitive or non- Sensitive for identity protection. A value of 0 indicates that the patient does not require additional identity protection, a value of 1 indicates that the patient needs additional identity protection	VistA File / Field 38.1 / N/A			
Sex	varchar(1)	No	No	**No**
Sex designation associated with a patient	VistA File / Field 2 / .02			
SiteID	smallint	Yes	Yes	**Yes**
Identification number for a Site				
SSN	varchar(15)	Yes	No	**No**
Social Security Number associated with a patient	VistA File / Field 2 / .09			
VistaTestPatient	bit	Yes	No	**No**
Indicator that a patient is a fictional "Test patient" copied over from VistA. A value of 0 indicates that the patient is a real patient; a value of 1 indicates that the patient is fictitious. This field is not currently used by the NUMI system	**VistA File / Field 2 / 2**			

6.4.22 Table: PatientAudit

Table 26: PatientAudit

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Comments	varchar(2000)	No	No	No
Comments				
CreatedBy	int	No	No	Yes
DateCreated	datetime	No	No	No
Date that the record was created				
PatientAuditID	int	Yes	Yes	No
PatientID	int	No	No	Yes

6.4.23 Table: PatientReview

Table 27: PatientReview

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Comments	varchar(4000)	No	No	No
Comments				
CreatedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
CriteriaMet	bit	Yes	No	No
Indicator that a patient has met InterQual criteria for the current Level of Care. A value of 0 indicates that the patient has NOT met the InterQual criteria, a value of 1 indicates that the patient has met the InterQual criteria				
CurrentCareLevelID	tinyint	No	No	Yes
Identification number for a Level of Care				
CurrentCareLevelOther	varchar(1000)	No	No	No
Additional description about the current level of care in a patient review				
Custom	varchar(25)	No	No	No
Comments - maximum length 25 characters				
DateCreated	datetime	No	No	No
Date that the record was created				
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
DateModified	datetime	No	No	No
Date that the record was inactivated				
FacilityTreatingSpecialtyID	smallint	No	No	Yes
Identification number for a Facility Treating Specialty				
HospitalAdmissionReview	tinyint	No	No	Yes

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Identification number for a Hospitalization Admission review Type. Possible values and their meaning are listed below: 0 No Review 1 Not an Admission Review 2 Hosp Acute Adm - Traditional Criteria 3 Admission Review-Type- Unknown 4 BH Initial Review 5 Transfer to Higher Level of Care 6 Transfer to/from Acute Care and BH 7 Observation converted to Hospital Admission 8 Hosp Acute Adm - Condition-Specific Criteria 9 Conversion to New Condition-Specific Criteria 10 Observation Review 11 Hospital Acute Admission 12 Admission Converted to Observation				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
InitialCompletedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
InsuranceCompanyDesc	varchar(6000)	No	No	No
Name of the patient's Insurance Company				
IQSubsetID	smallint	No	No	No
Identification of an InterQual subset designation associated with a patient review				
MASMovementTransactionTypeID	tinyint	No	No	Yes
Identification number for a Medical Administration Service Movement Transaction Type				
ModifiedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
NoPaReviewRequired	tinyint	No	No	No
Indicator that a Physician Advisor review, is needed. A value of 0 indicates a Physician Advisor review is NECESSARY, a value of 1 a Physician Advisor review is NOT necessary				
PatientAge	tinyint	No	No	No
Age of a patient associated with a review	VistA File / Field 2 / .033			
PatientID	int	Yes	No	Yes
Identification number for a patient				
PatientReviewID	bigint	Yes	Yes	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Identification number for a patient review				
PatientStayID	bigint	Yes	No	Yes
Identification number for a patient stay				
ReasonID	smallint	No	No	Yes
Identification number for a Reason Code				
RecommendedCareLevelID	tinyint	Yes	No	Yes
Identification number for a Level of Care				
RecommendedCareLevelOther	varchar(2000)	No	No	No
Additional description about the recommended level of care in a patient review				
ReviewDate	smalldatetime	Yes	No	No
Date a patient was reviewed				
ReviewLevel	tinyint	No	No	No
ReviewTypeID	tinyint	Yes	No	Yes
Identification number for a patient review Type				
ServiceSectionID	smallint	No	No	Yes
Identification number for a Service Section				
StatusChangeDate	datetime	No	No	No
Date that the patient's status changed				
StatusID	tinyint	No	No	Yes
Identification number for a patient review status				
StatusNumiUserID	int	No	No	Yes
Identification number for a NUMI user status				
TeamID	smallint	No	No	No
UMRAttendingPhysicianID	int	No	No	Yes
Identification number for an Attending Physician				
UMRFacilityTreatingSpecialtyID	smallint	No	No	Yes
Identification number for a Facility Treating Specialty				
UMRServiceSectionID	smallint	No	No	Yes
Identification number for a Service Section				
UMRWardLocationID	smallint	No	No	Yes
Identification number for a Ward location				
Unscheduled30DayReadmit	bit	No	No	No
VistaAttendingPhysicianID	int	No	No	Yes
VistA identification number for a Physician Advisor				
WardLocationID	smallint	Yes	No	Yes
Identification number for a Ward location				
criteriaMetOutcomeId	tinyint	No	No	Yes
NotMetComment	nvarchar(100)	No	No	No
SubsetDescription	varchar(max)	No	No	No
VersionCID	varchar(30)	No	No	No
EpisodeDayOfCare	tinyint	No	No	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
AdmissionSourceID	int	No	No	Yes
UMRAdmissionSourceID	int	No	No	Yes
AdmittingPhysicianID	int	No	No	Yes
UMRAdmittingPhysicianID	int	No	No	Yes

6.4.24 Table: PatientReviewAudit

Table 28: PatientReviewAudit

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Comments	varchar(2000)	No	No	No
Comments				
CreatedBy	int	No	No	Yes
DateCreated	datetime	No	No	No
Date that the record was created				
PatientReviewAuditID	bigint	Yes	Yes	No
PatientReviewID	bigint	No	No	Yes
StatusID	tinyint	No	No	Yes

6.4.25 Table: PatientReviewReason

Table 29: PatientReviewReason

Element Name	Data Type	Indexed	Primary Key	Foreign Key
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
OtherDesc	varchar(500)	No	No	No
Additional description about a patient review reason				
PatientReviewID	bigint	Yes	Yes	Yes
Identification number for a patient review				
PatientReviewReasonID	bigint	Yes	No	No
Identification number for a patient review reason				
ReasonID	smallint	Yes	Yes	Yes
Identification number for a patient review reason				

6.4.26 Table: PatientStay

Table 30: PatientStay

Element Name	Data Type	Indexed	Primary Key	Foreign Key
AdmissionDiagnosis	varchar(50)	No	No	No
Diagnosis for the patient at time of Admission	VistA File / Field 405 / .1			
AdmissionDRGID	smallint	No	No	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Identification number for an Admission Diagnosis Related Group	VistA File / Field 45 / 9			
AdmissionMASMovementTypeID	Smallint	No	No	Yes
Identification number for a Medical Administration Service Admission Movement Type	VistA File / Field 405 / .18 405.2 / .01			
AdmissionMovementIEN	varchar(50)	Yes	Yes	No
VistA identifier for a patient's Admission Movement	VistA File / Field 405 / IEN 405 / .14			
AdmitDate	datetime	No	No	No
Date that the patient was admitted to the hospital	VistA File / Field 405 / .01			
AdmittingPhysicianID	int	No	No	Yes
Identification number for a NUMI user	VistA File / Field 405 / .19 356.94 / .03			
AssignedReviewerID	int	Yes	No	Yes
Identification number for a NUMI user				
DateCreated	datetime	No	No	No
Date that the record was created				
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
DateModified	datetime	No	No	No
Date that the record was modified				
DischargeDate	datetime	No	No	No
Date that the patient was discharged from the hospital	VistA File / Field 405 / .01			
DischargeDRGID	smallint	No	No	No
Identification number for an Discharge Diagnosis Related Group	VistA File / Field 45.84 / 6			
DischargeMovementIEN	varchar(50)	No	No	No
VistA identifier for a patient's Discharge Movement	VistA File / Field 405 / IEN 405 / .17			
dismissStayReason	tinyint	No	No	Yes
Identification of a dismissed stay reason				
DispositionPlaceID	smallint	No	No	No
	VistA File / Field 45 / 75 45.6 / .01			
DispositionTypeID	smallint	No	No	No
	VistA File / Field 45 / 72			
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				

Element Name	Data Type	Indexed	Primary Key	Foreign Key
InvalidStay	bit	No	No	No
Indicator that the stay is not a valid stay for Utilization Management purposes. A value of 0 indicates that the stay IS valid for Utilization Management review, a value of 1 indicates that the stay is NOT valid for Utilization Management review				
LastAttendingPhysicianID	int	No	No	Yes
Identification number for a NUMI user				
LastFacilityTreatingSpecialtyID	smallint	No	No	Yes
Identification number for a Facility Treating Specialty				
LastMASMovementTransactionTypeID	tinyint	No	No	Yes
Identification number for a Medical Administration Service Last Movement Transaction Type				
LastMASMovementTypeID	smallint	No	No	Yes
Identification number for a Medical Administration Service Last Movement Type				
LastMovementDate	datetime	No	No	No
Date of last time a patient was moved/transferred prior to discharge	VistA File / Field 405 / .01			
LastMovementIEN	varchar(50)	No	No	No
VistA identifier for a patient's last stay Movement	VistA File / Field 405 / IEN			
LastServiceSectionID	smallint	No	No	Yes
Identification number for a Service Section				
LastWardLocationID	smallint	Yes	No	Yes
Identification number for a Ward location				
LengthofStay	int	No	No	No
Duration of a patient's stay in the hospital	VistA File / Field 45 / 81			
ModifiedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
NUMIHashCode	int	No	No	No
PatientID	int	Yes	Yes	Yes
Identification number for a patient				
PatientStayID	bigint	Yes	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
PriorStayDischargeDate	datetime	No	No	No
Date that the patient was discharged on their prior stay	VistA File / Field 405 / .01			
PTFIEN	varchar(50)	No	No	No
	VistA File / Field 405 / .16			
Readmission14Day	bit	No	No	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Indicator that the patient was readmitted to treatment within 14 days of discharge. A value of 0 indicates that the patient was NOT readmitted within 14 days of discharge, a value of 1 indicates that the patient WAS readmitted within 14 days of discharge				
Readmission24Hr	bit	No	No	No
Readmission30Day	bit	No	No	No
Indicator that the patient was readmitted to treatment within 30 days of discharge. A value of 0 indicates that the patient was NOT readmitted within 30 days of discharge, a value of 1 indicates that the patient WAS readmitted within 30 days of discharge				
ReminderDate	datetime	No	No	No
Date determining when the patient will be included in results within a range of Reminder Dates. This is primarily used for "worklist" kinds of screens and reports				
ReminderType	tinyint	No	No	No
Identification number for a patient stay Reminder Type				
ServiceConnectedAdmission	bit	No	No	No
	VistA File / Field 405 / .11			
LastAdmissionSourceID	int	No	No	Yes

6.4.27 Table: PatientStayAudit

Table 31: PatientStayAudit

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Comments	varchar(2000)	No	No	No
Comments				
CreatedBy	int	No	No	Yes
Identification number for a NUMI user				
DateCreated	datetime	No	No	No
Date that the record was created				
PatientStayAuditID	bigint	Yes	Yes	No
PatientStayID	bigint	No	No	Yes
StatusID	tinyint	No	No	Yes
IsAutoDismissed	bit	No	No	No

6.4.28 Table: Physician

Table 32: Physician

Element Name	Data Type	Indexed	Primary Key	Foreign Key
CreatedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
DateCreated	datetime	No	No	No
Date that the record was created				
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
DateModified	datetime	No	No	No
Date that the record was modified				
Disuser	bit	No	No	No
This field is currently not used in NUMI, and not brought in from VistA. The reference to the VistA File/Field value is for informational purposes, and future use.	VistA File / Field 200 / 7			
DUZ	bigint	Yes	No	No
Vista identifier for a User	VistA File / Field 405 / .19 200 / IEN			
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
ModifiedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
PhysicianID	int	Yes	Yes	No
Identification number for a NUMI user				
PhysicianName	varchar(100)	Yes	No	No
Name of the Physician	VistA File / Field 200 / .01			
Reason	varchar(200)	No	No	No
Reason provided by a Physician Advisor				
SiteID	smallint	Yes	No	Yes
Identification number for a Site				

6.4.29 Table: PhysicianAdvisorPatientReason

Table 33: PhysicianAdvisorPatientReason

Element Name	Data Type	Indexed	Primary Key	Foreign Key
CreatedByNumiUserID	int	No	No	No
Identification number for a NUMI user				
DateCreated	datetime	No	No	No
Date that the record was created				
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
DateModified	datetime	No	No	No
Date that the record was modified				

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
ModifiedByNumiUserID	int	No	No	No
Identification number for a NUMI user				
PAReasonCategory	tinyint	No	No	No
Identification of a Physician Advisor reason category				
PAReasonName	varchar(200)	No	No	No
Name of a Physician Advisor review reason				
PhysicianAdvisorPatientReasonID	smallint	Yes	Yes	No
Identification number for a Physician Advisor review reason				

6.4.30 Table: PhysicianAdvisorPatientReview

Table 34: PhysicianAdvisorPatientReview

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Comments	varchar(4000)	No	No	No
Comments				
CreatedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
DateCreated	datetime	No	No	No
Date that the record was created				
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
DateModified	datetime	No	No	No
Date that the record was modified				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
ModifiedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user OtherDesc	varchar(2000)	No	No	No
Additional description about the physician advisor portion of a patient review				
PatientReviewID	bigint	Yes	No	Yes
Identification number for a patient review				
PhysicianAdvisorID	int	Yes	No	Yes
Identification number for a Physician Advisor				
PhysicianAdvisorPatientReasonID	smallint	No	No	Yes
Identification number for a Physician Advisor patient review reason				
PhysicianAdvisorPatientReviewID	bigint	Yes	Yes	No
Identification number for a Physician Advisor patient review				

Element Name	Data Type	Indexed	Primary Key	Foreign Key
RecommendedCareLevelID	tinyint	No	No	Yes
Identification number for a Recommended Level of Care				
RecommendedCareLevelOther	varchar(2000)	No	No	No
Additional description about the physician advisor recommended level of care portion of a patient review				
StatusChangeDate	datetime	No	No	No
Date that the Physician Advisor record status was changed				
StatusID	tinyint	No	No	Yes
Identification number for a Physician Advisor review status				
StatusNumiUserID	int	No	No	Yes
Identification number for a NUMI user Physician Advisor review status				

6.4.31 Table: PhysicianAdvisorPatientReviewAudit

Table 35: PhysicianAdvisorPatientReviewAudit

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Comments	varchar(2000)	No	No	No
Comments				
CreatedBy	int	No	No	Yes
DateCreated	datetime	No	No	No
Date that the record was created				
PhysicianAdvisorPatientReviewAuditID	bigint	Yes	Yes	No
PhysicianAdvisorPatientReviewID	bigint	No	No	Yes
StatusID	tinyint	No	No	Yes

6.4.32 Table: Reason

Table 36: Reason

Element Name	Data Type	Indexed	Primary Key	Foreign Key
CreatedByNumiUserID	int	No	No	Yes
Date that the record was created				
DateCreated	datetime	No	No	No
Date that the record was created				
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
DateModified	datetime	No	No	No
Date that the record was modified				
Description	varchar(1000)	No	No	No
Description of a reason				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				

Element Name	Data Type	Indexed	Primary Key	Foreign Key
IsParentReason	bit	Yes	No	No
ModifiedByNumiUserID	int	No	No	Yes
Date that the record was modified				
ParentReasonID	smallint	Yes	No	No
Identification for a parent reason				
ReasonCategoryID	smallint	Yes	No	Yes
Identification for a reason category				
ReasonCode	varchar(100)	No	No	No
Identification number for a Reason Code				
ReasonDesc	varchar(900)	No	No	No
Description of a reason				
ReasonFactorID	tinyint	Yes	No	No
ReasonID	smallint	Yes	Yes	No
Identification for a reason				
ReviewerTypeID	tinyint	Yes	No	No
Identification for a reviewer type				
ReviewTypeID	tinyint	Yes	No	Yes
Identification for a review type				

6.4.33 Table: ReasonCategory

Table 37: ReasonCategory

Element Name	Data Type	Indexed	Primary Key	Foreign Key
ReasonCategoryID	smallint	Yes	Yes	No
ReasonCategoryDesc	varchar(50)	No	No	No
DateInactive	smalldatetime	No	No	No
Inactive	bit	No	No	No

6.4.34 Table: Region

Table 38: Region

Element Name	Data Type	Indexed	Primary Key	Foreign Key
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
Description	varchar(200)	No	No	No
Description of a Region				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
RegionCode	varchar(10)	Yes	No	No
Identification code for a Region				
RegionID	tinyint	Yes	Yes	No
Identification number for a Region				
RegionName	varchar(100)	No	No	No
Description of a Region name				

6.4.35 Table: Reports

Table 39: Reports

Element Name	Data Type	Indexed	Primary Key	Foreign Key
createDate	datetime	No	No	No
Date that the record was created				
Inactive	tinyint	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
inactiveDate	datetime	No	No	No
lastUpdateDate	datetime	No	No	No
Date that the record was last updated				
reportDescription	varchar(1000)	No	No	No
Description of a report				
reportDisplayName	varchar(60)	No	No	No
Identification of a report				
reportFileName	varchar(80)	No	No	No
reportId	bigint	Yes	Yes	No
Identification number for a report				
reportSortOrder	smallint	Yes	No	No
Order in which Reports are displayed on application screens				
ssrsreportpath	varchar(120)	No	No	No

6.4.36 Table: ReviewType

Table 40: ReviewType

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Abbreviation	varchar(10)	No	No	No
CERMEName	varchar(5)	Yes	No	No
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
ReviewTypeDesc	varchar(20)	No	No	No
Description of a review type				
ReviewTypeID	tinyint	Yes	Yes	No
Identification number for a review type				

6.4.37 Table: ServiceSection

Table 41: ServiceSection

Element Name	Data Type	Indexed	Primary Key	Foreign Key
DateInactive	smalldatetime	No	No	No

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Date that the record was inactivated				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
ServiceSectionDesc	varchar(100)	No	No	No
Description of a Service Section	VistA File / Field 49 / .01			
ServiceSectionID	smallint	Yes	No	No
Identification number for a Service Section	VistA File / Field 49 / IEN			
ServiceSectionIEN	varchar(50)	Yes	Yes	No
VistA identification number for a Service Section	VistA File / Field 49 / IE			
SiteID	smallint	Yes	Yes	Yes
Identification number for a Site				

6.4.38 Table: Site

Table 42: Site

Element Name	Data Type	Indexed	Primary Key	Foreign Key
DateActive	smalldatetime	No	No	No
DateInactive	smalldatetime	No	No	No
DisplayName	varchar(100)	No	No	No
Name of the displayed Site name				
FaciltyName	varchar(200)	No	No	No
Name of a Site Facility				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
Moniker	varchar(10)	Yes	No	No
Offset	smallint	Yes	No	No
SiteCode	varchar(10)	Yes	No	No
Identification code for a site				
SiteID	smallint	Yes	Yes	No
Identification number for a Site				
SiteName	varchar(100)	Yes	No	No
Name of a Site name				
Synchronize	tinyint	Yes	No	No
VISNID	tinyint	Yes	No	Yes
Identification number for a Veterans Integrated Service Network site				
IsStandardTime	bit	No	No	No

6.4.39 Table: Status

Table 43: Status

Element Name	Data Type	Indexed	Primary Key	Foreign Key
CreatedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
DateCreated	datetime	No	No	No
Date that the record was created				
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
DateModified	datetime	No	No	No
Date that the record was modified				
Enumeration	tinyint	No	No	No
Date that the record was modified				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
ModifiedByNumiUserID	int	No	No	Yes
Identification number for a NUMI user				
StatusDesc	varchar(50)	Yes	No	No
Description of a Status				
StatusID	tinyint	Yes	Yes	No
Identification number for a Status				

6.4.40 Table: TreatingSpecialtyDismissalType

Table 44: TreatingSpecialtyDismissalType

Element Name	Data Type	Indexed	Primary Key	Foreign Key
TreatingSpecialtyDismissalTypeID	int	Yes	Yes	No
DismissalTypeDesc	nvarchar(50)	No	No	No
DateInactive	smalldatetime	No	No	No
Inactive	bit	No	No	No
IsNonReviewable	bit	No	No	No

6.4.41 Table: VISN

Table 45: VISN

Element Name	Data Type	Indexed	Primary Key	Foreign Key
DateInactive smalldatetime No No No				
Date that the record was inactivated				
Description	varchar(200)	No	No	No
Description of a Veterans Integrated Service Network				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
RegionID	tinyint	Yes	No	Yes

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Identification number of a Veterans Integrated Service Network Region				
VISNCode	varchar(10)	Yes	No	No
Identification code of a Veterans Integrated Service Network				
VISNID	tinyint	Yes	Yes	No
Identification number of a Veterans Integrated Service Network				
VISNName	varchar(100)	Yes	No	No
Name of a Veterans Integrated Service Network				

6.4.42 Table: WardLocation

Table 46: WardLocation

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Bedsection	varchar(100)	No	No	No
Identifies a section of beds within a Ward location	VistA File / Field 42 / .02			
DateInactive	smalldatetime	No	No	No
Date that the record was inactivated				
Inactive	bit	No	No	No
Indicator that the record is inactive; a value of 0 means that the record is ACTIVE, a value of 1 means that the record is inactive				
Service	varchar(100)	No	No	No
Identifies a Service associated with a Ward location	VistA File / Field 42 / .03			
SiteID	smallint	Yes	Yes	Yes
Identification number for a Site				
SpecialtyID	smallint	Yes	No	No
Identification number for a Treating Specialty that can be associated with ANY Facility or Ward				
WardLocationDesc	varchar(100)	Yes	No	No
Description of a Ward location	VistA File / Field 42 / .01			
WardLocationID	smallint	Yes	No	No
Identification number for a Ward location				
WardLocationIEN	varchar(50)	Yes	Yes	No
VistA identifier for a Ward location	VistA File / Field 42 / IEN			

6.4.43 Table: WebLog

Table 47: WebLog

Element Name	Data Type	Indexed	Primary Key	Foreign Key
DFN	bigint	No	No	No
LookupSiteID	smallint	Yes	No	Yes

Element Name	Data Type	Indexed	Primary Key	Foreign Key
Message	varchar(4000)	No	No	No
NumiUserID	int	Yes	No	No
PatientSensitivity	tinyint	No	No	No
RemoteAddress	varchar(50)	No	No	No
RequestPage	varchar(100)	No	No	No
WebLogID	bigint	Yes	Yes	No

6.5 SQL Jobs

6.5.1 Table: SQLJobs

Table 48: SQLJobs

Job Name	Schedule
LogSyncDB_ValidateSynchronizer	Every hour
Counts number of Raw Stays synced within the past three hours and emails a warning to a predefined list of administrators if count equals zero.	
NUMI_PhysicianAdvisorPatientReview_AutoExpire	Every day at 12:00AM (Server Time)
Updates and auto-expires PUMA reviews older than 14 days.	
NUMI_usp_DaylightSavingsSite	Five different times one morning every spring
Runs the NUMI stored procedure usp_DaylightSavingsSite. Updates the offset field in the NUMI Site table for the change from standard time to daylight savings time.	
NUMI_usp_StandardTimeSite	One time one morning every fall
Runs the NUMI stored procedure usp_StandardTimeSite. Updates the offset field in the NUMI Site table for the change from daylight savings time to standard time.	

6.6 Report Database

NUMI can be configured to use a replicated database to produce reports. This enables a database load to be split off for report generation from the operational NUMI database to a report database.

6.6.1 Report Database Configuration

The report database connection information is configured in the NumiWebApp.config file. The information is contained in the application setting key “reportDbConnectionString”. The default setting is the NUMI operational database. To change to a replicated database, enter the replicated database connection information in the application setting key.

7 Exported Groups and/or Options and Menus

7.1 Exported Groups and/or Options

Not applicable.

7.2 Menus

NUMI provides menus which are accessible to users on the major UI screens. Those menus provide access to various features of the NUMI application. This section describes the menus and their underlying functionality.

7.2.1 Admin Menu

The Admin Menu is only available to NUMI site administrator users. Non-administrator users will not see this menu option on the UI. If administrator users have problems using this menu or its features, administrator users should validate that their profile indicates they have the appropriate access privileges.

Users option - This feature is used to find VistA users, add/edit NUMI user information, assign user privileges, and deactivate user sites.

Admin Sites option - This feature is used to find VistA users, and add or remove users from the Physician Advisor Reviewer, Primary Reviewer, Site Administrators, and Report Access lists.

Treating Specialty Configuration option- This feature allows Administrators to modify the current configuration of dismissal behaviors on Facility Treating Specialties. Administrators can change the Dismissal Behavior for Treating Specialties with or without a Dismissal Behavior configured, as well as configure a Treating Specialty that has no Dismissal Behavior."

7.2.2 Tools Menu

The Tools Menu is accessible to all NUMI users. However, the accessibility of certain options is based on individual access privileges.

Patient Selection/Worklist option - This feature is available to all users and lets them work with the Patient Selection screen, where they can select stays to perform primary reviews.

Utilization Management Review Listing option - This feature lets users work with the Patient Reviews screen, where they can see reviews that have either been saved for later, or saved/locked to the database. All users can Unlock and Copy reviews, and they can Delete their own reviews. Administrator users can Unlock, Copy and Delete any reviews.

Dismissed Patient Stays option - This feature is available to all users and lets them work with the Dismissed Patient Stays screen, where they can see patient stay reminders that have been dismissed.

Free Text Search option - This feature is available to all users and lets them search for patients using exact words, similar words, partial words or specific words. They can also filter by Date, Reviewer,

Ward, Service and Treating Specialty, Movement Type and Patient.

Physician Advisor Review option - This feature is available to Physician Advisor users and lets them work with their Worklist. From this screen, they can access and work on the reviews that have been assigned to them.

Manual VistA Synchronization – This feature is available to all users and lets them synchronize stay information between VistA and NUMI. A feed containing admissions and ward transfer information is passed to NUMI from VistA once every hour (at the top of the hour) during the daytime, and again at midnight. With this feature, users do not need to wait for the next feed. They can retrieve and synchronize information on demand. This feature comes in handy when they know a patient has been admitted to the hospital and is in VistA, but they do not see them in NUMI yet.

Patient Stay Administration option – This feature is available to NUMI Administrator users. Patient stays that are in NUMI, but that NUMI can no longer find in VistA, are marked invalid in the system and will show up on the Patient Stay Administration screen. NUMI Administrators will use this feature to verify the status of the stay in VistA and delete patient stays in NUMI that are no longer in VistA, or that NUMI incorrectly marked invalid due to VistA connection problems. This situation may exist because an invalid patient admission was entered and the record was deleted from the hospital database – but not before it was sent to NUMI. Here is some background information about how this process works:

Patient movements are entered into VistA and then synchronized into the NUMI database. Every time a stay is touched in NUMI, NUMI goes back to VistA to update the stay record with any changes in VistA. If nothing is returned from VistA when the record is requested, then NUMI marks its record of the stay as Invalid, and removes it from the patient selection list. It is put in a limbo state, but not deleted. NUMI Administrators can then review the invalid stays using this screen. Selecting them from the table will cause NUMI to again try to retrieve them from VistA. If it cannot, the Administrator can delete the patient stay from NUMI. If NUMI can retrieve the stay, then the Administrator has the option of selecting the Restore button to reactivate the stay.

Log out from NUMI option—This feature is available to all users and will redirect them to the Logout screen. From this screen, users can choose to log back in or log out from the SSO.

7.2.3 Help Menu

Online help for NUMI functionality consists of a Help Menu option on the major NUMI screens. The only option under this menu is User Guide. Selecting the option redirects users to the main Office of Quality, Safety and Value (OQSV) web page, where they will have hyperlinked access to view the latest version of the NUMI User Guide.

Help for CERME topics is available on the CERME screen in NUMI. Users will have access to a help dropdown containing help topics related to Change Healthcare CERME.

8 Security Keys and/or Roles

There are no VistA security keys or secondary menu options, and there are not any roles in NUMI. There are, however, six sets of activities which control a number of things, giving the appearance that there are roles. The activity sets are:

- ACCESS_ADMIN_TOOLS (add/remove users, add/remove permissions, and unlock and delete reviews)
- CREATE_AND_CONDUCT_PRIMARY_REVIEW
- CONDUCT_PHYSICIAN_ADVISOR_REVIEW
- REPORT_ACCESS
- FEE_BASED_CREATE_AND_CONDUCT_PRIMARY_REVIEW
- FEE_BASED_REPORT_ACCESS

8.1 VistA Rights needed for NUMI users

UM Reviewers will need to use Computerized Patient Record System (CPRS) to look up patient information while they work in NUMI, and will minimally need CPRS access. NUMI users must have the option *CPRSChart version n.n.n.n* (*OR CPRS GUI CHART*) on their menus.

It is also highly recommended that the VIAB WEB SERVICES OPTION be added to the System Command Options [XUCOMMAND] menu in each site's VistA system. If you do not add this to the Common Menu, you will need to add it to the secondary menu of each individual NUMI user.

8.2 General Information

The NUMI application is only accessible to authorized users. A User first needs to authenticate with the VA Identity and Access Management (IAM) before accessing the NUMI Login page. To authenticate with IAM, the user should select their VA Personal Identity Verification (PIV) card certificate and enter their PIV Personal Identification Number (PIN). NUMI also supports Secure Token Service (STS) integration with IAM. On successful authentication, the user will be directed to the appropriate landing page. If STS login fails, then users will need to work with their administrator to verify their account is set up correctly or submit a ticket for support.

The Tier 3 Development Team will initially grant access to the system by manually adding the user to the NUMI database. Once NUMI is in production, the process of adding/editing NUMI users and assigning privileges will be performed at the facility level by designated NUMI Site Administrators.

Through online administration screens, Site Administrators can add and edit NUMI user information, and designate access privileges after verifying the existence of a valid VistA account. They can also deactivate one or more of a user's Sites (while there is no way to actually delete users, deactivating all of their Sites will essentially remove their NUMI access), and add or delete users from available lists.

NUMI has five designated 'roles' for users:

- Primary Reviewer
- Physician Advisor Reviewer

- Report Access
- Site Administrator
- Super Users

All authorized NUMI users have access to NUMI Enhanced Reports SharePoint site: https://vaww.rtp.portal.va.gov/OQSV/10A4B/NUMI/enhanced/SitePages/Home.aspx

This section provides a detailed description of the auditing functionality that is available in and performed by the NUMI software. As is required by Health Insurance Portability and Accountability Act (HIPAA), in order to reduce healthcare fraud and abuse and guarantee security and privacy of patient data, the NUMI system includes functionality which keeps track of all activity related to a patient's record.

8.2.1 Audit and Accountability Policy and Procedures

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Control Implementation: VA has identified this control as an agency-wide common control provided VA-wide by Office of Cyber Security (OCS).

8.2.2 Auditable Events

Control: The information system generates audit records for the following events.

Control Implementation: The information system generates audit records for the following events: userid, date and time of event, actions of system administrators and operators, production of printed output, new objects and deletion of objects in user address space, security relevant events (logging into and out of the NUMI application), system configuration activities and events, events relating to use of privileges, all events relating to user identification and authentication, and the setting of userid' s.

The NUMI application will provide the means to create an audit trail of pertinent security and data related changes. It will log the following "events" on a user-by-user basis:

- All modifications to the NUMI database (insert, update, delete)
- Logging into and out of the NUMI application
- Database purges

8.2.3 Content of Audit Records

Control: The information system produces audit records that contain sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.

Control Implementation: The NUMI application audit records capture sufficient information to

establish what events occurred (identified by type, location, or subject), the sources of the events, and the outcomes of the events. A custom audit logger will be configured to save audit records to the database for reporting purposes. Information sent will include:

- User name
- Type of event
- Date and time of the event
- Other event-specific information

8.2.4 Audit Storage Capacity

Control: The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Control Implementation: The NUMI application allocates sufficient audit record storage capacity and establishes configuration settings to prevent such capacity from being exceeded.

8.2.5 Response to Audit Processing Failures

Control: The information system alerts appropriate organizational officials in the event of an audit processing failure, and take appropriate actions.

Control Implementation: In the event of an audit failure or audit storage capacity being reached, the NUMI application shall alert appropriate VA officials and takes the following additional actions: The system will notify the System Administrator and Information Security Officer by e-mail when approaching capacity and overwrite old audit records when full; it will provide a warning when allocated audit record equals or is greater than 85 percentage of maximum audit record storage: the space allocated allows for at least 1 week of data capture after the warning is generated. Currently the only auditing of events within the system boundary is at the O/S level.

8.2.6 Audit Monitoring, Analysis and Reporting

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials and takes necessary actions.

Continuous Monitoring Guidance: VA has identified this technical control for continuous monitoring activities at moderate and high impact levels. The production support team will be monitoring this control on some periodic basis by re-running the Security Control Assessment tests for AU-6 and documenting those activities, results, and any Plan of Actions and Milestones (POA&Ms) that may result within Security Management and Reporting Tool (SMART) Federal Information Security Management Act (FISMA).

Control Implementation: The Corporate Data Center Operations (CDCO) Security Team regularly review and analyze audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate NUMI project and CDCO officials. The system employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

8.2.7 Audit Reduction and Report Generation

Control: The information system provides an audit reduction and report generation capability.

Control Implementation: The NUMI application provides the capability to automatically process audit records for events of interest based upon selectable, event criteria. Currently the only auditing of events within the system boundary is at the O/S level.

8.2.8 Time Stamps

Control: The information system provides time stamps for use in audit record generation.

Control Implementation: VA has identified this control as a facility common control provided VA-wide by CDCO. All CDCO servers are synchronized to an external time server creating accurate time stamps for audit record generation.

8.2.9 Protection of Audit Information

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Control Implementation: The NUMI application protects audit information and audit tools from unauthorized access, modification, and deletion. Audit records are stored on a NUMI database.

8.2.10 Audit Record Retention

Control: The organization retains audit records for to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Control Implementation: The CDCO Security Team retains the NUMI application audit records for a minimum of one year or as documented in the National Archives and Records Administration retention periods, HIPAA legislation, VHA, or whichever is greater to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

8.3 Security - Authentication and Authorization

This section describes the Authentication and Authorization processes employed by the NUMI software.

8.3.1 Identification and Authentication Policy and Procedures

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Control Implementation: VA has identified this control as an agency-wide common control provided VA-wide by OCS.

8.3.2 User Identification and Authentication

Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Continuous Monitoring Guidance: VA has identified this technical control for continuous monitoring activities at all impact levels. The NUMI project team will be monitoring this control on some periodic basis by re-running the Security Control Assessment tests for IA-2 and documenting those activities, results, and any POA&Ms that may result within SMART FISMA.

Control Implementation: The NUMI application uniquely identifies and authenticates users (or processes acting on behalf of users). Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. The Control Enhancement requires multifactor authentication for remote system access that is National Institute of Standards and Technology defined level 3 or 4.

Currently the NUMI application System meets the Level 2 definition providing single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information.

8.3.3 Device Identification and Authentication

Control: The information system identifies and authenticates specific devices before establishing a connection.

Control Implementation: The NUMI application identifies and authenticates specific devices utilizing VA authentication solutions to identify and authenticate devices on local and wide area networks. The application uses shared known information such as Transmission Control Protocol/Internet Protocol addresses to authenticate authorized devices.

8.3.4 Identifier Management

Control: The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after of inactivity; and (vi) archiving user identifiers.

Control Implementation: The organization manages user identifiers by uniquely identifying each user verifying the identity of each user. Users sign on to the NUMI application using a SAML token obtained from Security Token Service using the IAM SiteMinder token, which grants them access to the appropriate VistA resources to run the NUMI application.

8.3.5 Authenticator Management

Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.

Control Implementation: The NUMI application manages information system authenticators through established procedures. NUMI utilizes SSO via IAM, granting them access specific content in the application. IAM manages two-factor authentication (2FA) and lost/compromised passwords, resetting passwords, revoking passwords and maintenance of system authenticators.

8.3.6 Authenticator Feedback

Control: The information system provides feedback to a user during an attempted authentication that feedback does not compromise the authentication mechanism.

Control Implementation: The NUMI application provides appropriate feedback to users during attempted authentication that does not compromise the authentication mechanism. This includes displaying asterisks when a user types a password, so it is not compromised.

8.3.7 Cryptographic Module Authentication

Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Control Implementation: VA Enterprise has not implemented cryptographic mechanisms in HL7 or VHA Health Information Model message transmission at this time.

8.4 Security – Access Control

This section describes Access Control security relevant to the NUMI system.

8.4.1 Physical and Environmental Protection Policy & Procedure

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Control Implementation: VA has identified this control as an agency-wide common control provided VA-wide by OCS.

8.4.2 Physical Access Authorizations

Control: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials.

Designated officials within the organization review and approve the access list and authorization credentials.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO. The CDCO develops and keeps current lists of personnel with authorized access to the facility as well as to information systems (except those areas officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the CDCO review and approve the access list and authorization credentials at least annually.

8.4.3 Physical Access Control

Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO. The CDCO controls all physical access points (including designated entry and exit points) to facilities containing information systems and verifies individual access authorizations before granting access to the facility. The CDCO also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the CDCO's assessment of risk.

8.4.4 Access Control for Transmission Medium

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO. VA does not require, at this time, application of control PE-4 for Moderate impact applications.

8.4.5 Access Control for Display Medium

Control: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO. The CDCO controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output. CDCO is not a public access facility thus reducing the likelihood of unauthorized individuals observing displayed information. In addition, access to the CDCO computer room, Security Services office space, and contracting office space is further limited by badge-controlled access for authorized individuals only.

8.4.6 Monitoring Physical Access

Control: The organization monitors physical access to the information system to detect and respond to physical security incidents.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO.

8.4.7 Visitor Control

Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO. The CDCO controls physical access to information systems by authenticating visitors before authorizing access to the facility or areas other than those designated as publicly accessible.

8.4.8 Access Records

Control: The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records after closeout.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO.

8.5 Mail Groups, Alerts and Bulletins

Mail Groups and Bulletins are Not Applicable. The NUMI software utilizes none of these.

There is only one alert that is created by the software. The Synchronizer Service will send off an email alert if zero Raw Stays have been imported in the past three hours.

8.6 Security - Contingency Planning

This section describes contingency planning that is associated with the NUMI system.

8.6.1 Contingency Planning Policy and Procedures

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Control Implementation: VA has identified this control as an agency-wide common control provided VA-wide by OCS.

8.6.2 Contingency Plan

Control: The organization develops and implements a Contingency Plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the Contingency Plan and distribute copies of the plan to key contingency personnel.

Control Implementation: The NUMI project is dependent on the production site to develop, maintain, and test their Contingency Plan which encompasses the NUMI application within their physical boundaries. The Contingency Plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the Contingency Plan and distribute copies of the plan to key contingency personnel. The NUMI System Owner or designated officials verify annually the Contingency Plan's maintenance and testing to verify the NUMI application requirements are met.

8.6.3 Contingency Training

Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training.

Control Enhancements: (1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations. (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

Control Implementation: VA has identified this control as a wide common control provided VA-wide by OCS.

8.6.4 Contingency Plan Testing and Exercises

Control: The organization: (i) tests and/or exercises the Contingency Plan for the information system using to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the Contingency Plan test/exercise results and initiates corrective actions.

Continuous Monitoring Guidance: VA has identified this technical control for continuous monitoring activities at MODERATE and HIGH impact levels. This will be done by monitoring this control on some periodic basis by re-running the Security Control Assessment tests for CP-4 and documenting those activities, results, and any POA&Ms that may result within SMART FISMA.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO.

8.6.5 Contingency Plan Update

Control: The organization reviews the Contingency Plan for the information system and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Control Implementation: The NUMI application is dependent on the CDCO to develop, maintain, and test their Contingency Plan which encompasses the NUMI application within their physical boundaries. The NUMI System Owner or designated officials verify annually the CDCO Contingency Plan's maintenance and testing to verify NUMI application requirements are met.

The project team will revise the plan to address the system or organizational changes or problems encountered during plan implementation, execution, or testing, as required.

8.6.6 Alternate Storage Site

Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information. The frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO. The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards. (2) The organization configures the alternate storage site to facilitate timely and effective recovery operations. (3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

The Continuity of Operations Planning (COOP) identifies the designated CDCO off-site storage facility, as well as the critical platform specific components necessary for recovery operations that will be stored at the site.

The off-site storage facility is geographically separated from the primary storage site so as not to be susceptible to the same hazards, and is configured to facilitate timely and effective recovery operations. CDCO also uses several offsite storage approaches ranging from the warm sites with replicated storage, offsite tape storage and an offsite subscription worksite recovery center.

The NUMI project team will identify an alternate storage site and initiate necessary agreements to permit the storage of information system backup information. The alternate storage site must be geographically separated from the primary storage site so as not to be susceptible to the same hazards. This facility is configured to facilitate timely and effective recovery operations. Any potential vulnerabilities of the alternate storage site will also be identified in the event of an area-wide disruption or disaster.

8.6.7 Alternate Processing Site

Control: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within when the primary processing capabilities are unavailable.

Control Enhancements: Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives:

1. The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards

2. The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions

3. The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

4. The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability.

Control Implementation: VA has identified this control as an agency-wide common control provided VA-wide by CDCO.

The CDCO COOP plans identify the designated CDCO alternate processing sites, necessary agreements to permit the resumption of information system operations for critical mission and business are established with each site, and critical equipment is pre-positioned at the site.

1. CDCO's service level agreements call for a base level of 99% system availability. This availability is bounded by the demarcation point for the VA Wide Area Network and excludes periods of scheduled maintenance and information systems not included within CDCO's accredited Local Area Network.
2. Systems are classified for recovery around three basic Recovery Time Objectives (RTOs) and two Recovery Point Objectives (RPOs). The RTOs supported are 12 hours, 72 hours,

and 30 days. The RPOs supported are 2 hours data loss and last back up.

Data is protected in normal operations through mirroring and periodic tape backup stored off site. In the case of essential support and mission critical systems, a second mirror of the data is maintained at the designated recovery site for the system. These procedures are covered in the Contingency Plans for the applicable platforms and applications. For systems the customer or the CDCO (for infrastructure) have designated as mission critical, the RTO of 12 hours is supported by underpinning contracts for maintenance services and software support that allow incidents to be resolved within the 12-hour window.

8.6.8 Telecommunications Services

Control: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within when the primary telecommunications capabilities are unavailable.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO.

8.6.9 Information System Backup

Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system and protects backup information at the storage location.

Continuous Monitoring: VA has identified this technical control for continuous monitoring activities at all impact levels. This control will be monitored by re-running the Security Control Assessment tests for CM-9 and documenting those activities, results, and any POA&Ms that may result within SMART FISMA.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO.

The CDCO performs full system backups, which are conducted once weekly. Applications and O/S are backed up on a need-to-be basis. Backups of sensitive, critical, and valuable information are stored in an environmentally protected and access-controlled site at least five miles from the site where the original copies reside. Backup tapes are verified at least once per quarter and whenever the COOP is tested.

8.6.10 Information System Recovery and Reconstitution

Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

Control Implementation: VA has identified this control as a facility common control provided at the facility level by CDCO. The COOP addresses recovery procedures in the event of a partial or full scale business disruption event. The plan includes recovery objectives that may be used to gauge the effectiveness of the recovery operations.

8.7 File Security

Not applicable. There are no VA FileMan files associated with the NUMI software.

9 Java Components (Client-Sided Java Components)

Not applicable. There is no software being loaded to user workstations for NUMI.

10 Set-up and Configuration

The NUMI server configuration installed at the primary production site includes:

- 1 Load Balancer
- 2 NUMI Exchange Web Servers
- 2 NUMI/CERMe Web application Servers
- 1 Database server for NUMI and CERME
- 1 Replicated database server for reporting
- 1 SSRS web hosting server for reporting

The load balancer manages the distribution of user requests between the two available web application servers.

The Web Servers are installed with NUMI Exchange web services. These servers use a 64-bit O/S. NUMI Exchange provides interoperability between NUMI and other VA systems and applications.

The Web Application Servers are installed with NUMI and CERMe. These servers use a 64-bit O/S, which is supported by Change Healthcare Corporation. NUMI interacts with CERMe to obtain InterQual® criteria, used to ensure the patients are receiving the appropriate level of care.

The Database Server is installed and configured with the NUMI and CERMe databases. These servers use a 64-bit O/S.

Installation of the application requires that certain files, tools and utilities are present on the servers. The Tier 3 Development Team also utilizes various tools and supporting technologies in the development of the application.

10.1 Deployment Package

The NUMI web application is deployed to the NUMI web server. During the application installation, various configuration files must be modified to support the user environments and connectivity. The NUMI deployment package is provided by the Tier 3 Development Team.

11 Troubleshooting

This chapter provides information about troubleshooting possible NUMI application errors. The NUMI database contains a table called InfoLog that can be used as a starting point for diagnosing the various system errors that may occur in the NUMI application. When configured in the NumiWebApp.config file, errors will be logged to this database table including (but not limited to) error message, the class and method where the error occurred in code, and the date/time the error occurred. In addition to errors, long running VDIF transactions will also be logged to the InfoLog table. Also, configurable in the NumiWebApp.config file is a VDIF timeout threshold value. VDIF transactions that take longer to complete than this value will be recorded in the InfoLog table.

11.1 High Level NUMI Exceptions

Table 49 lists some high level exceptions that would require troubleshooting.

Table 49: High level NUMI exceptions

Exception Description
Unable to login
Unable to access/view NUMI information
Application Timeout
Application Lockout
Login delays
Network connect problems
Unable to modify reviews
Unable to find reviews
Patient information not displaying
Unable to see information for multiple sites
Unable to select criteria checkboxes on the CERMe screen
Screen resolution/display problems

11.2 Error Components and their Meaning

Table 50 describes some messages that may display to users on the NUMI front end. Regarding back end messages, all NUMI-specific messages visible to end users or support are passed to the UI for troubleshooting and support. Additionally, the infrastructure (e.g., IIS; MS SQLServer; the Windows O/S; other network components) may report additional information. Documentation for those particular subsystems must be consulted for more details.

Table 50: Front End Messages

GUI Message or Symptom	High Level Corrective Action	NUMI Action
'Please select a VISN'.	User did not select a VISN on the Select VISN, then Site screen.	Instruct user to select a VISN from the VISN dropdown.
'Please select your hospital site'.	User did not select a Site on the Select VISN, then Site screen.	Instruct user to select a Site from the Site dropdown.
User cannot login.	VistA backups are running.	VistA backups run Monday-Friday at 1:30a.m. Instruct user to try logging in again at a later time.
User cannot see NUMI information.	User's browser does not allow pop- ups.	Instruct user to change their browser settings to accept pop- ups.
'This site might require the following ActiveX control…'	User's browser does not allow ActiveX controls.	Instruct user to change their browser settings to accept ActiveX controls by selecting 'Install ActiveX Control' from the ActiveX dropdown.
User cannot access NUMI.	User is not using EDGE browser	Instruct user to install current EDGE browser and try logging in again.
"You must select a patient"	User searched by patient name on Patient Selection/Worklist screen but did not click on a patient name in the result set.	Instruct the user to reinitiate their search and click on a patient name when the results display.
"Stay <stay number> for patient <patient name> cannot be retrieved from VistA and may be invalid. Please choose a different stay".	The user selected a stay from the Patient Selection/Worklist screen that is in NUMI but no longer in VistA.	One possible reason for this warning may be that an invalid patient admission was entered and the record was deleted from the hospital database, but not before it was sent to NUMI. Instruct the user to select a different stay.
User is involuntarily logged out.	Application timeout occurs after the user has been idle for 20 minutes.	Instruct user to try logging in again. See Section 0 for more details about timeouts).
User cannot login to NUMI.	User exceeded the maximum number of permitted login attempts. [This number varies by VistA and is based on the local VistA policy].	VistA will lock the user's Access and Verify Codes for 20 minutes. After 20 minutes, VistA will automatically reset the Access and Verify Codes and the user can try to login again. (See Section 4.4 for more details about lockouts).
User cannot login to NUMI.	VistA locked the user out of the application for exceeding the maximum number of login attempts.	If VistA has locked the user out, they will not be able to try logging in again for 20 minutes, at which time VistA will automatically unlock the Access/Verify Codes.
User cannot access NUMI.	User's PC is not connected to the network.	Check the user's PC connection to the network. Contact VA Helpdesk if you need further assistance.
User cannot access NUMI.	A power outage may have occurred at the primary or secondary production sites.	Check with appropriate support staff at the primary and secondary production sites and if a power outage has occurred, request estimate of power restoration. Advise users.
User cannot access NUMI.	A problem with an application, database or web server may have occurred.	Check with appropriate support staff to determine if there are problems with the application, database or web servers. If there are server problems, request estimate of system restoration. Advise users

GUI Message or Symptom	High Level Corrective Action	NUMI Action
User is unable to update a Review.	The review has been finalized and locked to the database.	If the user needs to modify the review, a NUMI Administrator will need to unlock the review.
User is unable to find a review.	Review has been deleted from NUMI.	If a review has been deleted it cannot be restored. Users with appropriate access rights should use caution when deleting reviews, for this reason.
User is unable to find a patient movement.	Patient movement has been dismissed.	Instruct user to select 'Dismissed Patient Select' option from the Tools menu. The review should display in the search results.
User is unable to find a review.	Review has been performed. Once a patient review has been performed, the patient's name will be removed from the Dismissed Patient Stays screen.	Instruct user that the review will display on the Patient Selection/Worklist screen 24 hours later (assuming the next day's date has been selected as the Next Review Date).
User is unable to find a review.	Review has been saved for later review.	Instruct user to select 'Utilization Management Review Listing' from the Tools menu. The review should display in the search results.
User cannot find a patient in NUMI.	Patient data is in VistA but is not showing up in NUMI.	There is an hourly feed of Admissions from VistA to NUMI, 24x7. Then the entire day will again be updated at midnight (per each time zone). User can either wait until the next feed, or they can use the synchronization feature under the Tools menu and manually synchronize NUMI with VistA.
User cannot find patient information in NUMI.	Patient data is not in VistA or patient has not been admitted.	Patient information needs to be added to VistA or patient needs to be admitted.
Patient name does not display in the Patient Movements List.	Patient record has been selected for review	Once patient record is selected for review their name will be removed from the Patient Movements List. The name will display again in 24-72 hours.
Patient name does not display in the Patient Movements List.	Next Review Reminder for the patient has been dismissed	If the Next Review Reminder has been dismissed for the patient, the record will not display in the Patient Movements List again unless it is selected for review from the Dismissed Patient Stays screen. Once the record is selected for review it will display in the Patient Movements List 24 hours later (provided the next day's date was identified as the Next Review Date).
User is unable to find a review.	Review has been saved for later review.	Instruct user to select the Utilization Management Review Listing option from the Tools menu. The review should display in the search results.
User cannot access one or more sites.	User does not have permission to visit different sites, or the sites they can visit have not been added to their profile.	A user's site administrator can grant them access rights to multiple sites by updating the user's profile from the Add User Permissions admin screen.

GUI Message or Symptom	High Level Corrective Action	NUMI Action
User with appropriate permissions' Security or Add-on settings are incorrect.	Security and Add-on settings are set up incorrectly.	Under Internet Options > Manage Add-ons, verify that the Toolbar add-ons are set to "Enable". Under Internet Options > Security > Internet > Custom Level, verify that Active Scripting is set to "Enable". Under Internet Options > Security > Local Intranet > Custom Level, verify that Active Scripting is set to "Enable". Under Internet Options > Security > Trusted Sites > Custom Level, verify that Active Scripting is set to "Enable". Under Internet Options > General, click the Delete Files button. Under Internet Options > General, click the Delete Cookies button.
NUMI screens do not display all information.	Screen cuts off information.	Incompatible screen resolution setting. Instruct user to set their screen resolution to 1024x768 or higher.
NUMI screen display is too large or too small.	Screen text/icon display too large or too small.	Incompatible screen resolution setting. Instruct user to set their screen resolution to 1024x768 or higher.
"Warning – Patient is Deceased"	The user has selected a patient who is deceased.	Instruct the user to click the 'Continue Primary Review' button, if they wish to continue working with the review.
"Warning – Sensitive Patient"	The user has selected a patient whose record contains sensitive information.	Instruct user to click the 'Continue Primary Review' button, to continue working. The user will need to prove they have a need to know. Access to this patient is tracked and their station Security Officer will contact them for their justification.
"Changing the subset for this review will erase all criteria point selections, criteria point notes and outcomes for this review. Do you want to change the subset for this review?"	The user has selected the 'Change Subset' button.	User can select 'Yes' option to change the subset or 'No' to cancel.
"Changing this choice will erase all criteria. Click Yes to change or No to keep the old value."	Changing Current Level of Care value on the CERMe screen will erase all criteria selections on the screen.	User can select 'Yes' option to change the Current Level of Care or 'No' to cancel.
"Admit to Inpatient / Observation"	Selection of certain criteria on the CERMe screen produces system message recommending admission.	User selects 'OK' button to continue working on the review.
"Admit to Inpatient / Observation and refer to Dual Diagnosis criteria subset for Concurrent review."	Selection of certain criteria on the CERMe screen produces system message recommending admission.	User selects 'OK' button to continue working on the review.

GUI Message or Symptom	High Level Corrective Action	NUMI Action
'Unsupported review type. Please use another CERME review'.	User has opened a review that is not supported in NUMI and then clicked the 'Continue Primary Review' button on the CERME screen. [A behavioral psych procedure is one example of when this message may display].	CERME supports the review but NUMI does not. A reason for this message may be that the user selected a Behavioral Health Procedure Review. Procedure Reviews are not supported in NUMI. Instruct user to select another review.
'You must select a patient'.	User has performed a search but did not select a patient name in the Patient Selection/Worklist screen result table.	Instruct must click on the name of the patient they wish to work within the result table.
'There are no more review steps'.	User clicked 'Next Step' button on the CERME screen.	This is a known Change Healthcare CERME message. It is not a NUMI system error that requires a help desk ticket. To bypass the message, instruct user to click 'OK', and then click the 'Continue Primary Review' button.
"This review will now lock into the NUMI database. Further changes require an administrator. Are you sure you are ready to lock this review?"	Selecting the FINAL SAVE/Lock to Database button locks the review and commits the information to the database.	If a user wishes to unlock a review, follow these guidelines when instructing them in how to do this: • Primary Reviewers can Unlock and Delete their own reviews. • NUMI site administrators can Unlock and Delete any reviews • NUMI site administrators can Unlock or Delete reviews on behalf of a Physician Advisor
"The Web page you are viewing is trying to close the window. Do you want to close this window?"	User initiates Logout action. System prompts for confirmation that user wants to logout of NUMI.	User selects 'Yes' to continue with Logout or 'No'. User can also click a 'here' hyperlink to login again.
No insurance information displays for the patient.	User has no insurance information on file.	No further action necessary.
"Please select a reason".	User did not select a Stay Reason while working on the Primary Review screen.	Instruct the user to select a Stay Reason.
"You do not have admin access to modify user privileges for: <user name>.	The user does not have administrative permissions for NUMI.	Instruct the user to contact the NUMI POC for their facility if they have a need to be able to perform administrative tasks on NUMI.
User unable to perform certain activities even though their privileges are correct.	A user's privileges were changed but they are still unable to perform certain activities on NUMI.	Changes to privileges will not take effect until the user logs out and back in. Instruct the user to do that and they should be able to access the features they need.

GUI Message or Symptom	High Level Corrective Action	NUMI Action
"Invalid URL Information entered ReviewManager.xml, URL tag. Check if URL points to the right Database or Check for URL syntax in CERME / Driver documentation. If using ODBC, check ODBC name as entered in Windows matches ReviewManager.xml entry. Userid/Password combination may not be correct. Error accessing /rm/iqm/html/gateway" OR…. "CERME has lost connection with the database server".	The user receives this message when trying to perform a review on the CERME screen in NUMI.	This error would occur when the CERME server loses connectivity with the database. The resolution is to submit a CA Technologies/Service Desk Manager (CA/SDM) help ticket so that someone in the support chain (e.g., Tier 3) can restart the CERME server service, or the application server (the actual hardware) can be rebooted by on-site support. **NOTE:** This problem is believed to be limited to a previous version of CERME and the newest version does not appear to be susceptible to the same problem.
User has questions / problems while working on the CERME screen.	Determine whether the question/problem relates to NUMI or CERME functionality. The only NUMI functionality on the screen is the tabs at the top of the CERME screen and the *Continue Primary Review* button. See the NUMI Action column for the appropriate next steps.	Instruct the user to either create a CA Technologies/ (CA/SDM) ticket, or call the VA SD and ask them to place one for them. The ticket will then go through the PS/PIMS team and be referred to Tier 3 support, if necessary, if the question/problem relates to NUMI functionality. If the question/problem relates to CERME functionality or the UM process or the application of the clinical criteria, advise the user to call or go to the Change Healthcare Customer Support Hub for assistance.

11.3 Common Executable Errors

Not Applicable. There are no common executable (.exe) messages in NUMI. The only messages generated are validation messages.

11.4 General Troubleshooting

11.4.1 CERMe

Problems related to CERMe functionality are to be reported to Change Healthcare Corporation for research and resolution.

11.4.2 Tier 2 and Tier 3 Support

For problems related to the NUMI application, please call your local NUMI site administrator. If the problem cannot be resolved by the site administrator, contact local IT support. If the issue can't be resolved locally, you may create a Service Now ticket in IT Service Management (ITSM) through the self-serve portal, or call the Enterprise Service Desk (ESD) at 888-596-4357. A ticket can be created at any time, but software support teams work during regular daytime business hours, and only tickets designated as emergencies will be addressed during off-hours. Below is the Service Now configuration for NUMI support:

CATEGORY: Affected Service

Affected Service: National Utilization Management Integration

GROUP: SPM.HEALTH.VFO

A member of the Tier 2 VistA Front Office group will respond to the ticket, and if it cannot be resolved at the Tier 2 level they will refer it to the Tier 3 support group.

11.4.3 After Hours Management

Figure 4: Architect Overview

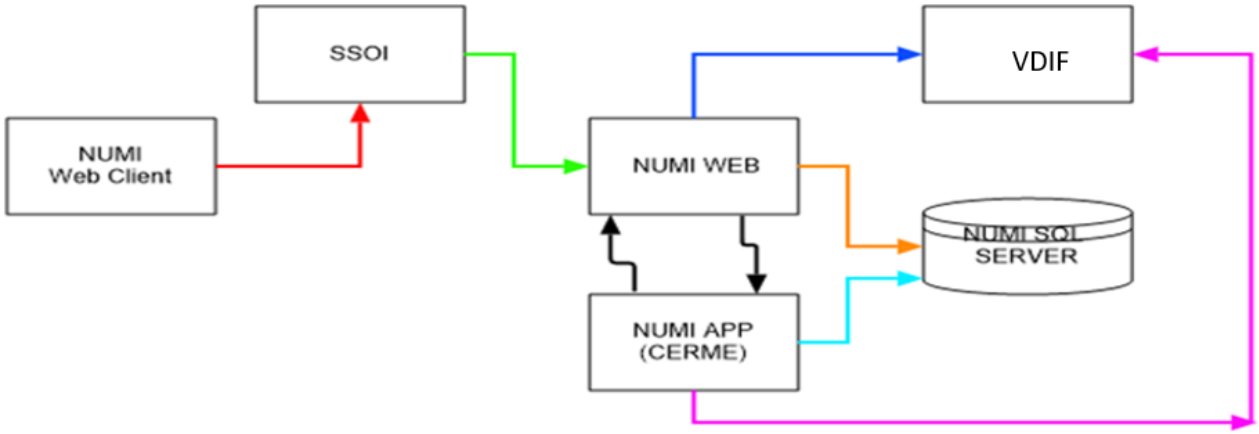

Table 51: After Hours Remediation

Symptom	High Level Corrective Action	NUMI Action
User cannot reach NUMI login screen.	Open ticket to address SSOI Assigned group: ACS Tier 3 Support	N/A
Reviews not opening in CERME	**Restart CERME service**	**Restart CERME service**

Intermittent unhandled exceptions while clicking on patients	Open ticket with VDIF	Check NUMI db info log table with this query:
		`select info, username, datecreated from infolog`
		`where datecreated > 'today'`
		`and info like '%closed%'`
		
		If the info field contains a similar error to:
		Error connecting to VDIF: The underlying connection was closed: An unexpected error occurred on a send.
		The underlying connection was closed: An unexpected error occurred on a receive.
		
		Use this a confirmation of the problem and open ticket with VDIF.

11.5 Interface Control Document (ICD) References for Messaging

Specifications

Not applicable. NUMI does not utilize Health Level 7 (HL7) messages or use any ICD references to them.

12 Appendix A– Acronyms and Terms

Table 52 contains descriptors for acronyms and terms used in this document.

Table 52: Acronyms and Terms

Acronym / Term	Descriptor
.NET Framework	A software component that is a part of MS Windows O/S. It has a large library of pre-coded solutions to common program requirements, and manages the execution of programs written specifically for the framework. The.NET Framework is a key MS offering, and is intended to be used by most new applications created for the Windows platform
Active X	A component object model developed by MS for Windows platforms. Software based on ActiveX technology is prevalent in the form of Internet Explorer plugins and, more commonly, in ActiveX controls, ActiveX based applications launched from web pages
ActiveX Control	A reusable component which implements the IUnknown interface. Such components do not amount to an entire application; rather they provide a small building-block that can be shared by different software. The fact that command buttons look the same in almost any program on a platform is an example of component reusability that is not just limited to ActiveX controls. ActiveX controls are very important prior to the computer's security and are normally used to setup passwords
Agile Iterative Development	A conceptual framework for software engineering that promotes development iterations throughout the life-cycle of the project. Software developed during one unit of time is referred to as an 'Iteration'. Each Iteration is an entire software project including planning, requirements analysis, design, coding, testing, and documentation
API	Application Programming Interface
ASP	Active Server Pages- MS's first server-side script engine for dynamically-generated web pages
ASP.NET	A web application framework marketed by MS that programmers can use to build dynamic web sites, web applications and web services. It is part of MS's .Net platform and is the successor to MS's ASP technology
C# (C 'Sharp')	An object-oriented programming language developed by MS as part of the .Net initiative
CDCO	Corporate Data Center Operations
CERMe	Care Enhance Review Management Enterprise
Component	An assembly, or part thereof, that is essential to the operation of some larger assembly and is an immediate subdivision of the assembly to which it belongs
COOP	Continuity of Operations Planning
COTS	Commercial Off The Shelf
CPRS	Computerized Patient Record System
DAL	Data Access Layer
DAO	Data Access Objects
ERM	Entity-Relationship Model
FISMA	Federal Information Security Management Act
GUI	Graphical User Interface
HIPPA	Health Insurance Portability and Accountability Act
HTTPS	Hyper Text Transfer Protocol Secured
IAM	Identity and Access Management—The authentication service that validates the logged in user through PIV or other mechanisms.

Acronym / Term	Descriptor
ICD	Interface Control Document
IIS	Internet Information Server
IRM	Information Resource Management
IEN	Internal Entry Number
Internet Information Server	A set of Internet-based services for servers using MS Windows. It is the world's second most popular web server in terms of overall websites, behind Apache HTTP Server
Interconnection Security Agreement	Federally mandated for any system, contractor or agency that touches the Federal network. This is a component of the Security Certification and Accreditation (C&A) process which is also Federally mandated
ISO	Information Security Officer
JavaScript	A scripting language most often used for client-side web development. JavaScript was influenced by many languages and was designed to have a similar look to Java, but be easier for non-programmers to work with. The language is best known for its use in websites (as client-side JavaScript), but is also used to enable scripting access to objects embedded in other applications
MDO	Medical Domain Objects
MDWS	Medical Domain Web Services. MDWS was the mechanism for importing VistA information into NUMI before VIA.
Medora UM	A class III Web-based application that interfaces with CERMe
Module	An interchangeable subassembly that constitutes part of a larger device or system
MSBuild	Development tool used for build scripts
National Utilization	A Web-based application that automates documentation of clinical features
Management Integration	relevant to each patient's condition and the associated clinical services provided as part of VHA's medical benefits pack
NUMI	National Utilization Management Integration
OCS	Office of Cyber Security
O/S	Operating System
OQSV	Office of Quality, Safety and Value
PIV	Personal Identity Verification
POA&Ms	Plan of Actions and Milestones
Production Environment	Used for live product operation. The build manager creates production builds for this environment and coordinates installation with the operations staff
	Quality, Safety and Value
RAID	Redundant Array of Inexpensive Disks
RPC	Remote Procedure Call- A client/server infrastructure that increases the interoperability, portability and flexibility of an application by allowing the application to be distributed over multiple platforms
RTC	Rational Jazz Team Server
RTO	Recovery Time Objectives
Runtime	Describes the operation of a computer program, the duration of its execution, from beginning to termination
SAN	Storage Area Network
SDM	Service Desk Manager
Secure Sockets Layer	Encrypts data so that no one who intercepts is able to read it Can assure a client that they are dealing with the real server they intended to connect to Can prevent any unauthorized clients from connecting to the server Prevents anyone from meddling with data going to or coming from the server

Acronym / Term	Descriptor
Security Requirements	Document support for the Certification and Accreditation (C&A) process relevant to the acceptance of the NUMI application as production-ready by the OCS
SLA	Service Level Agreement- A document describing the level of service and support that shall be provided to a system or application
SMART FISMA	Security Management and Reporting Tool FISMA.SMART FISMA is a database that monitors FISMA compliance.
SOAP	Simple Object Access Protocol. A protocol for exchanging XML-based messages over computer networks, normally using HTTP/HTTPS.SOAP forms the foundation layer of the web services protocol stack providing a basic messaging framework upon which abstract layers can be built
SQL	Structured Query Language
SSL	Secure Socket Layer
SSO	Single Sign On
SSRS	SQL Server Reports Server
Subversion	Development tool used for source control (including tagged releases)
Trac	An enhanced Wiki and issue tracking system for software development projects. Trac uses a minimalistic approach to web-based software project management
UI	User Interface
UM	Utilization Management-The process of evaluating and determining the coverage and the appropriateness of medical care services across the patient health care continuum to ensure the proper use of resources
Stay Synchronizer	A mechanism for getting information for a Stay in ADT's prior to the query date range
UML	Unified Modeling Language
Unified Modeling Language	An ISO specification language for modeling objects
URL	Uniform Resource Locator
User Interface	Specifies the features for user interface (specific page) models or paradigms
VB.NET (Visual Basic .NET)	An object-oriented computer language that can be viewed as an evolution of MS's Visual Basic (VB) implemented on the MS .Net Framework
VDIF	Veterans Data Integration and Federation
VDIF-EP	Veterans Data Integration and Federation Enterprise Platform
VHA	Veterans Health Administration
VIA	VistA Integration Adapter
VistA	Veterans Information Systems Technology Architecture
VISN	Veterans Integrated Service Network. References one of the many Veteran's Administration sites
VWS	VistA Web Services
VWS Services	Required to get patient and patient movement data from VistA and provide as Web service
Web Services	A software system designed to support interoperable Machine to Machine interaction over a network. The term refers to Clients and Servers that communicate using XML messages that follow the SOAP standard
Web Service Description Language	Web services programming language
Wiki	Software that allows users to create, edit, and link web pages easily
WSDL	Web Services Description Language

Acronym / Term	Descriptor
XML	Extensible Markup Language- A general-purpose markup language. Its primary purpose is to facilitate the sharing of structured data across different information systems, particularly via the Internet. Required to parse fields from Change Healthcare CERMe
XPath (XML Path Language)	A language for selecting nodes from an XML document. In addition, XPath may be used to compute values (strings, numbers, or boolean values) from the content of an XML document

13 Appendix B - Dependencies

This Appendix describes general dependencies associated with NUMI.

- The software for the VDIF is functional and operating
- The software for the IIS application servers is functional and operating
- The software for VistA is functional and operating
- The software for CERMe is functional and operating
- The Stay Synchronizer is functional and operating
- The SQL Server Database is functional and operating
- The primary production site is fully operational
- Computer center equipment, including components supporting the NUMI application is connected to an Uninterruptible Power Supply that provides electricity, even during a power failure
- The equipment, connections and capabilities required to operate the NUMI application are available and functional
- Backups of the application software and data are intact and available
- Service Level Agreements are in place and maintained to support the NUMI hardware, software, interfacing systems and communications providers

14 Appendix C – Interfacing

This Appendix describes interfaces that are associated with the NUMI software. (There are no external interface models or external design elements for NUMI). NUMI interfaces with a COTS product from Change Healthcare Corporation. Change Healthcare CERMe provides CERMe Review Text that is presented to users in Read-Only format.

The process for interfacing NUMI with Change Healthcare is:

- User performs review in the NUMI Web application
- User selects Save and an XML string is sent to CERMe
- The CERMe servlet launches
- User is allowed to enter additional data
- User chooses Save in the CERMe software
- The data is processed through the algorithm
- The results are sent back to NUMI as an XML string
- NUMI stores the CERMe results
- NUMI then needs a link back to a minimal record in CERMe The CERMe Interface provides:
- An Editor account that allows users to add/update reviews with the embedded CERMe

Interface
- A Read Only account that allows users to view the contents of a review performed in the CERMe Interface - but not to make changes

User account setup is determined by the user permissions, as determined by NUMI.

15 Appendix D – References and Official Policies

This Appendix identifies references and official policies relevant to the NUMI project.

- FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems"
- FIPS 201-1, "Personal Identity Verification of Federal Employees and Contractors"
- FIPS 140-2, "Security Requirements for Cryptographic Modules"
- CDCO Directive 7600, CDCO Handbook 7600.1
- VA Directive 6500.3, "Information Security Program"
- VA Directive and Handbook 0710, "Personnel Suitability and Security Program"
- VA Directive and Handbook 0730, "Security and Law Enforcement"
- VA Directive 6100, "Telecommunications"
- VA Directive and Handbook 6102, "Internet/Intranet Services"
- VA Directive 6502, "Privacy Program"
- NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook"
- NIST SP 800-18, Revision 1 "Guide for Developing System Security Plans"
- NIST SP 800-23, "Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products"
- NIST SP 800-26, "Security Self-Assessment Guide for Information Technology Systems"
- NIST SP 800-27, Rev A, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)"
- NIST SP 800-28, "Guidelines on Active Content and Mobile Code"
- NIST SP 800-30, "Risk Management Guide for Information Technology Systems"
- NIST SP 800-34, "Contingency Planning Guide for Information Technology Systems"
- NIST SP 800-35, "Guide to Information Technology Security Services"
- NIST SP 800-36, "Guide to Selecting Information Security Products"
- NIST SP 800-37, Draft, "Guide for the Security Certification and Accreditation of Federal Information Systems"
- NIST SP 800-40, "Procedures for Handling Security Patches"
- NIST SP 800-42, "Guideline on Network Security Testing"
- NIST SP 800-46, "Security for Telecommuting and Broadband Communications"
- NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems"
- NIST SP 800-48, "Wireless Network Security: 802.11, Bluetooth, and Handheld Devices"
- NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program"
- NIST SP 800-53, Revision 1 Final, "Recommended Security Controls for Federal Information Systems"
- NIST SP 800-53A, Draft, "Techniques and Procedures for Verifying the Effectiveness of

Security Controls in Federal Information Systems"
- NIST SP 800-56A, "Recommendation on Key Establishment Schemes"
- NIST SP 800-57, "Recommendation on Key Management"
- NIST SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories"
- NIST SP 800-61, "Computer Security Incident Handling Guide"
- NIST SP 800-63, "Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology"
- NIST SP 800-64, "Security Considerations in the Information System Development Life Cycle"
- NIST SP 800-65, "Integrating Security into the Capital Planning and Investment Control Process"
- NIST SP 800-66, "An Introductory Resource Guide for Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule"
- NIST SP 800-88, "Guidelines for Media Sanitization"

16 Appendix E – Section 508 Compliance

This Appendix describes the approach used by the NUMI team to ensure that the NUMI application is in compliance with 508 requirements to provide visually impaired users of Web pages with access equivalent to that of users of the UI. The paragraphs that are quoted in this appendix come from Electronic and Information Technology Accessibility Standards Final Rule (Federal Register 21 December 2000, 36 CFR Part 1194).

Paragraph (a)
"*A text equivalent for every non-text element shall be provided (e.g., via "alt" "longdesc" or in element content).*"

This requirement is met in NUMI mostly through the design of the framework used by individual pages. Alternate text was added to all graphical buttons, identifying the object, its state (e.g., whether disabled or not), and what it does, in a clear and concise manner. Images that serve as graphic elements or placeholders that do not convey any meaning do not need to be given alternate text. However, testing programs that look for Section 508 compliance may flag such images as problems when they are not.

Paragraph (b)
"*Equivalent alternative for any multimedia presentation shall be synchronized with the presentation.*" No multimedia presentations shall be used.

Paragraph (c)
"*Web pages shall be designed so that all information conveyed with color is also available without color, for example form context or markup.*"

The tabs at the top of each page and the buttons on each page convey information using the color they take on. For instance, the current tab may be highlighted in blue and a button that is disabled may appear gray.

In order to be compliant with this paragraph, text was added to explain the state of a button. In the

case of a tab, the alternate text for the tab would say, “Currently in the X section” or alternate text for a button might identify its state.

Paragraph (d)
“*Documents shall be organized so they are readable without requiring an associated style sheet.”*

Style sheets are used to display the text in a particular style, color and font size. This can present a problem if the style sheet does not allow the user to increase or decrease the font size. Using relative measurements allows the fonts to change based on the user’s preferences.

Paragraph (e) “*Redundant text links shall be provided for each active region of a server side image map*.”

Server side image maps shall not be used.

Paragraph (f)
“*Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shap*e.”

Client side image maps shall not be used.

Paragraph (g)
“*Row and column headers shall be identified for data tables.*”

The application uses tables for both page formatting and data presentation. For the tables that present data, row and column headers are clearly identified for screen reader accessibility.

Paragraph (h)
“*Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.*”

Text is provided to distinguish between data and header cell contents, and to associate content with the appropriate headers.

Paragraph (i)
“*Frames shall be titled with text that facilitates frame identification and navigation.*” Frames technology shall not be used.

Paragraph (j)
“*Pages shall be designed to avoid causing the screen to flicker with frequency greater than 2 Hz and lower than 55 Hz.*”

Screen flicker is kept to a minimum and falls within the accepted range.

Paragraph (k)
“*A text-only page, with equivalent information or functionality, shall be provided to make a Web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.*”

NUMI has been made compliant on all pages with the exception of the COTS product CERME, held within it's own iFrame. This is a Change Healthcare product and when the vendor implements accessibility options we will ensure they're provided to users of NUMI.

Paragraph (l)
"*When pages utilize scripting languages to display content, or to create interface elements the information provided by the script shall be identified with functional text that can be read by assistive technology.*"

The site uses scripting extensively for form validation and navigation. Most of this scripting does not write content to the browser and does not affect content. However, several issues remain: The margin text that runs in the left panel of the page uses a script to update the content of that area depending on what field the user's cursor is currently in. This updated information is not available to a user of an assistive technology. To address this problem, NUMI displays the margin text for the user in a dialog box if the user presses a keyboard shortcut.

Another issue associated with scripting and accessibility concerns the way buttons work. The user takes an action by clicking on a button, which in turn triggers a script to run and execute a particular action. If the user cannot use the mouse to click on the button, the action cannot take place. To address this problem, buttons are programmed to trigger actions if the user hits a key on the keyboard while focus is on a button.

Paragraph (m)
"*When a Web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with §1194.21(a) through (l).*"

The site does not require any applet or plug-in to display site content.

Paragraph (n)
"*When electronic forms are designed to be completed on-line, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all direction and cues.*"

All form fields identify their content to the screen reader. In addition, the forms are designed in such a way as to maximize usability in terms of direct access to information, field elements, and functionality (equivalent to that of the graphical view), including directions, context-sensitive help, etc.

Paragraph (o)
"*A method shall be provided that permits users to skip repetitive navigation links.*"

NUMI navigational links appear at the page top and bottom. To address this issue, links were added to the top of the page taking the user to the main areas within the page. One link goes to the main content. Another links to the navigational elements.

In addition to the accessibility links, the text only view of the site reorganizes the content of the page. Repetitive links and content fall to the bottom of the screen, while the main content of the page

remains near the top. Also keyboard shortcuts were added to make jumping between sections of the page easier.

Paragraph (p)
"*When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required."*

The site does not have a timed response per prompt. However, in compliance with security requirements, the site has a timeout so that if the user does not take an appropriate action in the form within a given amount of time the session is terminated. The site gives warnings that this is going to take place, which gives a user ample opportunity to take the appropriate action to keep the session from timing out. The users cannot change the time set for the timeout, as this is determined by VHA security policy. However, by acting on the timeout warnings, the user can extend/reset the 20-minute timeout period.

Assistive Technology

There are many products available to assist persons with disabilities, such as speech or refreshable Braille screen readers, programs that can enlarge portions of the screen, or hardware alternatives to keyboards and mice. It is beyond the scope of this document to reference all the different assistive technologies that are available and how NUMI would work with each. Below are the major categories of assistive devices and what shall be done in NUMI to support each.

Screen readers: Alternate text shall be given to all visual information, including graphical buttons and form controls.

Screen magnification and text enlargement: The graphical view shall be resizable to accommodate different screen sizes and resolutions.

Alternative input devices: All elements were designed to allow manipulation without the need for a pointing device. In addition keyboard shortcuts shall be provided to make navigation inside a page easier. Assuming the assistive technologies are following industry standards, NUMI shall work with assistive technologies.

Testing for 508 Compliance

Testing for compliance to 508 guidelines can be challenging, especially on a site as complex as NUMI. Often automated tools are used to make the job easier. For a standard website this would be a straightforward process; the tool would be run and it would list any possible compliance issues. Any issues found would then be verified by a manual test. Automated tools are often ineffective on sites with a high level of user interactivity. Because NUMI is an application that interacts with the user to such a high degree, automated tools are rendered incapable of properly testing the application. That is why testing of NUMI shall be carried out manually, using actual assistive technologies or some of the techniques described below.

The simplest test for accessibility shall be to attempt to use the application using only the keyboard. The tab key moves the highlight from one element to the next allowing elements to be activated or data to be input. A tester shall verify if buttons can be activated and if form fields can be manipulated using only the keyboard.

Another test to see if page elements would be readable to assistive technology shall be to see if all graphical elements are giving meaningful alternate text. To do this the tester can hover the pointer over the element (image) and see if a tool tip appears. They shall verify that the text of the tool tip describes what the element is or does.

Another way to test the site shall be to use a screen reader to try to navigate and use the site. The tester shall verify that the information and auditory cues that are being conveyed by the screen reader provide sufficient information for the user to know what to do on any given page in the site.

17 Appendix F – NUMI Development Tools

This Appendix addresses tools used for the development of NUMI. C# / .ASP.NET

This language was chosen for development of NUMI by the Tier 3 development team, who did the initial field development.

MS Internet Information Server (IIS)

IIS is the application server that is required to publish .NET applications. IIS v.7.5 is being used for NUMI development and will be used for NUMI production.

MS.NET Framework 2.0

MS.NET is a software technology that is available with the MS operation system. It includes a library of pre-coded solutions to common programming problems and a virtual machine that manages the execution of programs written for this framework, and is used by a wide variety of Windows applications. The MS .NET framework and MS C# are being used in the development of the NUMI application. The NUMI GUI is being developed as ASPs, accessible to authorized users. The middle tier interacts with the VDIF web services. The patient review information is stored in the NUMI database tools that are used to support the integration.

Log4Net

Apache Log4Net is a tool to help the programmer output log statements to a variety of output targets. It is the .NET version of Java's Log4J. Log4Net is a part of the Log4J framework to the .NET runtime. The framework has remained similar to the original Log4J, while taking advantage of new features in the .NET runtime.

Log4Net is used in NUMI to log programming error codes and system messages. Logging in the first release is not expected to be read by anyone other than the developers. More robust auditing is targeted for the next major release. In the meantime, in addition to various text log files, NUMI has a separate database that has tables to capture each synchronization event for each site, and a table that captures records that cannot be captured in the NUMI database due to bad data or other anomalies.

Rational Jazz Team Server

Rational Jazz Team Server (RTC) is the source version control system which is used to maintain current and historical versions of files such as source code, web pages, and documentation. RTC is used for the NUMI source code control.

Change Healthcare CERME

CERMe is the COTS product that has been integrated into NUMI to calculate utilization and runs on a Jetty web server.

Visual Studio

This is the Integrated Development Environment (IDE) used to develop and test the NUMI application. Visual Studio is used to develop console and GUI applications along with Windows Forms applications, web sites, web applications, and web services in both native codes together with managed code for all platforms supported by .NET Framework.

18 Appendix G– NUMI Workflow Example

Figure 5 and Figure 6 describe an example NUMI workflow from a UM user's perspective.

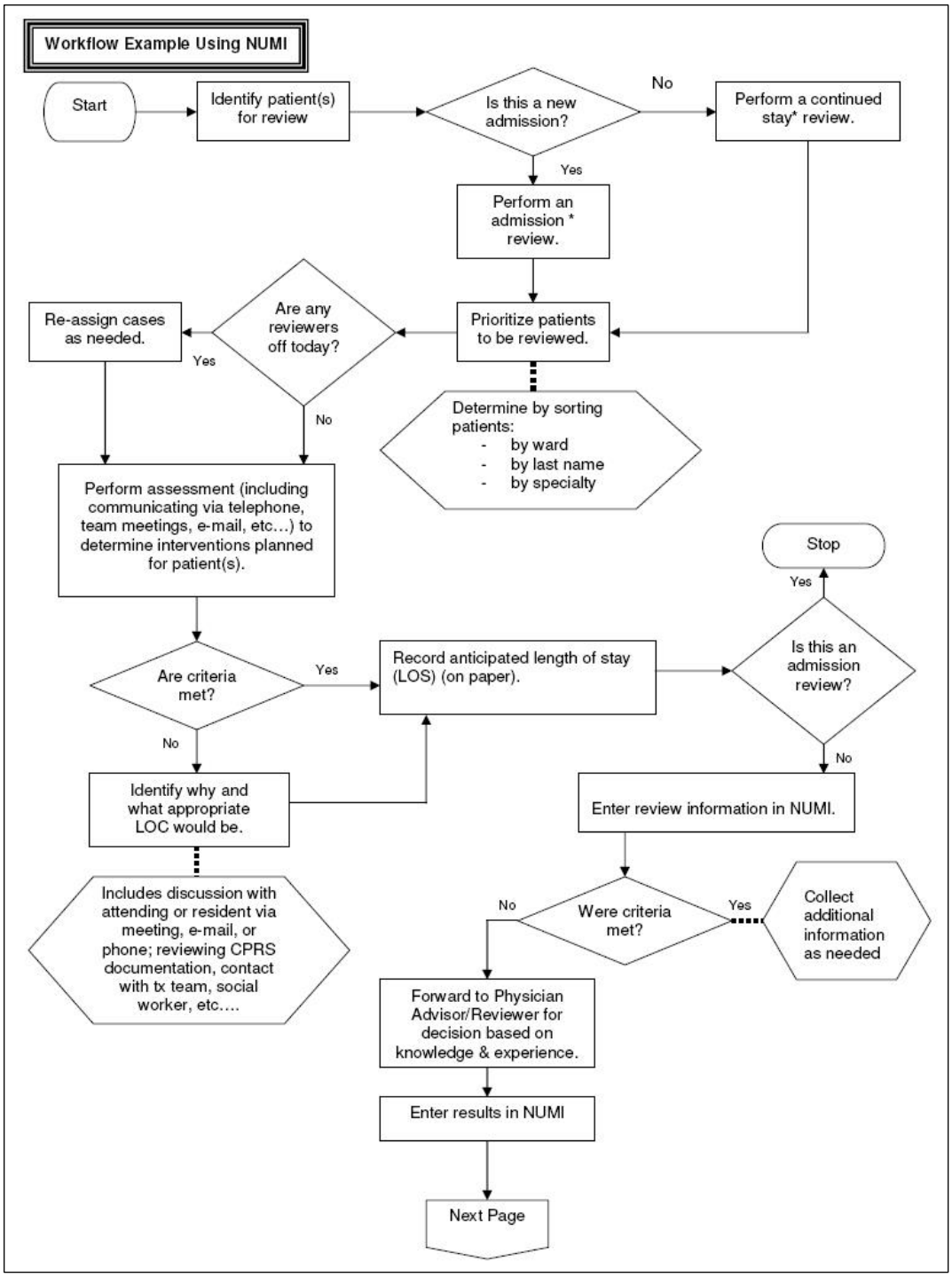

Figure 5: NUMI Workflow Example (part 1)

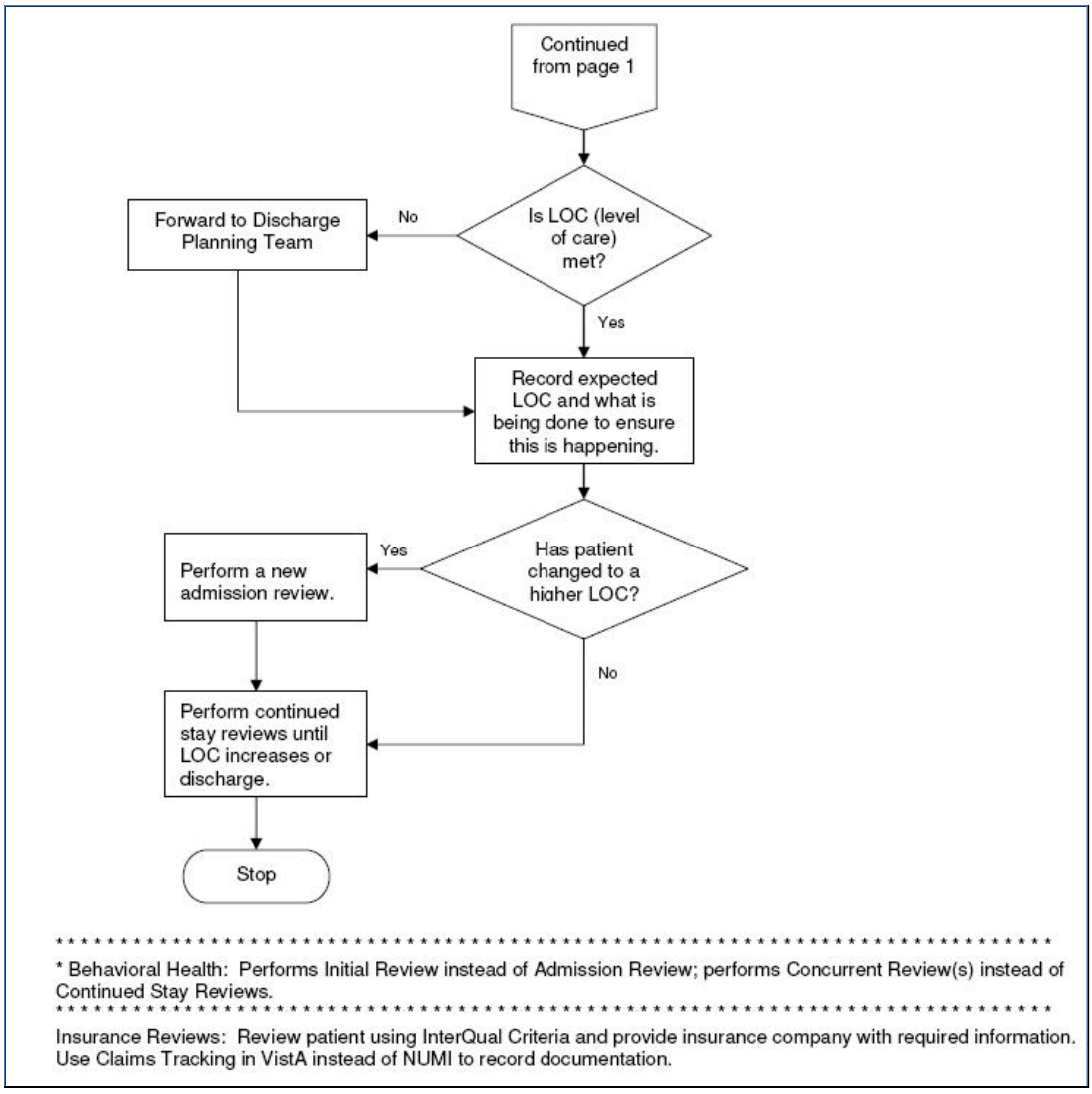

Figure 6: NUMI Workflow Example (part 2)

19 Appendix H – Free Text Search Criteria

Certain database tables/columns are checked when a user performs a Free Text search in NUMI.

Table 53 lists tables and columns checked during search from UM Review Listing and Free Text Search pages:

Table 53: Free Text Search from UM Review Listing and Free Text Pages

Table	Column
FacilityTreatingSpecialty	FacilityTreatingSpecialtyDesc
MASMovementTransactionType	MASMovementTransactionTypeDesc
NumiUser	VISTAName
Physician	PhysicianName
WardLocation	WardLocationDesc
Patient	PatientName

Table	Column
Patient	SSN
PatientReview	Comments
PatientReview	Custom
PatientStay	AdmissionDiagnosis

NUMI Free Text Search Functionality

Full-text queries perform linguistic searches against text data in full-text indexes by operating on words and phrases based on rules of a particular language. Full-text queries include simple words and phrases or multiple forms of a word or phrase from database. Users can perform a Free Text search in NUMI in 4 different ways:

Search by '*Exact*' word

In full-text search: A word is considered to be a token. A token is identified by appropriate word breakers, following the linguistic rules of the specified language. A valid phrase can consist of multiple words, with or without punctuation between them.

Search by '*Similar*' word

(Thesaurus): A thesaurus defines user-specified synonyms for terms. For example, if an entry, "{car, automobile, truck, van}", is added to a thesaurus, you can search for the thesaurus form of the word "car". All rows in the table queried that include the words "automobile", "truck", "van", or "car", appear in the result set because each of these words belong to the synonym expansion set containing the word "car".

Search by '*Partial*' word

(Part Of): A prefix term refers to a string that is affixed to the front of a word to produce a derivative word or an inflected form.

For a single prefix term, any word starting with the specified term will be part of the result set. For example, the term "auto" matches "automatic", "automobile" and so forth.

For a phrase, each word within the phrase is considered to be a prefix term. For example, the term "auto tran*" matches "automatic transmission" and "automobile transducer", but it does not match "automatic motor transmission".

Search by '*Specific*' word

(Inflectional): The inflectional forms are the different tenses of a verb or the singular and plural forms of a noun. For example, search for the inflectional form of the word "drive". If various rows in the table include the words "drive", "drives", "drove", "driving" and "driven", all would be in the result set because each of these can be inflectionally generated from the word drive.

20 Appendix I– NUMI Database Servers

NUMI database servers are all on Virtual Machines The servers all use Dynamic Host Configuration Protocol. Instead of connecting to them via Internet Protocol addresses, they must be connected to via their Domain Name System names instead. Users who have an account in the Administrators group can access these servers.