Distributed Query Tool

Overview and Administrators Guide

Powered by Pop**Med**Net[TM]

Based on release 3.2

June 2013

Contents

Document History

The following table is a revision history for this document.

Table 1: Document History

Version	Author(s)	Date	Description
3.1	Lincoln Peak Partners	11/15/2012	Created.
3.2	Jeff Brown, Elizabeth Balaconis, Megan Mazza, Melanie Davies	5/13/2013	New Build. This new documentation represents a new release of the PMN software. Prior Mini-Sentinel query tool documentation was based on release 2.3.24 and this documentation is based on PMN 3.2.0. New features include User Registration, Plug-in Architecture, Security Group Access Control, and Projects.

1 Overview and Background

The **PopMedNet™** system enables simple, efficient creation and use of distributed data networks, through a set of tools and web-based services. It is optimized to facilitate distributed analyses of medical product safety, comparative effectiveness, quality, medical resource utilization, cost-effectiveness, and related studies. The system provides secure, customized, private portals, query tools, and file transfer capabilities. It supports both menu driven queries and distributed analyses using complex, single use or multi-use programs designed to execute against a local data resource.

Data partners exercise full control over the files they make available for querying, the results returned to requestors, and the individuals who are permitted to submit queries. The PopMedNet™ software can accommodate a wide scope of network sizes and complexity, ranging from of single datasets held by only two organizations through multi-year projects encompassing dozens of organizations and dozens of data resources.

This document describes the overall system architecture, and details the technical and security approaches implemented. Individual networks may adopt different implementations.

Note: This document uses screen shots from the reference implementation of the PopMedNet™ system.

Networks powered by PopMedNet™ software can customize and brand the network as desired. The Department of Population Medicine at the Harvard Pilgrim Health Care Institute (HPHCI) led development of the system in collaboration with Lincoln Peak Partners (LPP). Lincoln Peak Partners provides support services and secure hosting for current system users, and leads development of system enhancements.

This document describes PopMedNet Release 3.1, a major upgrade to the previous version 2 release. Release 3.1 includes a redesigned and enhanced security system as well as a "plug-in" framework for queries and the data models that support them. This approach provides a more secure, extensible, and scalable system for integration of request models implemented in both native and foreign technologies.

2   System Overview

The PopMedNet™ application (PMN) is comprised of two separate components, the Portal website and the DataMart Client. The **Portal** (there is one Portal per Network) is the starting point for all information requests and controls all system communications, security, and governance policies. Data partners receive queries, process them, and securely return them to the Portal via their local **DataMart**[*] **Client**. There is exactly one Portal in the network and each network data partner can have one or more DataMarts. All query requests and communications within the network are securely routed from the Portal to the DataMarts Client and then back to the Portal. The reference material provides additional details on the querying process.

To participate in a network, data partners must:

1. Install and configure the DataMart Client on one or more local computers or servers
2. Assign one or more staff members as the DataMart Administrator(s) responsible for interacting with the system (via the DataMart Client and the Portal) on behalf of the data partner
3. Create data in a standard format and make it available for querying.
4. Set DataMart preferences to establish settings, such as what data can be queried and who can submit queries to the DataMart

The DataMart Administrator or other staff members do not need any special information technology or computer expertise to install the software, manage the DataMart, or respond to distributed queries.

2.1   The DataMart Client

The DataMart Client application allows the DataMart Administrator to view queries distributed to the DataMart, execute queries locally, review the results, and upload the results to the portal. The DataMart Client is a .NET/C# Windows desktop application developed by LPP that is installed locally on an Administrator's desktop. All communications between the DataMart Client application and the Portal use HTTP/SSL/TLS connections to securely transfer queries and results between the application and the Portal. The application uses ODBC and other database client connections, as well as web services, to access local databases used to process queries and generate results.   The actual data connection is based on the type of request and its corresponding data model.

The following sections provide an overview of responding to a query using the DataMart Client application; however see the *PopMedNet DataMart™ Administrator Manual* for a detailed presentation of configuring and using the DataMart Client (DMC) application

2.2   The Portal

---

[*] The term "DataMart" is used in an information technology context referring to the place where the data are held for querying. Use of this term does not imply that data partner information is being sold or being made broadly available; data partners maintain control of all their data and all its uses.

The PopMedNet™ network portal is a dedicated secure website which manages all network interactions with the data partners. The portal is based on a Microsoft .Net technology stack using ASP.NET MVC 3 for the web site framework, C# as the programming language, and Managed Extension Framework (MEF) to implement request model plug-ins, Entity Framework (EF 4.2) to support the data model and SQL Server (2008 R2) for persistence.

For investigators, the portal handles user settings (e.g., contact information, passwords, and email notification settings), the composition and routing of requests to data partners, and the management of results. For DataMart Administrators, the portal enables creation and enforcement of permission settings (i.e., who can submit requests and what they can submit), establishment of new DataMarts, email notification settings, and audit reporting.

The following sections provide an overview of composing a request, submitting to DataMarts, monitoring its status, and viewing the results; however see the *PopMedNet™ Investigator's Manual* for a detailed presentation of composing and submitting requests within PopMedNet.

Note: The term "Request" is used interchangeably with "Query". With the introduction of PopMedNet Release 3, the application has the ability to compose and route a variety of queries, commands, and general *requests* to DataMarts through a "plug-in" framework that allows the network to be easily extended to introduce new requests types.

2.3   Request Model Plug-ins

PopMedNet™ Release 3.1 introduced a new plug-in framework for extending the number and type of requests that may be supported by the network. The plug-in framework abstracts the concept of a query into a more general **Request** that is submitted to one or more DataMarts that execute the request and return a **Response**. Requests contain a header that is common to all requests and zero, one, or more **Documents** that comprise the request. Responses have a header that is common to all responses, and zero, one, or more Documents that comprise the response. A Document is a binary stream that is marked with a mime-type containing data, such as a table of patient counts serialized into a data stream, text file, html file, or virtually any type of office document such as a Word document, Excel Worksheet, image file, or even a program file.

There are several types of plug-ins that may be integrated into PopMedNet™ as follows:

- ✓ Native Plug-ins – tightly integrated ASP.NET MVC 3 components that implement the native plug-in interfaces
- ✓ Remote Plug-ins – loosely integrated external websites that provide query composers, developed in virtually any technology, that can compose queries outside of the PopMedNet portal and route them to PopMedNet networks via a secure web service gateway
- ✓ Redirect Plug-ins – loosely integrated external websites that provide query composers in developed in virtually any technology where queries are initiated within PopMedNet™ and use a HTTP redirect bridge to switch between PopMedNet and the foreign application.

NOTE: See Lincoln Peak for information on how to develop plug-ins for PopMedNet.

The following sections provide an overview of the existing *native* Request Model Plug-ins that have been developed for PopMedNet.
Supported Query Types (Requests)
The system currently supports a number of queries types:

- ✓ Summary Queries - Menu-driven queries that execute against summary tables
- ✓ ESP Queries - Menu-driven queries that execute against ESP databases
- ✓ File Distribution Queries – Requests used to exchange documents between the portal and DataMarts
- ✓ SQL Distribution Queries – Requests used to distribute raw SQL code between the portal and DataMarts
- ✓ Remote Query Composers - Queries composed from a number of external applications, such as I2B2 and hQuery, that use an interface native the application to compose the query and submit it to a PopMedNet network

2.4   Menu-Driven Queries

Menu-driven queries are created by users using a standardized query builder interface integrated into the portal and distributed to data partners. These requests may be routed to DataMarts and executed against standardized data repositories created and maintained by the data partners.   The user interface for menu-driven requests consist of a set of controls including text edit controls, check boxes, drop-down lists, and selection lists that allow the user to compose the query from pre-defined settings displayed in the controls.

2.4.1   Summary Queries

PopMedNet™ software currently supports querying against Summary Tables. The structure of the currently supported tables is described in *PopMedNet Summary Table Description* document available on the Resource page of the Portal. Briefly, these tables provide summary counts of individuals by period, age group, and sex. The summary counts include information on medication use (e.g., number of dispensings, users, and days supplied), diagnoses (e.g., number of individuals with the diagnosis), procedures, and the overall data partner population.

The summary queries are grouped into four request models as follows:

Table 2: Summary Queries

Model	Request Type
Incidence	ICD-9 Diagnosis (3 digit codes)
	Pharmacy Dispensings by Drug Class
	Pharmacy Dispensings by Generic Name
Prevalence	ICD-9 Diagnosis (3 digit codes)
	ICD-9 Diagnosis (4 digit codes)
	ICD-9 Diagnosis (5 digit codes)
	ICD-9 Procedures (3 digit codes)

Model	Request Type
	ICD-9 Procedures (4 digit codes)
	Enrollment
	HCPHCS Procedures
	Pharmacy Dispensings by Drug Class
	Pharmacy Dispensings by Generic Name
	Dispensings by National Drug Code
Most Frequently Used	HCPCS Procedures
	ICD-9 Diagnosis (3 digit codes)
	ICD-9 Diagnosis (4 digit codes)
	ICD-9 Diagnosis (5 digit codes)
	ICD-9 Procedures (3 digit codes)
	ICD-9 Procedures (4 digit codes)
	Pharmacy Dispensings by Drug Class
	Pharmacy Dispensings by Generic Name
Administrative	Refresh Dates

2.4.2 ESP Queries

The ESP Queries consist of two query types, an ICD-9 Diagnosis query and a Reportable Disease query, that use a menu-driven user interface to query the ESP database. Electronic Support for Public Health System (ESP) uses a standardized data model and a set of complex algorithms to identify selected diseases of public health concern such as acute hepatitis B, Lyme disease, influenza-like illness, and diabetes. The ESP algorithms are based on the ESP data model that is a standardize representation of EHR-based encounter and patient demographic information. The ESP application is installed behind the provider's firewall, giving the provider control over access and use of their data. The ESP queries are grouped into the following request model:

Table 3: ESP Queries

Model	Request Type
ESP Query Builder	ICD-9 Diagnosis
	Reportable Disease

2.4.3 File Distribution Query

A File Distribution Query allows users to securely distribute electronic files to data partners. Although any type of file can be distributed, a common use is expected to be the distribution of SAS and SQL programs and work plans to data partners who will download and execute the programs and then securely upload results based on institutional policies. The File Distribution query is grouped into the following request model:

Table 4: File Distribution Query

Model	Request Type
File Distribution	File Distribution

2.4.4   SQL Distribution Query

A SQL Distribution Query allows users to securely distribute SQL code to data partners. This allows investigators to write SQL code and distribute it to data partners who are willing and able to accept and run SQL queries. Data partners run the query as they normally would any other menu driven query via the DataMart Client application. The SQL Distribution Query is grouped into the following request model:

Table 5: SQL Distribution Query

Model	Request Type
SQL Distribution	SQL Distribution

2.5   Network Workflow

Figure 1 illustrates the flow of requests and information within the network. The workflow can be divided into activities undertaken by the requestor and those that are the responsibility of the data partner. Each is described below.

1- Query created and submitted by authorized user on the secure network portal
2- Data partners notified of query and retrieve it from the secure network portal
3- Data partners review and run query against their local data
4- Data partners review results
5- Data partners securely return results to the secure network portal for review by requestor
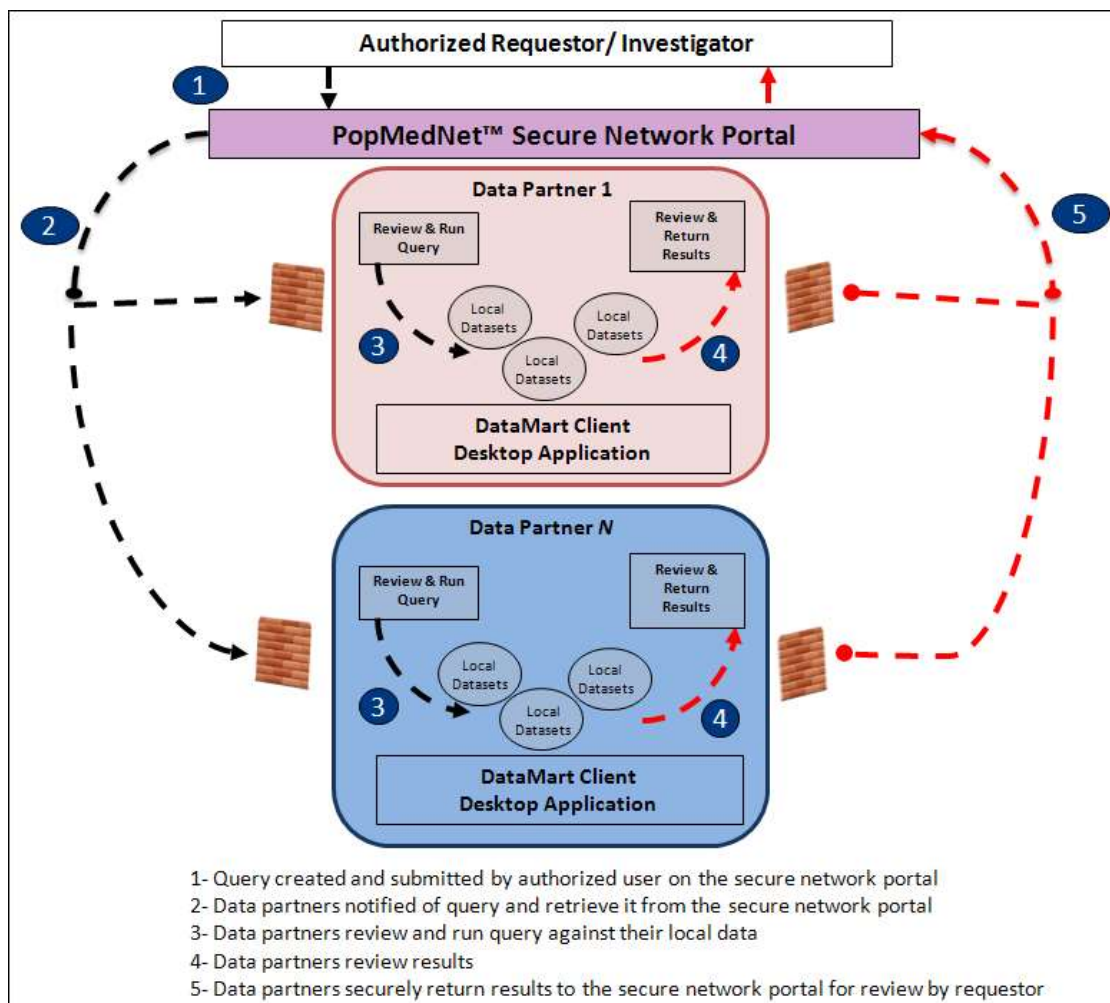
Figure 1: Network Workflow

2.6   Project Based Requests

One of the major enhancements in PMN R3.2 is the introduction of Projects. Projects allow networks to group activities within one or more Projects. A project establishes security policies for composing and executing requests for users and DataMarts assigned to the project. Projects are created within an organizational Group. Groups have one or more member organizations whose users and DataMarts may participate within projects owned by the group. Note that the network may have one or more groups, and an organization may be a member of one or more groups. Users may be a member of one or more projects. Note that with the introduction of Projects, all requests are submitted within the context of a project. See section 5.20 for a discussion on creating and configuring Projects.

2.7   Composing and Submitting a Query (requestor actions)

Submitting a query through the network requires several steps. A brief description of these steps is listed in the following sections. See the **PopMedNet™ Distributed Query Tool Investigators Manual** for details on composing and routing requests.

2.7.1   Logging into the Portal

Each PopMedNet user is provided a set of credentials consisting of a username and password that represents the user's account. The user must enter the credentials into a logon page, confirm the terms and conditions of the site, and then click Login to authenticate the user against an instance of a PopMedNet site.

Figure 2: Logon Page

Logging into the portal establishes a security context that determines the features the user is allowed to access and actions the user is allowed to perform. The features and actions allowed by a user are managed by a list of Access Control rights (ACL). Network Administrators assign these rights to the user's PopMedNet account directly or indirectly by adding the user as a member of a one or more **Security Groups**. Security Groups are collections of users, and other security groups, that are assigned ACLs. Membership in a security group causes the user's account to inherit all the rights associated with the group. Users may be members of zero, one, or more security groups. For example, the query types that may be composed by the user and the DataMarts where they may be routed for execution depends on the rights assigned to the user's account or the security groups for which the user is a member. Security groups provide a convenient and powerful method to build and manage roles with in PopMedNet that can easily be assigned to new and existing users.

2.7.2 Using the Portal Landing Page

Once authenticated, the user is transitioned to the **Home page**.

PopMedNet — Distributed Research Network Technologies for Population Medicine — Welcome, bwan

Home | Requests | Profile | Resources | Reports | Network — Contact Us | Logoff

What's New

Software Version 3.2.0 Features and Enhancements

- PopMedNet 3.2 Feature Enhancements:
  - Projects - Project based request processing and administration
- PopMedNet 3.1 Feature Enhancements:
  - User Workspaces - Built-in folders that allow requests to be automatically organized into sub-folders
  - Shared Folders - Allows users to share requests with other users.
  - Network Navigator - Visual tools network browser that allows the user to navigate through the network hierarchy.
  - Bread-crumb Navigation Control - Control the maintains position within the network hierarchy providing context and allowing the user to easily back up through the hierarchy
  - Sticky User Settings - Remembers users settings, such as collapsible controls, the number of requests shown on the request page will be remember from session to session.
  - Auto DataMart Configuration - this will make it easier for datamart administrators to configure their datamart client. This feature streamlines the datamart client configuration process as it can be done from the portal.
  - User Registration - Allows users to register for an account by entering contact information, username, and password in addition to the traditional user creation process performed by Administrators.
  - User registration Workflow Process - User registration requests enter a task based workflow process used by Administrators to approve or reject user registrations via a new Task panel displayed on the home page.
- PopMedNet 3.0 ONC Query Health Enhancements:
  - Query Envelope - Formalization of the PMN request tunnel to comply with ONC Query Health requirements
  - Enhanced Security - Implementation of mutual authentication over TLS using X.509 certificates
  - I2B2 Request Plugin - Integration of I2B2 request composer that submits request to the PMN network that are routed to I2B2 end-points used to process the request
- MDPHnet Feature Enhancements:
  - Menu-driven query builder request plugin used to compose ICD-9 Diagnosis requests and Reportable Disease Requests submitted against ESP databases.
- PopMedNet 3.0 Design and Technical enhancements:
  - New Request Model Plug-in architecture allowing the application to be easily extended to accommodate new request types and data models.
  - Upgraded technology platform that includes Microsoft .NET 4, Entity Framework 4, MVC 3, WCF, and MEF under Visual Studio 2010 solution.
  - Consolidation of all request and response data into documents that may be displayed using built-in viewer or downloaded to for use by custom applications.
  - Redesigned/rewritten DataMart Client application that uses a simplified threading model to process requests.
  - Use of the Windows Credential Manager to store local DataMart Client credentials.

Notifications

Date	Event	Message
3/13/2013 4:25:13 PM	My Profile Updated	Profile of user 'OPS\bswan' has been updated by OPS\bswan
3/13/2013 4:24:45 PM	My Profile Updated	Profile of user 'OPS\bswan' has been updated by OPS\bswan
3/13/2013 4:24:26 PM	Project Change	Project Change: Project = 2ecbb084-8f2f-4111-af1b-0d94a305fa5b, ActingUser = OPS\bswan, CrudEventKind = changed
3/13/2013 4:22:28 PM	Registration Submitted	User 'OPS\msullivan' submitted a registration
3/13/2013 11:51:40 AM	New Request Submitted	New request of type 'MFU: HCPCS Procedures' has been submitted by OPS\bswan
3/13/2013 11:44:54 AM	Project Change	Project Change: Project = 2ecbb084-8f2f-4111-af1b-0d94a305fa5b, ActingUser = OPS\bswan, CrudEventKind = changed
3/13/2013 11:33:59 AM	Project Change	Project Change: Project = 2ecbb084-8f2f-4111-af1b-0d94a305fa5b, ActingUser = OPS\bswan, CrudEventKind = changed
3/12/2013 4:41:08 PM	New Request Submitted	New request of type 'MFU: HCPCS Procedures' has been submitted by OPS\bswan
3/11/2013 4:41:16 PM	New Request Submitted	New request of type 'MFU: HCPCS Procedures' has been submitted by OPS\bswan
3/11/2013 11:51:21 AM	New Request Submitted	New request of type 'Prev Metadata: Refresh Dates' has been submitted by KPCO\KPCODataMartAdministrator

Page: 1 2 3 4 — Showing 10 notifications per page

Tasks

Name	id	Date	User	Status	Type
Mike Sullivan	16	03/13/2013 04:22 PM	msullivan	Awaiting Approval	Registration

Showing 20 tasks per page

Requests

Version 3.2.0 | Terms and Conditions | Info — © 2013 PopMedNet, All Rights Reserved. — LINCOLNPEAK

Figure 3: Home Page

The home page is a landing page that contains a set of controls that provide the user with information that is relevant to his daily tasks. The following controls are available on the home page:

- ✓ What's New   - A message panel used to communicate site information, upgrades, and new features
- ✓ Notifications – A list of recent notifications on requests and responses performed or associated with the user
- ✓ Requests – A list of recent requests that have been initiated by the user or require the user's approval or review

Collapsible content panels are used throughout the user interface that allows the user to collapse, expand, and maximize a content area within the page. Additionally, for panels that contain grid controls, the user may specify the number of items displayed in the grid, set column sort orders, and column filters. All these settings are preserved across user sessions.

2.7.3   Creating a New Request

The user creates a new request by clicking the "New" button in the Requests content panel.

⊟ Requests						⊡
▲ Name	Id	Date ▼	User	Status ▼	Type ▼	Project
File Distribution - 1	32	03/13/2013 09:52 AM	bswan	Draft	File Distribution	Mini-Sentinel
ICD-9 Diagnosis - 0	33	03/13/2013 11:34 AM	bswan	Draft	ICD-9 Diagnosis	Mini-Sentinel
Incl: ICD-9 Diagnoses (3 digit codes) - 2	7	03/07/2013 01:06 PM	bswan	Completed	Incl: ICD-9 Diagnose	Mini-Sentinel
Incl: ICD-9 Diagnoses (3 digit codes) - 4	24	03/11/2013 10:49 AM	bswan	Completed	Incl: ICD-9 Diagnose	Mini-Sentinel
MFU: HCPCS Procedures - 0	11	03/07/2013 01:08 PM	bswan	3/4 completed	MFU: HCPCS Proced	Mini-Sentinel
MFU: HCPCS Procedures - 1	13	03/07/2013 04:39 PM	bswan	Scheduled	MFU: HCPCS Proced	Mini-Sentinel
MFU: HCPCS Procedures - 1 (Daily 1)	14	03/07/2013 04:16 PM	bswan	3/4 completed	MFU: HCPCS Proced	Mini-Sentinel
MFU: HCPCS Procedures - 1 (Daily 2)	15	03/07/2013 04:41 PM	bswan	3/4 completed	MFU: HCPCS Proced	Mini-Sentinel
MFU: HCPCS Procedures - 1 (Daily 3)	21	03/08/2013 04:41 PM	bswan	3/4 completed	MFU: HCPCS Proced	Mini-Sentinel
MFU: HCPCS Procedures - 1 (Daily 4)	22	03/09/2013 04:41 PM	bswan	3/4 completed	MFU: HCPCS Proced	Mini-Sentinel
Page: 1 2 3 Showing 10 requests per page						New

Figure 4: Requests Panel

2.7.4   Selecting a Request Model

The new request action displays a popup dialog containing the lists of Request Models available to the user based the user's access rights. Queries are grouped together in request models which are contained in request model plug-ins.
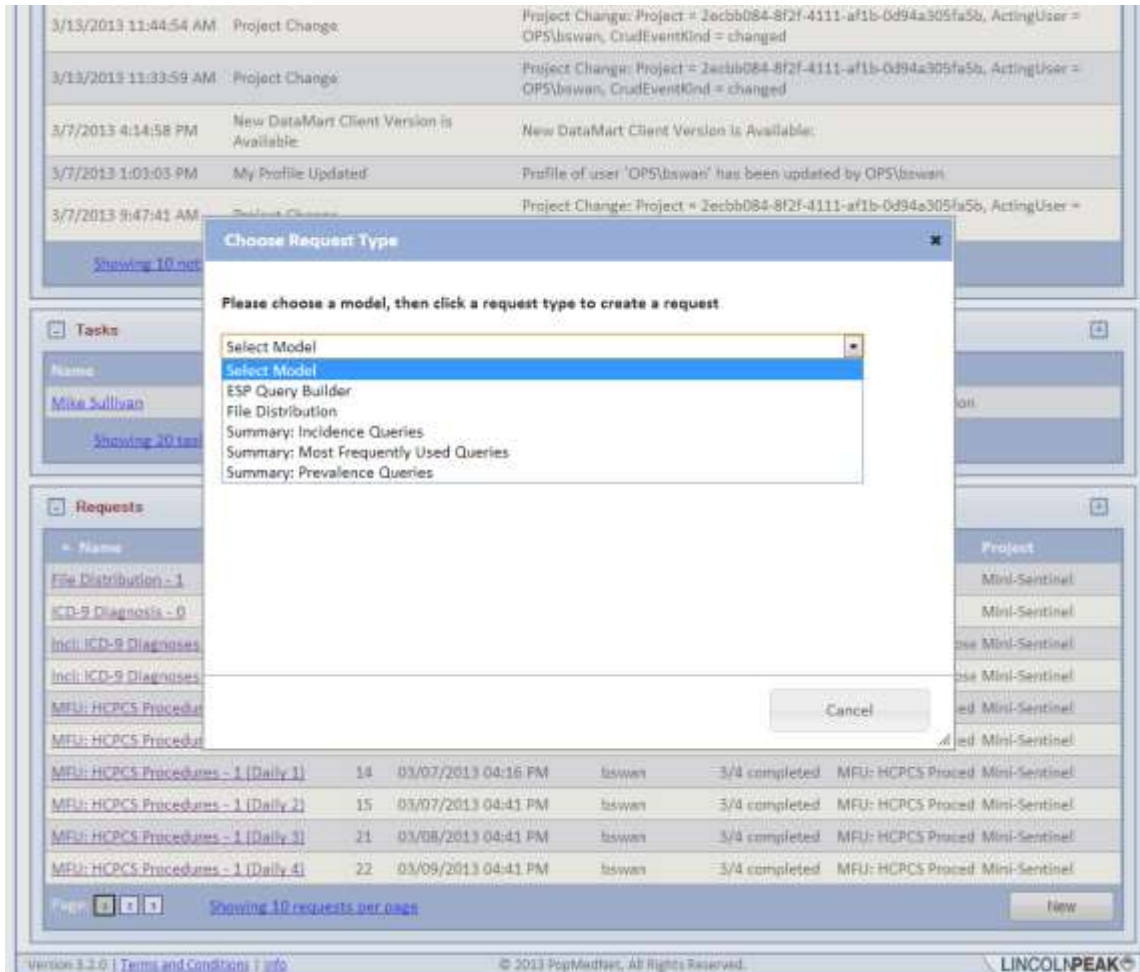
Figure 5: New Request Dialog

2.7.5 Selecting a Request Type

Once the request model has been chosen, the request types for that model are displayed. A draft request is created once the user chooses a request type.
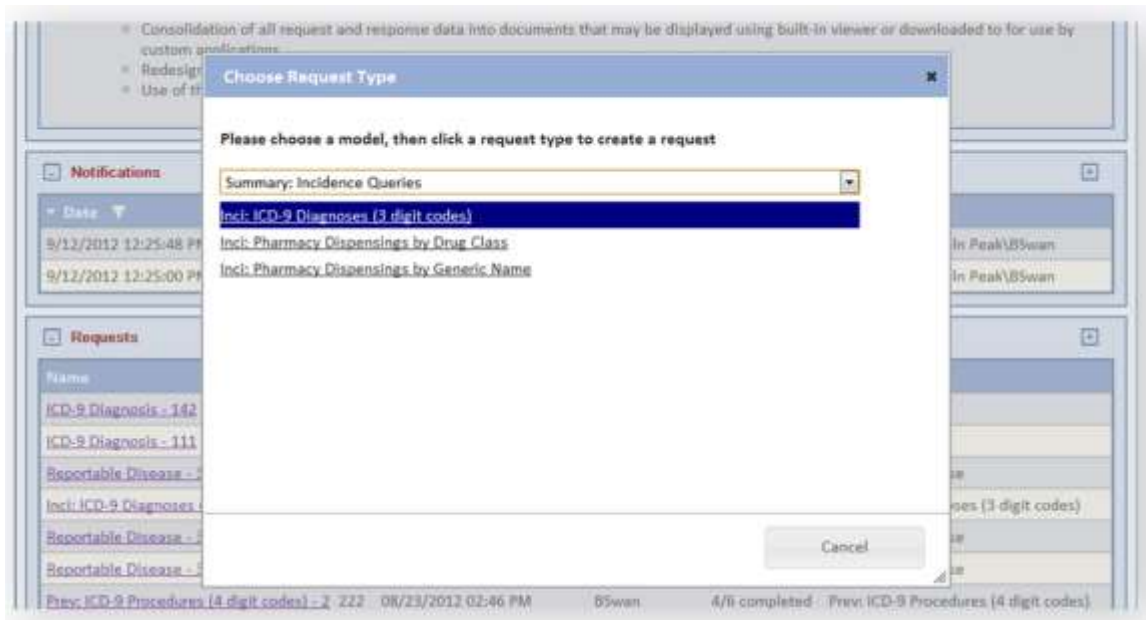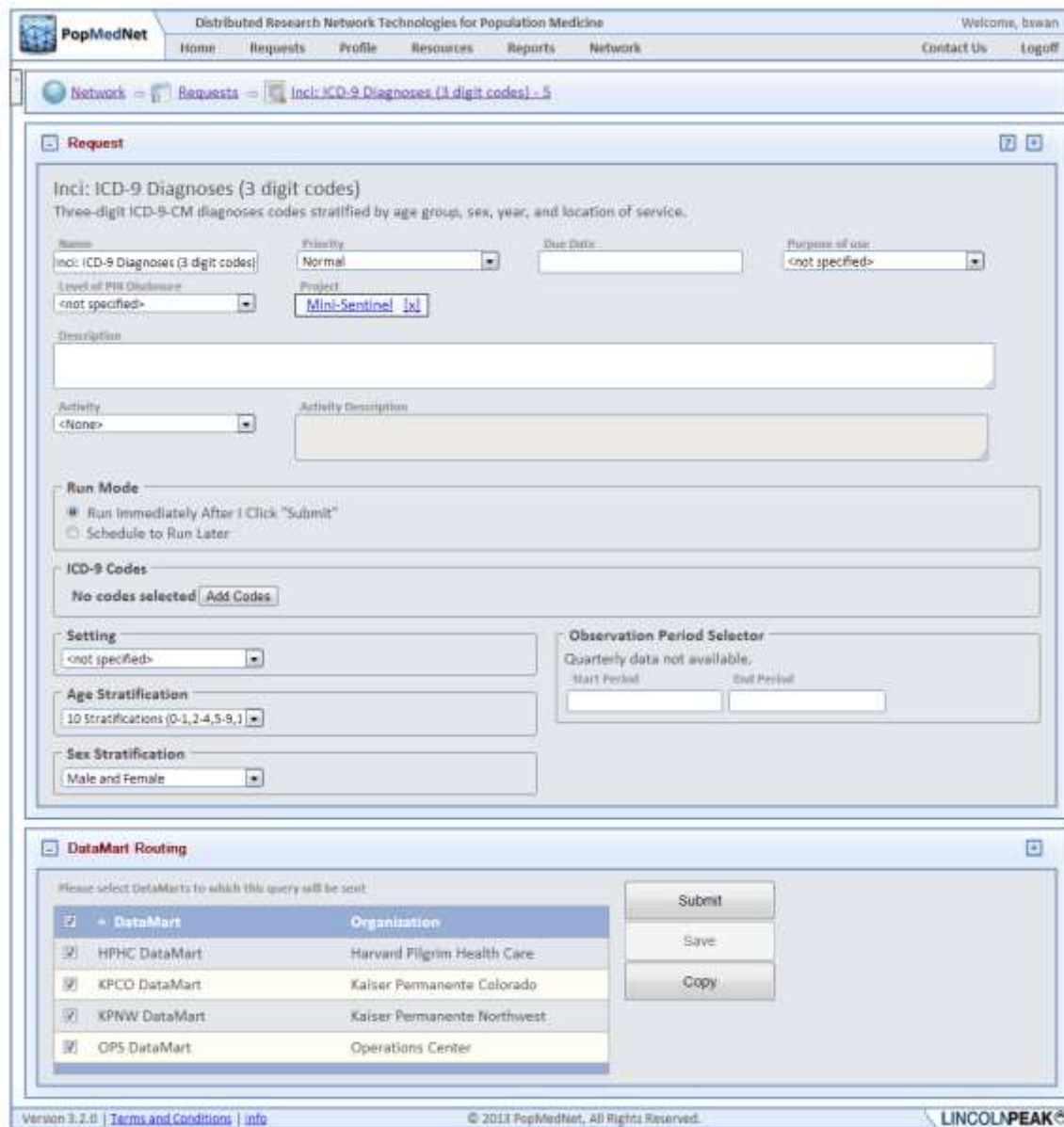
Figure 6: Request Type Dialog

2.7.6 Building a Request

Upon choosing a new request, the respective query composition page is displayed. The user uses the controls on the page to enter information and criteria for the request. This information will be visible to the DataMart administrator who processes the request, as well as any Query Administrator or Group DataMart Administrators who approve requests and responses.

Figure 7: Request Composer Page

2.8 Using the Code Selector

For queries that require the user to choose one or more codes, such as ICD-9 diagnosis codes, the user enters the codes through the Code Selector, a popup dialog that allows the user to search and add codes for the query criteria.

Figure 8: ICD-9 Code Selector Dialog

The user may type the code value or code name in the edit control and see the codes that match in the search results grid below the edit control. Alternatively, the user may click the category control, choose a category, say "Endocrine, Nutritional and Metabolic Diseases, and Immunity Disorders", and all codes with the chosen category will be displayed in the search results list.

The user adds a code to the query criteria by clicking the "add" button next the code item. Selected codes can be removed by clicking the "remove" button.

2.9 Scheduling Requests

A new feature of PopMedNet™ Release 3 is the ability to schedule a request to be submitted at a later time and to set a recurrence pattern for repeated submittals. By default, a request will be submitted for execution immediately upon clicking the "Submit" button. Alternatively, the user may click the "Schedule to Run Later" button in the Run Mode grouping to display a dialog to enter the scheduling details.

Figure 9: Schedule Request Dialog

A request may be scheduled to run on a Daily, Weekly, Monthly, or Yearly pattern. After selecting the pattern, the user enters the date range during which the request will be submitted for execution. Once the schedule is set and the user saves the request, the request will enter a "Scheduled" status. While the request's schedule is active, each scheduled occurrence will cause a copy of the request to be submitted to the selected DataMarts. A scheduled request may be paused, or cancelled by editing the scheduled request and changing the Run Mode to Run Immediately to unschedule the request and convert the request back to Draft status.

2.10 Routing Requests to DataMarts for Execution

The user completes the query criteria by selecting the DataMarts the query should be routed to for execution.
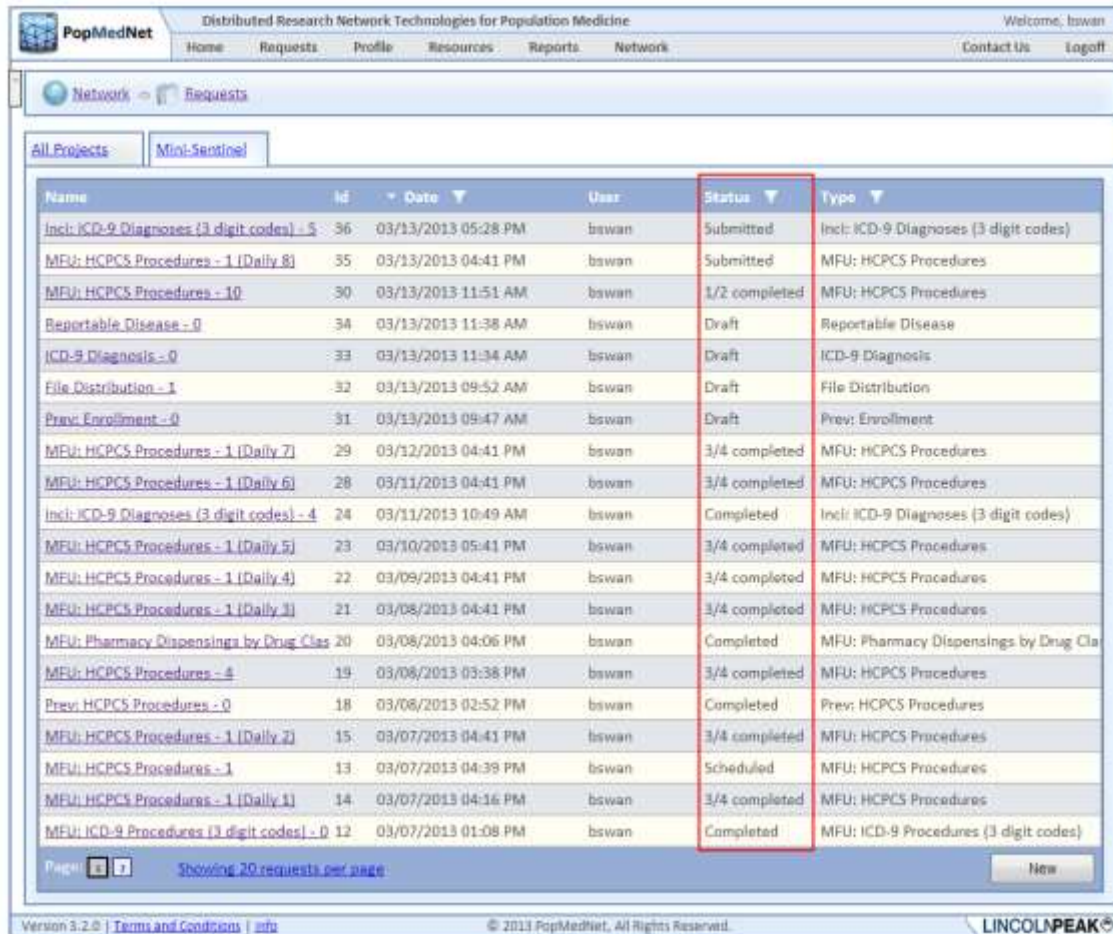
Figure 10: DataMart Routing Panel

Clicking the Submit button will place the request in the selected DataMarts's queue for processing. Clicking the Save button will save the request in a draft state where it can be edited and submitted at a later time. Clicking the Delete button will delete the request. Clicking Copy will make a copy of the request containing all the settings of the original request.

Once the request has been submitted for execution, a notification event is generated that optionally sends email notifications to related users. For instance, the DataMart Administrator(s) responsible for processing the request will be notified, and if query approval is required, administrators responsible for approving requests will be notified.

2.11 Viewing Status on Requests

Once the request is saved or submitted, its status is displayed in the Requests grid visible on the Home page as well as the Request page. The Request page is dedicated to managing on requests.

Figure 11: Requests Page – Request Statuses

2.12 Editing a Draft Request or Viewing Request Detailed Status

If the request is in a Draft status, clicking the request name for an item in the grid will navigate to the request composition page seen in the last section, allowing the user to resume construction of the request and ultimately submit it.

If the request has been submitted, clicking on the request name for a row in the requests grid will navigate the user to the Request Status page.

Figure 12: Request Status Page

The request status page contains a header that identifies the request followed by two grids that show the request DataMart routings that have been completed and those that are still pending.

Depending on the user's rights, the pending DataMarts may be cancelled and new ones be added to the request's routings.

2.13 Viewing Results

Clicking the View Results button on the request status page will display the results page. Depending on the user's rights, all completed DataMart results must be viewed together. For other users, such as Enhanced Investigators, one or more individual DataMart results may be selected for viewing either aggregated or sequentially.

Figure 13: Request Response Page

The DataMart results displayed in the page may be downloaded to the user's desktop by clicking the Export button as either an Excel spreadsheet or a CSV file.

2.14 Other Request Types

The process described above is the virtually the same process for all query types. The detail page used to compose the query may contain slightly different controls that are required for the particular query type. The pages contain brief instructions on the use of the controls.

The following is the query composer for the **File Distribution** query. Instead of creating a summary query, the user selects files to distribute to data partners.

Figure 14: File Distribution Request Composer Page

2.15 Responding to a Query (data partner actions)

Responding to a query through the network requires several steps by the DataMart Administrator using the locally installed DataMart Client. Data partners have the ability to set a notification for small cell counts (a parameter setting) and to re-set those counts to "0" before uploading to the portal. The status of a query will be updated in the Portal according to the actions of the DataMart Administrator.

1. Select Run Query to view results from your DataMart.

Figure 15: DataMart Client Request Detail Form

2. Review the results; obfuscate low cell counts if necessary. You may then select Upload Results which will send your results to the Portal for viewing by the submitter. You may also hold a query for further review or reject a query.

Figure 16: DataMart Client Request Detail Form with Response

3. Provide comments or instructions for the requestor (i.e., the Investigator) to view on the Portal when you run a query, hold or reject.
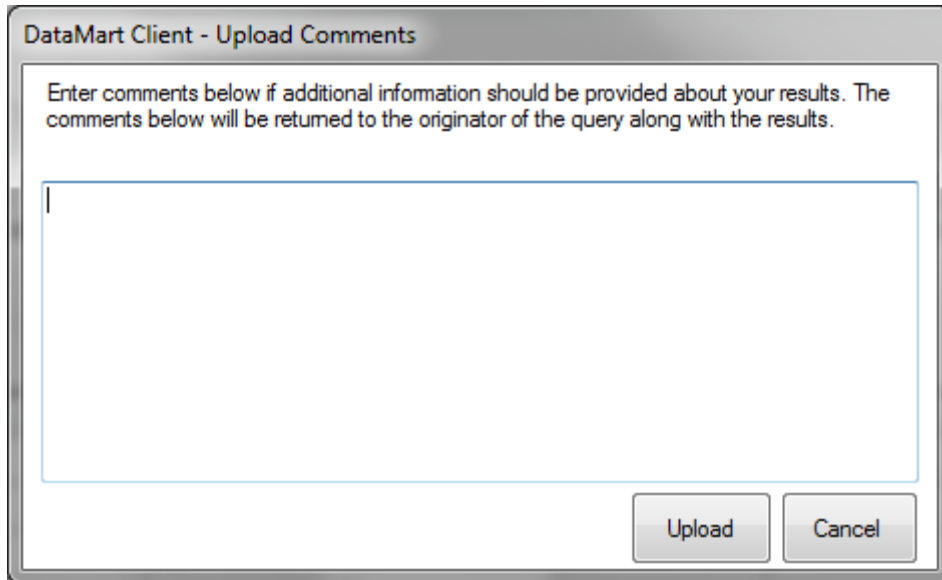
Figure 17: DataMart Client Response Upload Dialog

Responding to a **file distribution query** follows the same query review process. Instead of downloading a query for execution, the DataMart Client downloads the file(s) and can later upload files in response to the request. A screenshot for responding to file distribution queries is below.

Figure 18: DataMart Client File Distribution Request Detail Form

3   System Security Policies and Features

PopMedNet™ has undergone a redesign of the user authentication and user authorization facility for release 3. The result is a more secure and flexible application with increased granularity over granting access rights to users. Additionally, the workflow processes from PMN 2 have been carried over to PMN 3 and integrated into the new authorization mechanism. The following sections provide an overview of these subsystems.

3.1   User Authentication

Authentication is the process of obtaining identification credentials, such as name and password, from a user and validating those credentials against the PMN credential authority. If the credentials are valid, the user that submitted the credentials is considered an authenticated user. Once a user has been authenticated, the authorization process determines whether that user has access to a given resource as described under the User Authorization section below.

PopMedNet implements standard forms authentication provided by ASP.NET against a local user store that is part of the PMN database with custom interface implementation used to manage the PMN user object on whose behalf the code is running.

3.2   User Credentials

Users are assigned a **Username** and **Password** which they use to register themselves to the PMN. These credentials are used to log into the Portal and when establishing a DataMart Client application secure connection to the PMN web services used to exchange requests and responses. Usernames are unique identifiers within a PMN network site instance.   Strong passwords are enforced that require a combination of characters, digits, and special characters, and a minimum length of 9.   Users are forced to change their passwords periodically based on a site-wide configurable parameter (see website configuration section).

3.3   Secure TLS Connections

All access to PMN Portal and to its web service interface is over secure connections using TLS (HTTPS). The DataMart Client application requires user credentials to establish a connection with the PMN Portal web services used to exchange requests and responses. As a convenience, the DataMart Client application stores the user's credentials in Windows Credential Manager to bypass credential prompting when starting the DataMart Client application.

3.4   Mutual Authentication using X.509 Certificates

The DataMart Client application may optionally be configured to require X509 certificates over a TLS connection enabling mutual authentication in a 2 factor design where the user is required to provide both a personal certificate recognized by PMN and a valid username/password.

See the DataMart Administrators guide for details on how to enable X509 certificate authentication.

3.5   User Authorization

Authorization determines whether a user should be granted access to a specific resource, such as the ability to submit a specific request to a set of DataMarts.   In PMN 3, authorization is implemented and enforced through a security group framework described in the following sections.

3.6   Security Groups and Access Control Lists

The PMN Release 3 Access Control system is a significant change to the Roles/Rights system in PMN Release 2. PMN Release 3 provides more granularity, control, and flexibility. There are a number of key concepts that Administrators need to understand to use access control:

- ✓ Access Right – a right to perform a function or access a feature within PMN against a single object or object in the context of other objects.
- ✓ Security Objects – entities within PMN such as Organizations, Users, and DataMarts that require rights to access them.
- ✓ Access Control List (ACL) – the list of access rights attached to single security object or a set of security objects that are associated with a user or group of users who are members of a Security Group.
- ✓ Security Group – a named collection of users and other security groups that are assigned ACLs.

3.7   Access Right

An **Access Right** is the ability to permit or deny the use of a PMN feature or action by a user against an object type, specific object, or combination of objects. There are a large number of access rights defined within PMN. Rights affect the use of various PMN entities, such as Users, Organizations, and DataMarts, or a combination of objects. For instance, the ability to submit a specific request type to a given DataMart, or the ability to perform administrative tasks, such as creating organizations, users, and DataMarts.

The following image shows an Access Right in the Network/Access/Global permissions panel of the Portal that determines the right to manage global access rights within the network, and create organizations and DataMarts:
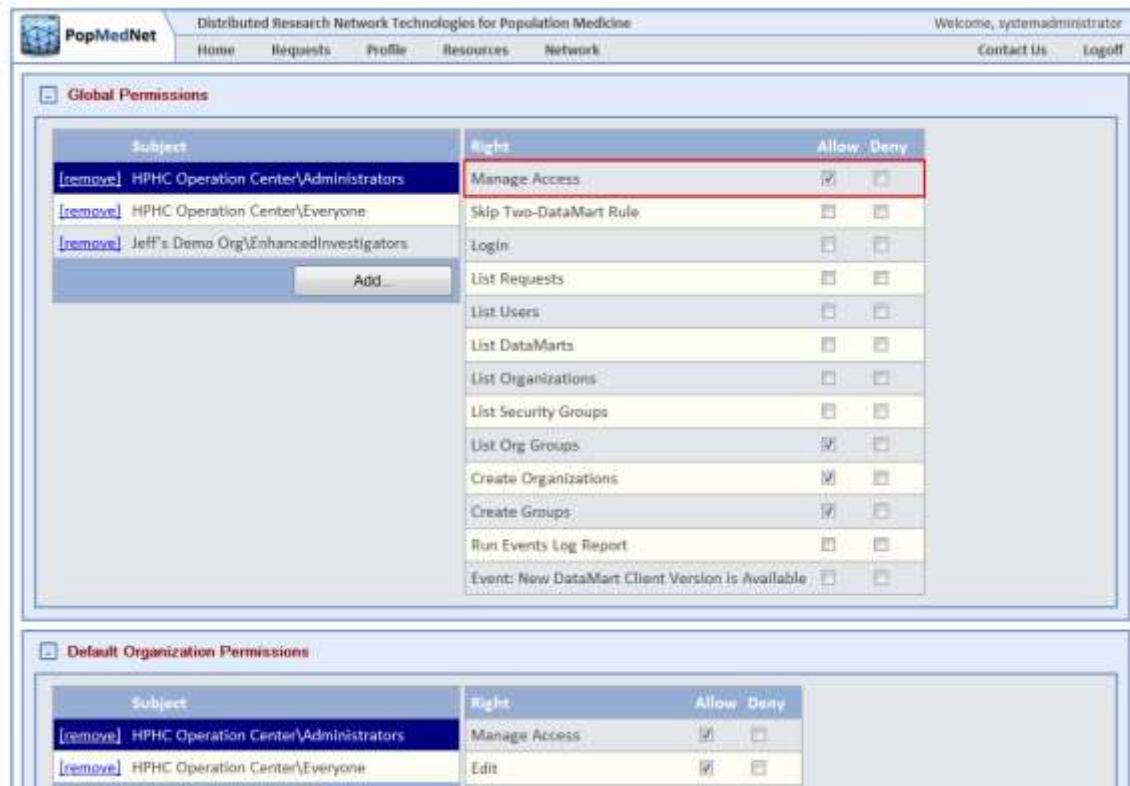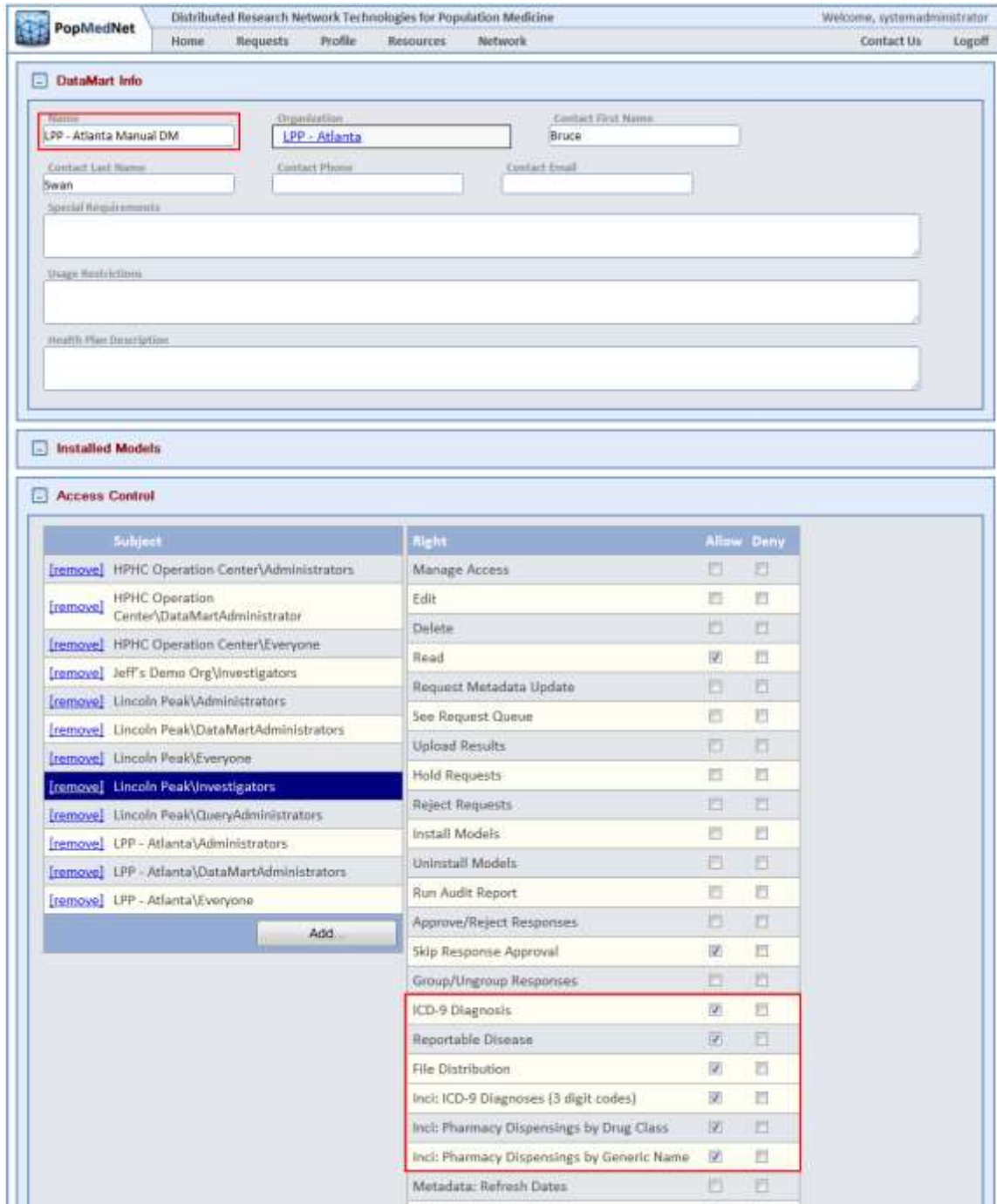
Figure 19: Network Access Page – Global Access Rights

Each right can be Allowed, Denied, or left unchecked. Clicking the "Allow" checkbox grants the user the right. Clicking the "Deny" checkbox explicitly denies the user the right even if the user had been granted the right through **inheritance**, a topic discussed later in this section. Leaving the right unchecked simply doesn't grant or deny the user the right to perform the related action, so users inherited right applies if once has been specified.

3.8   Security Objects

Security Objects are PMN entities such as Organizations, Users, and DataMarts that expose access rights to perform actions against them. In some instances, the rights apply to a single kind of object; say the right to create Organizations. In other cases, the rights apply a given object in the context of another object(s), in which case we associate the right to a **set** of security objects. For instance, the right to submit a request type, i.e. an ICD-9 Diagnosis query, to a specific DataMart; call it "LPP – Atlanta Manual DM". In this case, the "submit" right would be applied to the set **{ICD-9 Diagnosis, LPP – Atlanta Manual DM}**.

The following image shows the granting the rights to submit a set of request types to the LPP – Atlanta Manual DM to the Lincoln Peak Investigators security group:

Figure 20: DataMart Profile Page – DataMart Request Access Rights

In the image above, note that DataMart objects have many rights, some of which are references to specific request types, others rights control how can administer the DataMart.
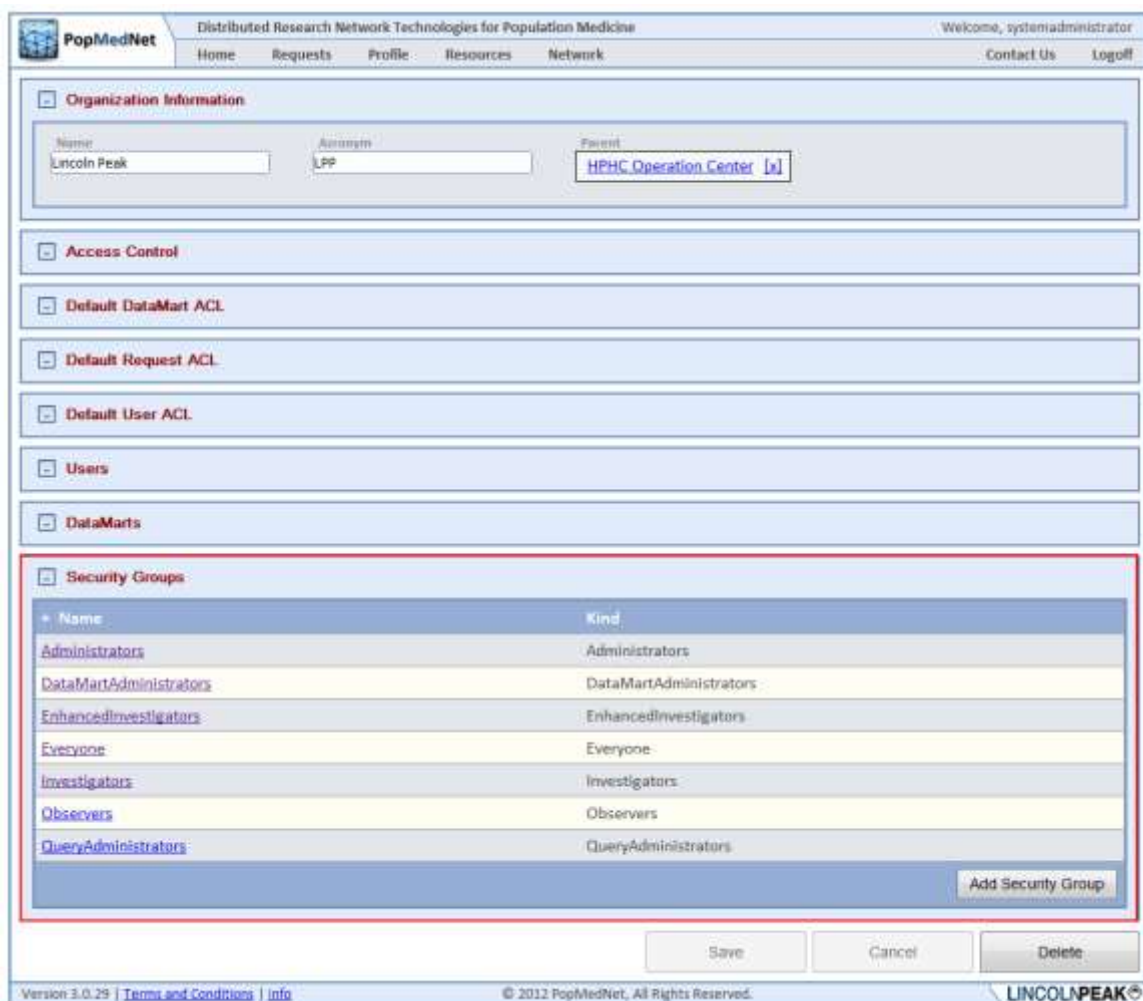
3.9   Access Control Lists

An **Access Control List (ACL)** is a collection of access rights attached to a security object or set of objects. An ACL contains a reference to the object or set of objects it applies to, and specifies which users that are granted or denied access to objects.

3.10 Security Groups

A **Security Group** is a collection of users and other security groups that are assigned rights relative to a security object or set of security objects. While ACL's can be assigned to a individual user, security Groups are a convenient way to manage rights within the network by defining the rights applied to a given group and then adding multiple users as members of that group. Users who are members of a security group take on the rights of that group. Users may be members of one or more security groups allowing them to take on multiple roles within the network.

Security groups are defined at the organizational level. Each Organization has a set of security groups by default that models the typical roles with PMN. The following image displays the security groups for the Lincoln Peak organization:

Figure 21: Organization Profile Page – Security Groups

Custom security groups may be created by clicking the "Add Security Group" button. The security groups names are not unique across organizations, therefore they must be referenced using a fully qualified name composed of the organization that owns the security group followed by the "/" sign and then the group name, such as "Lincoln Peak/Investigators". This

---

distinguishes the Investigators group in Lincoln Peak from other organizations' Investigators groups.

Security groups may contain other security groups by clicking on the security group name at the bottom of the organization page to navigate to the security group detail page. Next click the "Add" button in the Member of Groups panel, and then navigate choose other security groups to be members of this group.
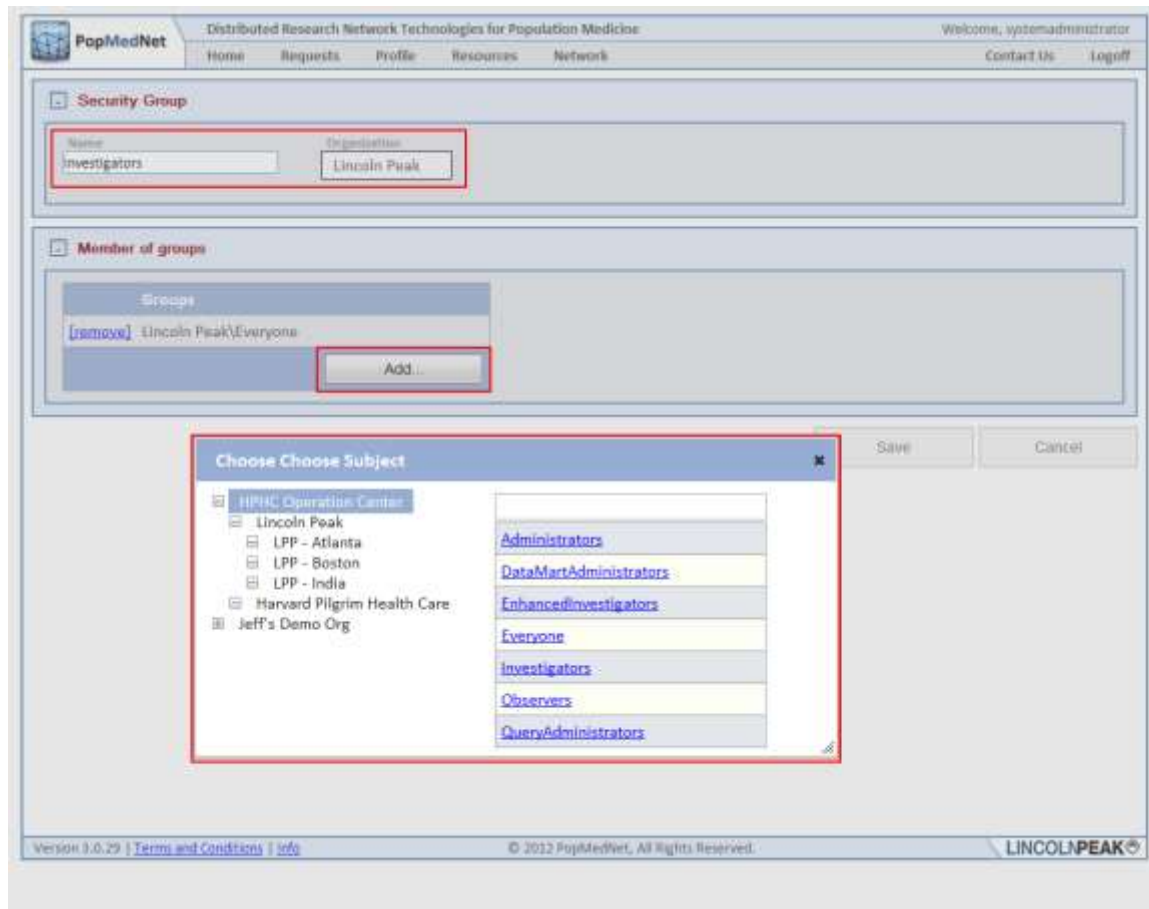
Figure 22: Security Group Page –Editing a Security Group

Organizations may have sub-organizations, so you may need to expand a parent organization to navigate to the groups in its sub-organizations in the organization tree control.

3.11 Security Group Membership for Users

Users may be members of one or more Security Groups. This allows a single user account to be assigned multiple roles by simply adding the user as a member of one or more security groups on the user's profile as illustrated in the following figure.
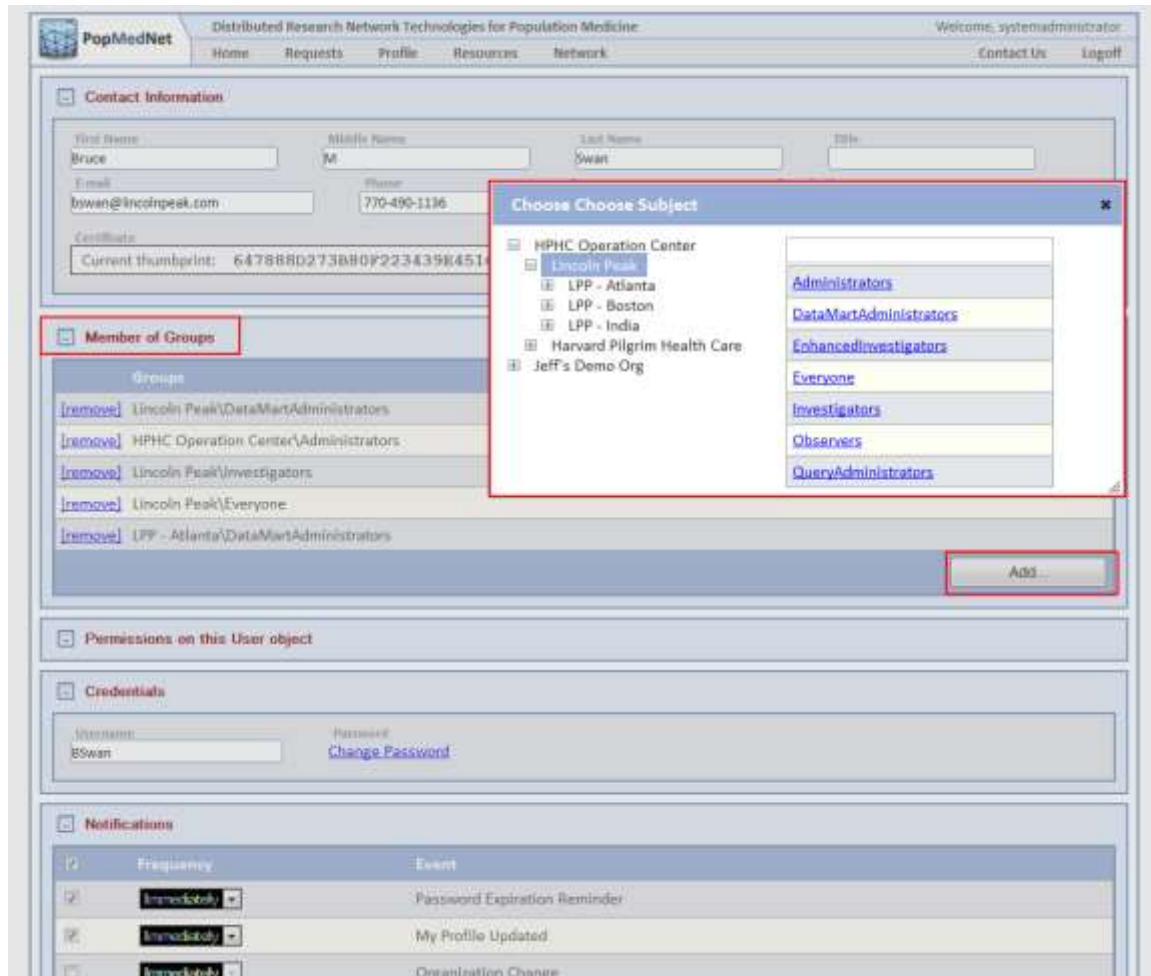
Figure 23: User Profile Page – Adding Users to Security Groups
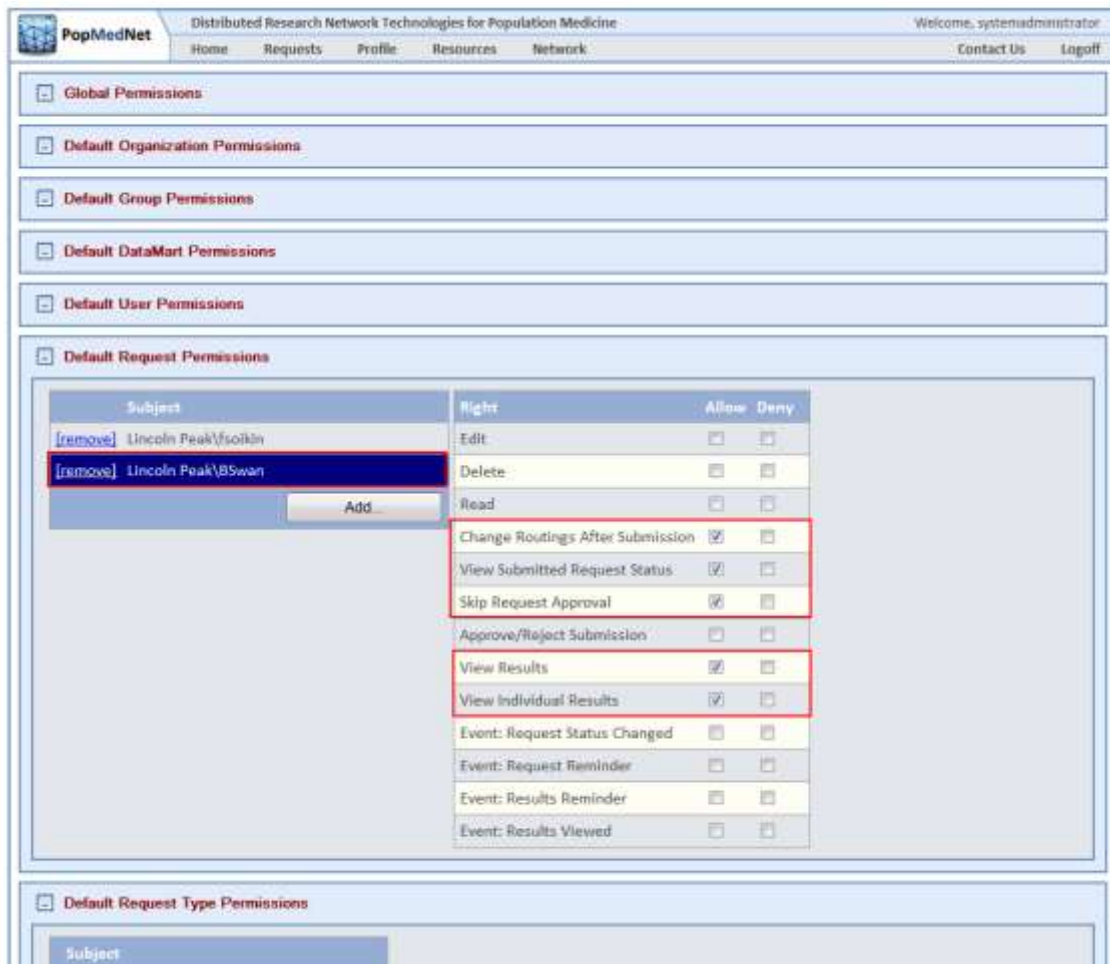
As is shown in the illustration, go to the user's profile and click the "Add …" button in the "Member of Groups" panel to display the list of security groups within organization.   Once the user is member of a group, the user inherits all the rights of the group.

3.12   Access Right Inheritance

As with PopMedNet™ Release 2, users may inherit rights set at a higher level in the organizational hierarchy. There are two types of inheritance within PMN: Organizational Inheritance and Membership Inheritance. These are discussed in the next two sections.

3.13   Organizational Inheritance
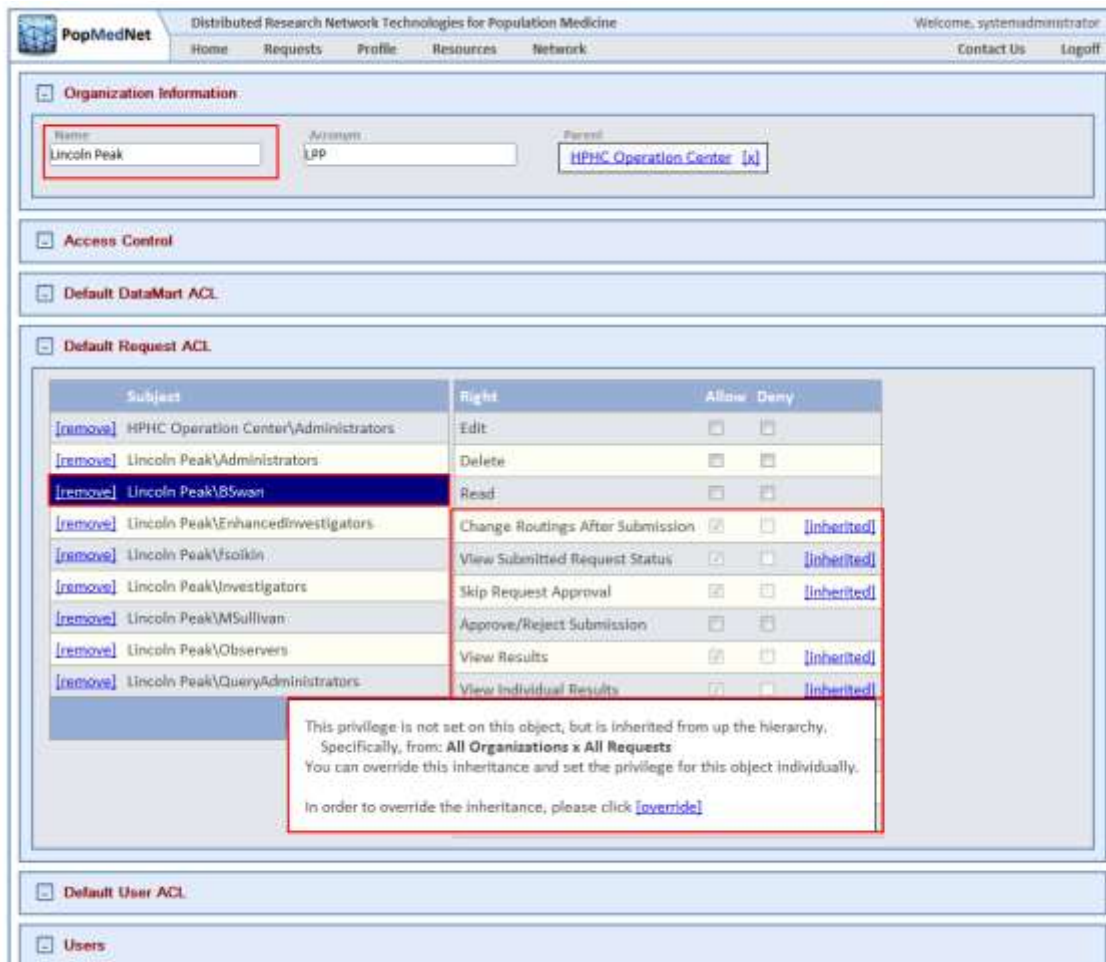
Organizational inheritance is formed by assigning rights to users at either the PMN network Global / Default access controls (Network/Access Control) or by assigning rights to the user through their Organization or Group. For instance, if the user is granted a global access right, say to view individual DataMart results:

Figure 24: Network Access Page – Global Inheritance

Then the user will have this right for all DataMart results unless explicitly denied by a lower level entity. The following figure illustrates the inheritance link that is displayed at the user's organization for the rights that have been granted by the Network/Access Control page:

Figure 25: Organization Profile Page – Inheritance Popup Message

As is shown the figure above, when inheritance is detected for a right, an "inherited" link is displayed. Clicking the link displays the inheritance override popup dialog. Clicking the "override" link allows the administrator to explicitly override the inherited right, such as denying the right for a specific organization show in the figure below:

Figure 26: Organization Profile Page – Global Inheritance Override

In the above case, the user is explicitly denied from viewing individual results at the organization level that was inherited from the global default page. Similarly, overrides may be set for specific DataMarts by finding the user or security group in the Access Control panel of a given DataMart and overriding the inherited right.

3.14   Security Group Inheritance

The other way users inherit rights is by adding them to security groups that are members of other groups. For instance, a user may be a member of the "Enhanced Investigators" group, and the Enhanced Investigators group is a member of the Investigators group as follows:

Figure 27: Security Group Page – Security Group Inheritance

In this case, any users who are members of the Lincoln Peak\EnhancedInvestigator group will also inherit the rights of the Lincoln Peak\Investigators group since the EnhancedInvestigator group is a member of the Investigator's group.

3.15 Access Rights Reference

Access rights are divided into four areas:

- ✓ Global and Default Access Rights – used to manage network-wide settings and defaults across all PMN objects.
- ✓ Organizational Access Rights – used to manage access for each Organization including defaults for its users and DataMarts.
- ✓ DataMart Access Rights – used to manage access to each DataMart.
- ✓ Group Access Rights – used to manage access for each Group.

The following sections describe each of the PMN access rights.

3.16 Global Permissions and Defaults

The Global Permissions can be found by navigating to the Network/Access Control page.

Table 6: Global Permissions

Category	Right	Description
Global Permissions	Manage Access	Ability to modify the global and default access rights
	Skip Two-DataMart Rule	Disables requirement for users to submit requests to DataMarts from at least two organizations different from their own
	Login	Ability to login
	List Requests	Ability to view the request queue
	List Users	Ability to view the list of network users

Category	Right	Description
	List DataMarts	Ability to view the list of DataMarts
	List Organizations	Ability to view the list of organizations
	List Security Groups	Ability to view the list of security groups
	List Groups	Ability to view the list of groups
	Create Organizations	Ability to create new organizations
	Create Groups	Ability to create new groups
	Run Events Log Report	Ability to run event log report
	Event: New DataMart Client Version Available	Ability to subscribe to new DataMart client version available event
Default Organization Permissions	Manage Access	Ability to modify any organization's access rights
	Edit	Ability to modify any organization's profile
	Delete	Ability to delete any organization
	Read	Ability to view any organization's profile
	Create Users	Ability to create users for any organization
	Create DataMarts	Ability to create DataMarts for any organization
	Event: New Request Submitted	Ability to subscribe to new request submit events for all users
	Event: Organization Change	Ability to subscribe to subscribe to the event for changes for all organizations
Default Group Permissions	Manage Access	Ability to modify any group's access rights
	Edit	Ability to modify any group's profile
	Delete	Ability to delete any group
	Read	Ability to view any group's profile
	Event: Group Change	Ability to subscribe to changes for any group
Default DataMart Permissions	Manage Access	Ability to modify any DataMart's access rights
	Edit	Ability to modify any DataMart's profile
	Delete	Ability to delete any DataMart
	Read	Ability to view any DataMart's profile
	Request Metadata Update	Ability to issue a Metadata update request for any DataMart
	View Request Queue	Ability to view any DataMart's request queue in the DataMart client application
	Upload Reponses	Ability to upload responses to all DataMarts' requests in the DataMart client application

Category	Right	Description
	Hold Requests	Ability to hold responses for all DataMarts' request queue in the DataMart client application
	Reject Requests	Ability to reject responses for all DataMart's request queue in the DataMart client application
	Install Models	Ability to install models for any DataMart
	Uninstall Models	Ability to uninstall models for any DataMart
	Run Audit Report	Ability to run an audit report for any DataMart
	Approve/Reject Reponses	Ability to approve or reject responses for any DataMart's requests
	Skip Response Approval	Ability to disable the requirement for responses to be approved by an administrator for all DataMarts
	Group/Ungroup Responses	Ability to group/ungroup multiple DataMart responses into a single virtual result
	Event: DataMart Change	Ability to subscribe any DataMart change event
Default User Permissions	Manage Access	Ability to modify any User's access rights
	Edit	Ability to modify the profile for any users
	Delete	Ability to delete any user account
	Read	Ability view any user profile
	Change Password	Ability to modify any user's password
	Change Login	Ability to modify any user's username
	Manage Notifications	Ability to modify any user's notification options
	Change X.509 Certificate	Ability to modify any user's X.509 certificate thumbprint
	Event: User Change	Ability to subscribe to the profile change event for any user
	Event: Registration Submitted	Ability to subscribe to new user registration events for all organizations
	Event Registration Status Changed	Ability to subscribe to any registration status change events for all organizations
Default Request Permissions	Edit	Ability to edit requests created by any user
	Delete	Ability to delete requests created by any user
	Read	Ability to view requests created by any user
	Change Routings After Submission	Ability to change DataMart routings for all requests

Category	Right	Description
	View Submitted Request Status	Ability to view submitted request status for all requests
	Skip Request Approval	Disables requirement for requests to be approved
	Approve/Reject Submission	Ability to approve / reject request submitted by any user
	View Results	Ability to view results from any user
	View Individual Results	Ability to view individual results
	Event: Request Status Changed	Ability to subscribe to the request status change event for requests created by any user
	Event: Request Reminder	Ability to subscribe to the request reminder event for requests created by any user
	Event: Results Reminder	Ability to subscribe to the results reminder change event for requests created by any user
	Event: Results Viewed	Ability to subscribe to the results viewed event for requests created by any user

3.17 Organization Permissions

The Organization Permissions can be found by clicking on an Organization after navigating to the Network/Organizations list page.   These settings apply to the selected organization.

Table 7: Organization Permissions

Category	Right	Description
Access Control	Manage Access	Ability to modify the organizational access rights
	Edit	Ability to modify the profile of the organization or sub-organizations
	Delete	Ability to delete organization or sub-organizations
	Read	Ability to view the organization's profile
	Create Users	Ability to create users for the organization or sub-organizations
	Create DataMarts	Ability to create DataMarts for the organizations or sub-organizations
	Event: New Request Submitted	Ability to subscribe to new request submit events for the organization's users and any sub-organizations
	Event: Organization Change	Ability to subscribe to subscribe to the event for changes to the organization and any sub-organizations
Default DataMart Permissions	Manage Access	Ability to modify the access rights for any DataMart of the organization or sub-organizations

Category	Right	Description
	Edit	Ability to modify the profile of any DataMart's of the organization or sub-organizations
	Delete	Ability to delete any DataMart of the organization or sub-organizations
	Read	Ability to view the profile of any DataMart of the organization or sub-organizations
	Request Metadata Update	Ability to issue a Metadata update request for any DataMart of the organization or sub-organizations
	View Request Queue	Ability to view request queue in the DataMart client application of any DataMart of the organization or sub-organizations
	Upload Reponses	Ability to upload responses to requests in the DataMart client application of any DataMart of the organization or sub-organizations
	Hold Requests	Ability to hold responses to requests in the DataMart client application of any DataMart of the organization or sub-organizations
	Reject Requests	Ability to reject responses for request in the DataMart client application of any DataMart of the organization or sub-organizations
	Install Models	Ability to install models for any DataMart of the organization or sub-organization
	Uninstall Models	Ability to uninstall models for any DataMart of the organization or sub-organizations
	Run Audit Report	Ability to run an audit report for any DataMart of the organization or sub-organizations
	Approve/Reject Responses	Ability to approve or reject responses for any DataMart of the organization or sub-organizations
	Skip Response Approval	Ability to disable the requirement for responses to be approved by an administrator for all DataMarts of the organization or sub-organizations
	Group/Ungroup Responses	Ability to group/ungroup multiple responses of any DataMart of the organization or sub-organizations into a single virtual result
	Event: DataMart Change	Ability to subscribe DataMart change event of any DataMart of the organization or sub-organizations
Default User Permissions	Manage Access	Ability to modify access rights of any users of the organization and sub-organization

Category	Right	Description
	Edit	Ability to modify the profile for any users of the organization and sub-organizations
	Delete	Ability to delete any user account of the organization or sub-organizations
	Read	Ability view the profile of any user of the organization or sub-organizations
	Change Password	Ability to modify any user's password
	Change Login	Ability to modify any username of any user of the organization or sub-organizations
	Manage Notifications	Ability to modify the notification options of the user of the organization or sub-organizations
	Change X.509 Certificate	Ability to modify the X.509 certificate thumbprint of any user of the organization or sub-organizations
	Event: User Change	Ability to subscribe to the profile change event for any user of the organization or sub-organizations
	Event: Registration Submitted	Ability to subscribe to new user registration events for the organization and sub-organizations
	Event Registration Status Changed	Ability to subscribe to any registration status change events for the organization or any sub-organizations
Default Request Permissions	Edit	Ability to edit requests created by any user of the organization or sub-organizations
	Delete	Ability to delete requests created by any user of the organization or sub-organizations
	Read	Ability to view requests created by any user of the organization or sub-organizations
	Change Routings After Submission	Ability to change DataMart routings for all requests submitted by users of the organization or sub-organizations
	View Submitted Request Status	Ability to view submitted request status for all requests submitted by users of the organization or sub-organizations
	Skip Request Approval	Disables requirement for requests to be approved submitted by users of the organization or sub-organizations
	Approve/Reject Submission	Ability to approve / reject request submitted by users of the organization or sub-organizations
	View Results	Ability to view results from users of the organization or sub-organizations

Category	Right	Description
	View Individual Results	Ability to view individual results of requests submitted by users of the organizations or sub-organizations
	Event: Request Status Changed	Ability to subscribe to the request status change event for requests created by users of the organization or sub-organizations
	Event: Request Reminder	Ability to subscribe to the request reminder event for requests created by users of the organization or sub-organizations
	Event: Results Reminder	Ability to subscribe to the results reminder change event for requests created by users of the organization or sub-organizations
	Event: Results Viewed	Ability to subscribe to the results viewed event for requests created by users of the organization or sub-organizations

3.18 DataMart Permissions

The DataMart Permissions can be found by clicking on a DataMart after navigating to the Network/DataMarts list page.   These settings apply to the selected DataMart.

Table 8: DataMart Permissions

Category	Right	Description
Access Control	Manage Access	Ability to modify the access rights for the selected DataMart
	Edit	Ability to modify the profile of the selected DataMart
	Delete	Ability to delete the selected DataMart
	Read	Ability to view the profile of the selected DataMart
	Request Metadata Update	Ability to issue a Metadata update request for the selected DataMart
	View Request Queue	Ability to view request queue in the DataMart client application of the selected DataMart
	Upload Reponses	Ability to upload responses to requests in the DataMart client application of the selected DataMart
	Hold Requests	Ability to hold responses to requests in the DataMart client application of the selected DataMart
	Reject Requests	Ability to reject responses for request in the DataMart client application of the selected DataMart
	Install Models	Ability to install models for the selected DataMart

Category	Right	Description
	Uninstall Models	Ability to uninstall models for the selected DataMart
	Run Audit Report	Ability to run an audit report for the selected DataMart
	Approve/Reject Reponses	Ability to approve or reject responses for the selected DataMart
	Skip Response Approval	Ability to disable the requirement for responses to be approved by an administrator for the selected
	Group/Ungroup Responses	Ability to group/ungroup multiple responses of the DataMart into a single virtual result
	Event: DataMart Change	Ability to subscribe DataMart change event of the selected DataMart
ESP Query Builder	ICD-9 Diagnosis	
	Reportable Disease	
File Distribution	File Distribution	
Incidence Summary Queries	Inci: ICD-9 Diagnosis (3-digit)	
	Inci: Pharmacy Dispensings by Drug Class	
	Inci: Pharmacy Dispensings by Generic Name	
	Metadata Refresh Dates	
Prevalence Summary Queries	Prev: Dispensings by National Drug Code	
	Prev: Enrollment	
	Prev: HCPCS Procedures	
	Prev: ICD-9 Diagnosis (3-digit codes)	
	Prev: ICD-9 Diagnosis (4-digit codes)	
	Prev: ICD-9 Diagnosis (5-digit codes)	
	Prev: ICD-9 Procedures (3 digit codes)	
	Prev: ICD-9 Procedures (4 digit codes)	

Category	Right	Description
	Prev: Pharmacy Dispensings by Drug Class	
	Prev: Pharmacy Dispensings by Generic Name	
MFU Summary Queries	MFU: HCPCS Procedures	
	MFU: ICD-9 Diagnosis (3-digit codes)	
	MFU: ICD-9 Diagnosis (3-digit codes)	
	MFU: ICD-9 Diagnosis (4-digit codes)	
	MFU: ICD-9 Diagnosis (5-digit codes)	
	MFU: ICD-9 Procedures (3-digit codes)	
	MFU: ICD-9 Procedures (4-digit codes)	
	MFU: Pharmacy Dispensings by Drug Class	
	MFU: Pharmacy Dispensings by Generic Name	

3.19 Providing Access to DataMart Requests

The primary purpose PMN is to allow investigators to issue queries to DataMarts. In PopMedNet™ 3, this is managed by granting the rights to issue a specific query or request to the user either indirectly via membership in a Security Group or directly by adding them to each DataMart and setting the access rights for specific requests. Once the user has the right to issue a query for at least one DataMart, this request type will become available in the new request dialog box, and the individual DataMart(s) for which the user has rights to issue the query will appear in the DataMart routings list at the bottom of the request detail page. The following figure shows an example of granting access an Investigator security group for a specific DataMart:

Figure 28: DataMart Profile Page – DataMart Request Permissions

The access rights for requests appear once its Request Model is installed at the DataMart. The following figure shows the list of installed models for the DataMart in the above figure.

Figure 29: DataMart Profile Page – Installed Request Models

For example, when the ESP Query Builder request model was installed at the above DataMart, the following requests became visible in the Access Control panel:

Figure 30: DataMart Profile Page – DataMart Request Type Rights for Specific Request Model

3.20 Built-in Security Groups

As was described in the sections above, PMN uses group-based access control to give users permission to perform certain functions. The system currently has six built-in security groups for each organization. The following lists these groups along with a brief description of their purpose.

✓ Everyone - can perform minimum functions such as the ability to login and navigate the network organizations, users, and DataMarts.

✓ Administrators - can add new data partners; create groups, organizations, and roles; add/delete users; re-set passwords; and view all queries submitted.

✓ Investigators - can submit queries to DataMarts that have given them or their organization permission to submit queries and view only aggregated query results.

✓ Enhanced Investigators - can submit queries to DataMarts that have given them or their organization permission to submit queries and review their query results. This group has the additional right to view site results individually across the organizations within the query.

✓ Query Administrators - approves outgoing queries for an organization-useful for query budgeting. This role also acts like an Enhanced Investigator for querying and viewing results.

✓ Response Administrators - able to review, aggregate, and release results for an organization or group. A group of data partners can designate a person as the group administrator, and select rules that require the group administrator to review group results before the results are released to the requestor. Results can be released individually or as an aggregate.

✓ DataMart Administrator - manages the local DataMart(s) for each data partner. This group can set DataMart preferences on the Portal and DataMart Client (e.g., what data can be queried and by whom). There can be one or more DataMart Administrators per data partner. DataMart Administrators cannot send queries to other DataMarts.

✓ Observer - can view queries and results and get notifications for all users within the user's organization and sub-organization.

Additional security groups may be defined and developed at the discretion of a Network or Organizational Administrator in accordance with the governance of the system.
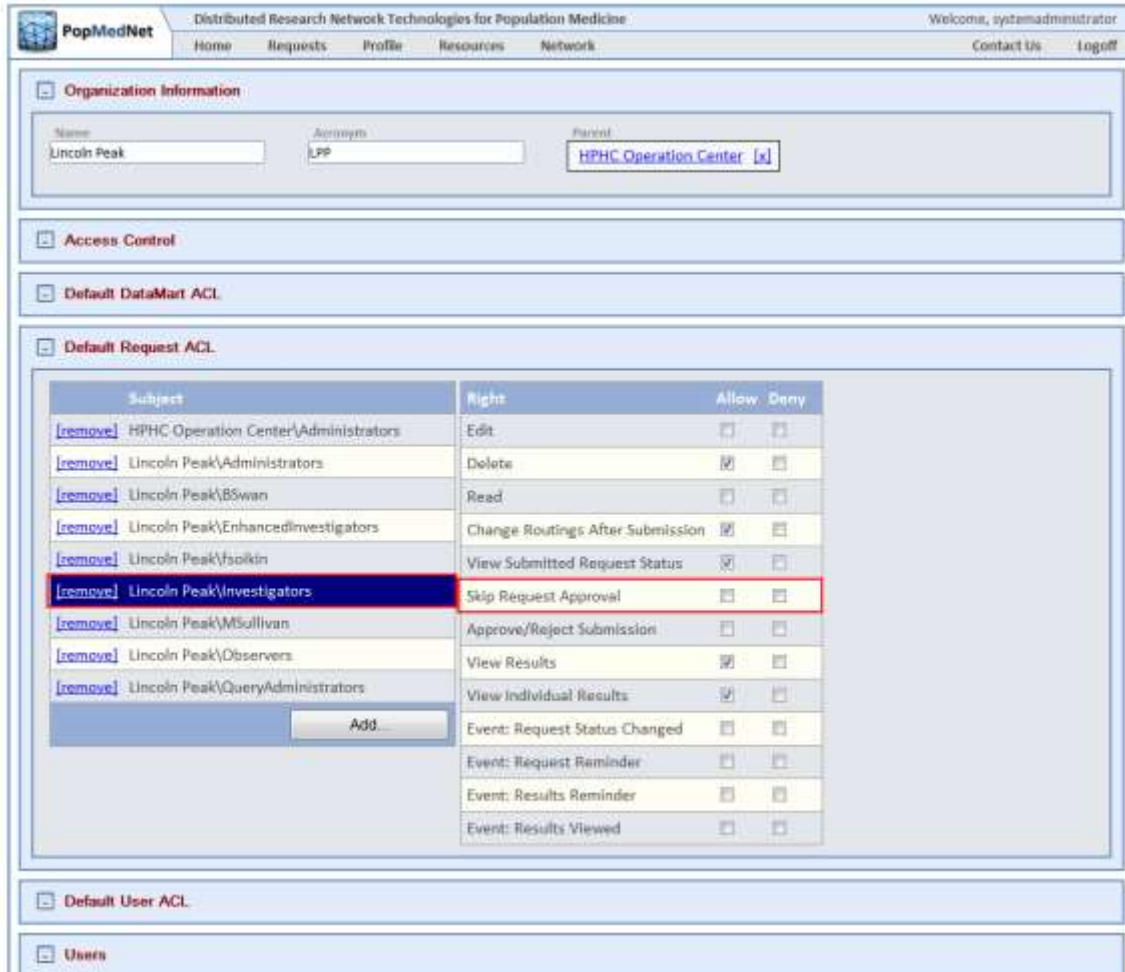
3.21 Request / Response Workflow Policies

In addition to Authentication and Authorization facilities described above, there are a set of workflow policies that may be enabled in PMN.

3.22 Review and Approve Requests

PopMedNet provides a policy that requires requests to be reviewed and either approved or rejected by administrators. This policy is enabled by first ensuring the "Skip request approval" rights is disabled on all users that require their requests to be reviewed and then granting the "Approve/Reject Submission" right and the "Read" permission in the "Default Request ACL" panel of the organization, or global access page, of the users (Administrators) performing the review. This will allow administrators to review and approve requests for all users' requests requiring approval within their organization or sub-organizations.

The following figure illustrates the settings for users whose queries should be reviewed:

Figure 31: Organization Profile Page – Request Review Required Right

The following figure illustrates the settings users (Administrators) performing the review:

Figure 32: Organization Profile Page – Request Review/Approve Rights

By default, all users require their requests to be approved; this feature must be explicitly disabled to prevent this. Also, rather than grant rights to individual users, network and organizational administrators can add users who will perform the review to the QueryAdministrators security group of organization or parent organization of the users being reviewed.

3.23 Review and Approve DataMart Responses

PopMedNet provides a policy that requires responses to be reviewed and either approved or rejected by administrators. This policy is enabled by first ensuring the "Skip response approval" rights is disabled on all users that require their responses to be reviewed and then granting the "Approve/Reject Response" right in the "Default DataMart ACL" panel and the "Read" permission in the "Default Request ACL" panel of the organization, or global access page, of the users performing the review. This will allow administrators to review and approve responses for all users' requests requiring approval within the response administrator's organization or sub-organization.

The following figure shows the settings for users who require their responses to be reviewed:

Figure 33: Organization Profile Page - DataMart Client Application Response Review Required Rights

The following figure shows the settings assigned to response administrators:

Figure 34: Organization Profile Page - Response Review/Approve Rights

Alternatively, users to perform response reviews may be added to the ResponseAdministrators security group of the organization or its sub-organizations of the users who require the review.

4 PopMedNet™ Sample Governance Policies

Each network using the PopMedNet™ system can develop and implement its own governance policies. This section provides a set of sample governance policies for illustration purposes. The policies listed below are available for use or customization based on network needs; additional policies can be designed and implemented as required by a network.

- ✓ Representatives from HPHCI and LPP will serve as network administrators.

- ✓ New data partners and network users can only be added to the network by the Network Administrator and in accordance with network governance policies.

- ✓ Security group-based access control gives network users permission to perform certain functions; network users who have two roles (e.g., Investigator and DataMart Administrator) by adding them to their organization's security groups for those functions.   These users can use a single account that to perform their duties since they may be a member of multiple groups in PopMedNet™ Release 3.

- ✓ Approved partners may view site-specific results, all others will only be able to view aggregated results; network rules will ensure results cannot be disaggregated.

- ✓ Data partners will appoint one or more individuals to serve as DataMart Administrators for their sites. DataMart Administrators will be responsible for responding to queries distributed to their DataMart through the network.

- ✓ DataMart Administrators will retain full control over access to their data and of the transmission of query results. They will have the ability to accept or reject each query on a case-by-case basis.

- ✓ Data partners may use the network to query their own data.

- ✓ DataMart Administrators can, at any time, create audit reports of activity related to their DataMart.

- ✓ DataMart Administrators will determine their DataMart access settings on the Portal, including contact information, the tables available for querying, and the users/ organizations/groups able to send queries. These settings can be changed at any time.

- ✓ System Administrators will not alter any DataMart settings without prior approval of a DataMart Administrator; DataMart Administrators can opt to be alerted via email when any DataMart settings change.

- ✓ Query results **may not** be used in a proposal or in any report without the consent of the Network member organization where the data originated.

- ✓ No publication or external report other than use in research proposals is permitted.

5   Managing PopMedNet Entities

The following lists the PopMedNet entities that are managed through the Portal:

- ✓ Organizations
- ✓ Groups
- ✓ DataMarts
- ✓ Users
- ✓ Security Groups
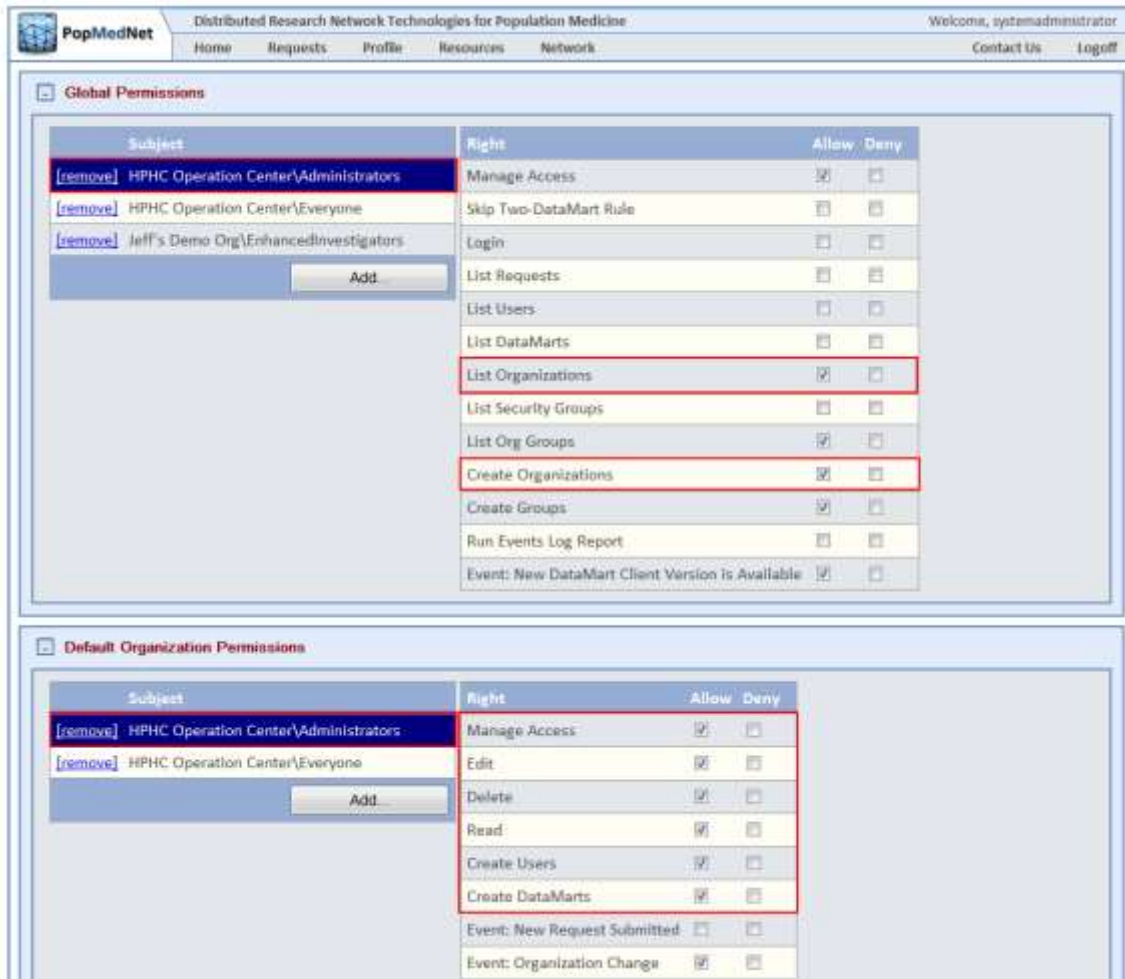
The following sections describe how to use PMN to manage these entities.

5.1   Managing Organizations

Organizations are a collection of Users and DataMarts that model real world organizations. Organizations may have zero, one, or more sub-organizations but a sub-organization may have only a single parent organization.   Establishing an organizational hierarchy allows some PMN features to extend to sub-organizations. For instance, users with access rights for to review and approve requests submitted by users in their organization can also view and approve requests of users in sub-organizations.

5.2   Viewing and Creating Organizations

There are a set of access rights that determine whether users can view, create, edit, and delete organizations. These rights may be applied at the global level or within an existing organization. The following figure shows the global access rights to manage organizations for the entire network:

Figure 35: Network Access Page – Global Default Organizational Rights

An organization is created by clicking the "Add Organization" button in the Organization List page as shown in the following figure:
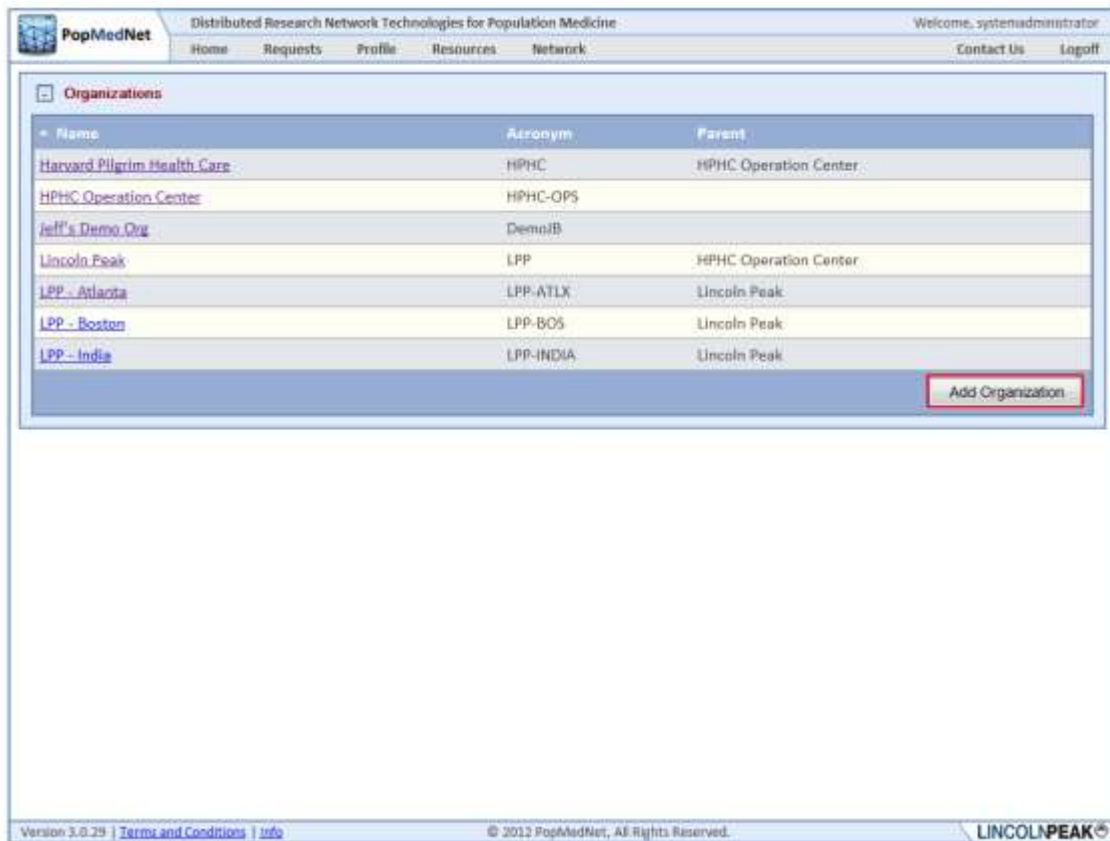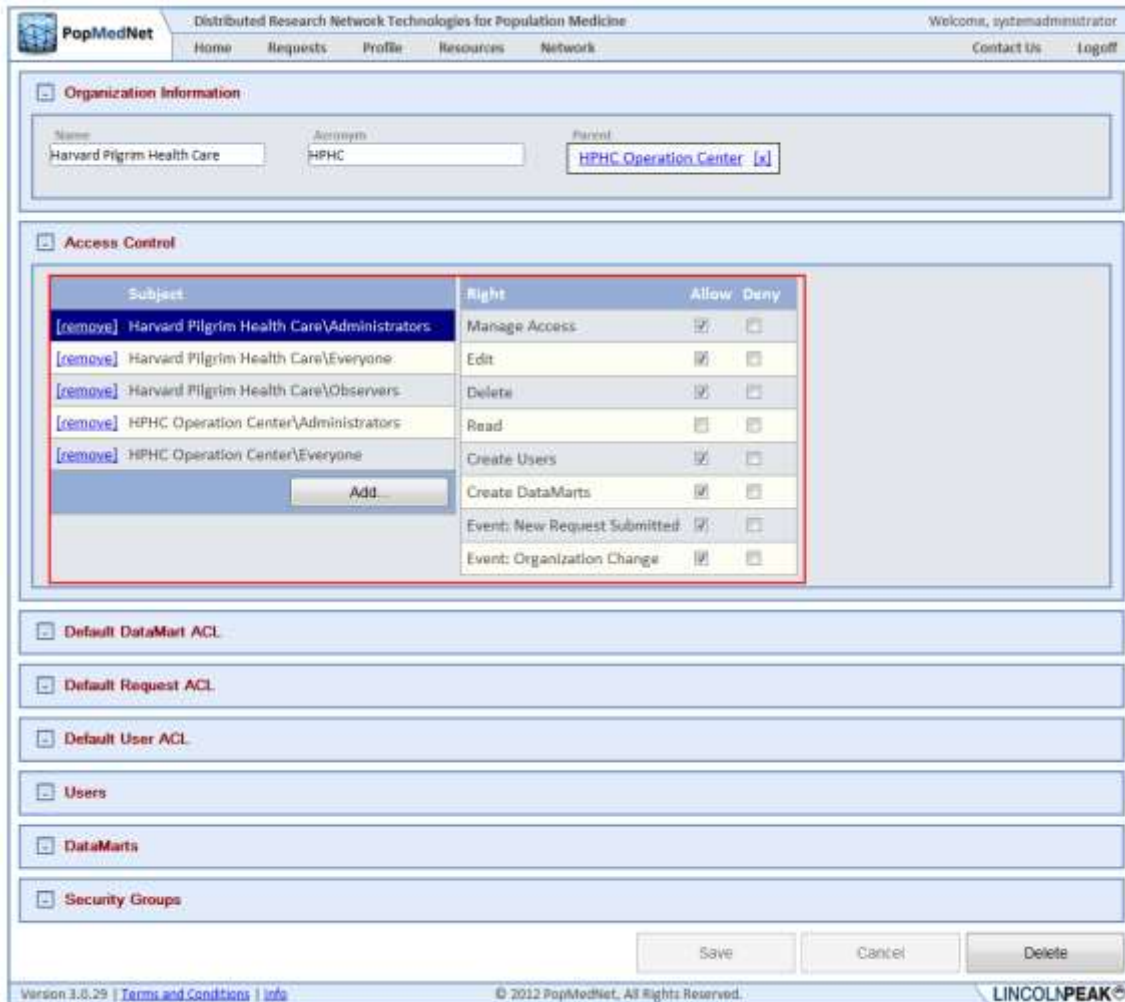
Figure 36: Organization Page – Add Organization

Once an organization is created, enter the organization's name, acronym, and parent organization or "None" if this is a root organization.

5.3   Controlling Access to Organizations and their Users and DataMarts

Use the Access Control panel to allow access to features within the organization as shown in the following figure:

Figure 37: Organization Profile Page – Organizational Rights

There are sections to allow defaults to be set for Users and DataMarts that are members of the organization as shown in the following figure:
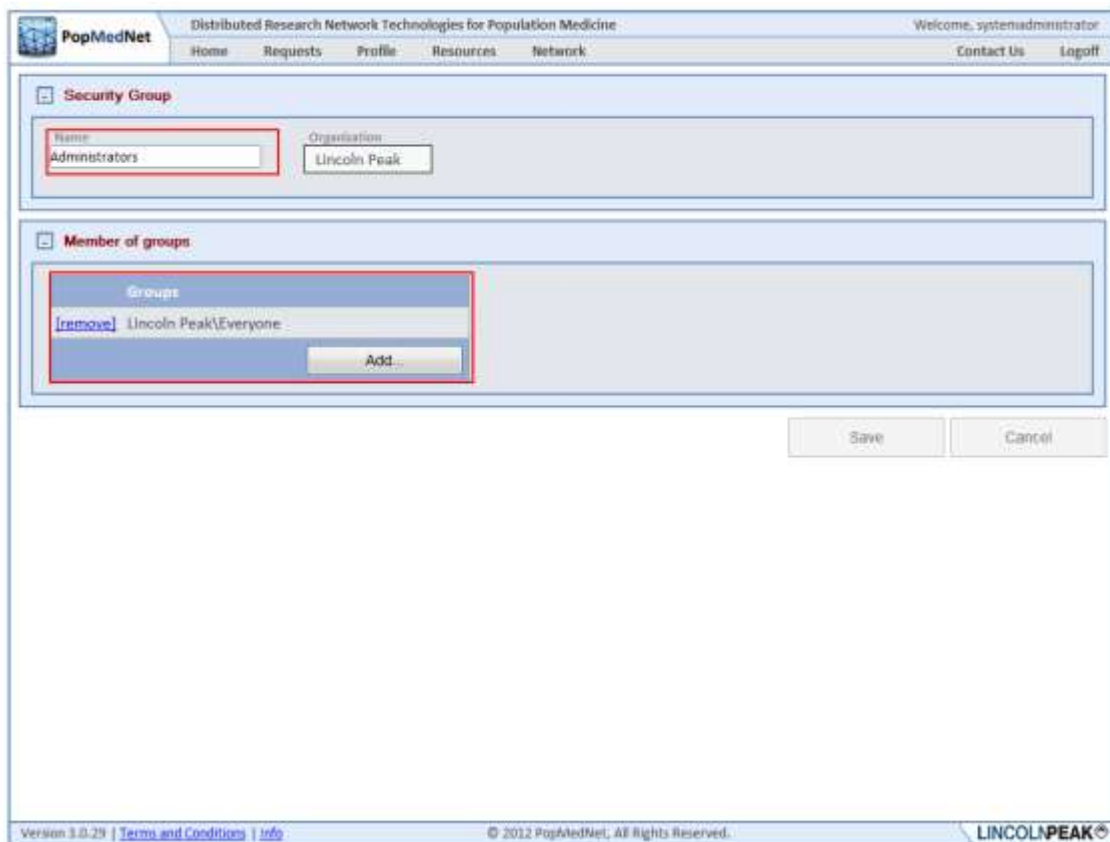
Figure 38: Organization Profile Page – Organizational Rights

The Default DataMart ACL and Default User ACL settings apply to DataMarts and Users owned by this organization and any sub-organization. The Default Request ACL settings apply to requests submitted by users of the organization or its sub-organizations. The default settings may be overridden at a lower level organization or by user.

5.4   Configuring an Organization's Security Groups

Each Organization is created with a set of built-in Security Groups. These groups may be edited to change their name or to add membership to other security groups by clicking on the group name.
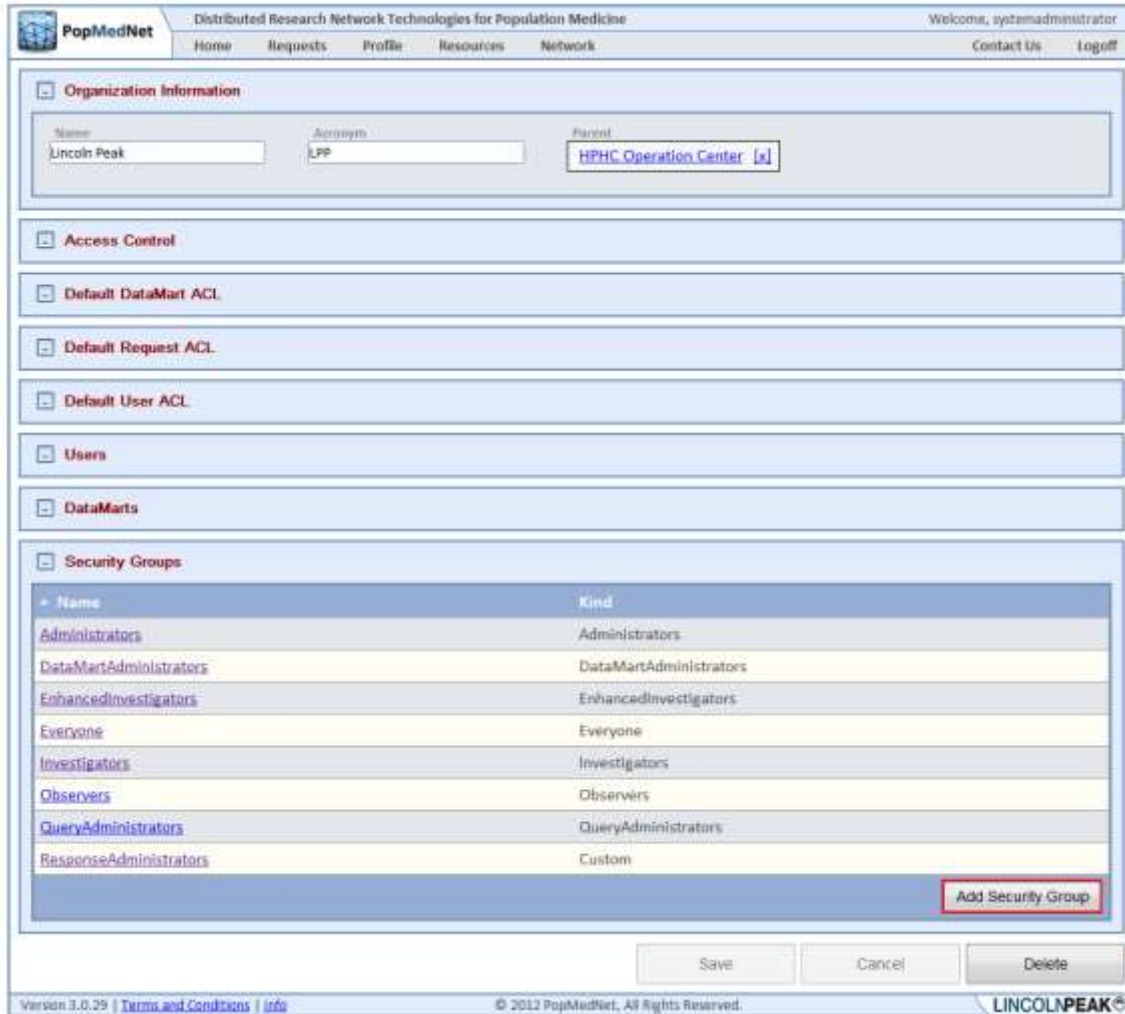
Figure 39: Organization Security Group Detail Page

Adding membership to other security groups allows the member group to inherit the rights of the added group. Custom groups may be created by clicking Add Security Group button:

Figure 40: Organization Profile Page – Add Organization Security Group

Custom security groups behave like built-in security groups. Once the organization is configured, Users and DataMarts may be added to the organization by either clicking the Add button in the DataMarts list panel or Users list panel respectively.

Figure 41: Organization Profile Page – Add Organization Users and DataMarts

Alternatively, DataMarts and Users can be added off the Network/DataMarts and Network/Users lists, respectively.

Figure 42: DataMart Page – Add DataMarts

Figure 43: User Page – Add Users

The details of adding DataMarts and Users are discussed in the next two sections.

5.5 Managing DataMarts

DataMarts represent Data Partners who respond to requests issued by investigators. DataMarts are created at the Portal and administered by users with the DataMart Client desktop application as mentioned in the overview section at the beginning of this document. DataMarts are owned by a single organization. There may be one or more users with rights to administer the DataMart.

5.6 Viewing and Creating DataMarts

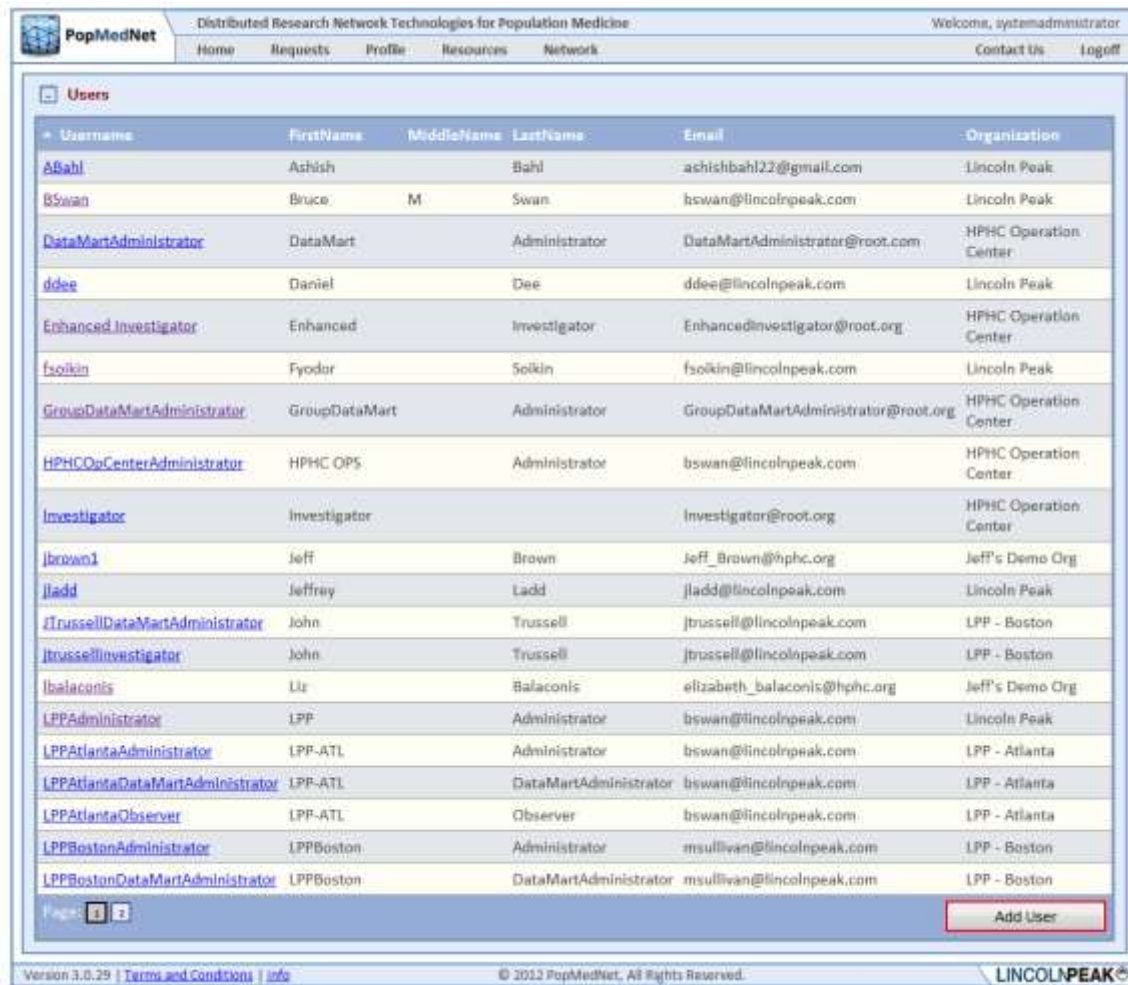There are a set of access rights that determine whether users can view, create, edit, and delete DataMarts. These rights may be applied at the global level, within the DataMart's organization detail page, or in the DataMart detail page. The following figure shows the global access rights to manage DataMarts for the entire network for the HPHC Operation Center Administrator's security group.

Figure 44: Network Access Page – Global Default DataMart Permissions

Before anyone can create a DataMart, the "Create DataMarts" access right in the Access Control panel of the Organization that will own the DataMart needs to be granted to administrators.

Figure 45: Organization Profile Page – Create DataMarts Rights

A DataMart may be created by clicking the Create DataMart button in the owning organization's detail page or by navigating to the list of all DataMarts via Network/DataMarts menu as shown in the following figures.

Figure 46: Organization Profile Page – Add DataMart

Figure 47: DataMarts Page – Add DataMart

Once created, the DataMart is configured by entering a DataMart name, acronym, and parent organization that owns the DataMart, along with other information, such as contact information, that is visible to users who navigate to it via the Portal.

Figure 48: DataMart Profile Page – DataMart Info Panel

5.7   Installing Request Models

Once the DataMart is created, the Access Control rights may be set, including the right to install or uninstall request model plug-ins as shown in the following figure.

Figure 49: DataMart Profile Page – Install and Uninstall Model Rights

Each DataMart may support one or more of the Request Models. As was mentioned in the PopMedNet™ overview, a Request Model contains one or more request types that may be composed and routed to one or more DataMarts for execution. If a DataMart supports a request model plug-in, then it must be installed by clicking the "Install …" button before configuring access to its requests for it. The following figure shows a number of request models that have been installed.

Figure 50: DataMart Profile Page – Installed Models Panel

5.8　Granting Access to Route Requests to a DataMart

Once the request model is installed, the access rights to route the request to the DataMart become visible in the Request ACL panel allowing the administrator can grant access to route them to the DataMart for execution. The following figure shows granting access to the MFU Summary Queries to a group of Investigators.

Figure 51: DataMart Profile Page – Model Request Rights

5.9   Administering a DataMart

DataMarts may be administered by one or more users, referred to as DataMart Administrators. The following figure shows the access rights that need to be granted to allow a user or group of users the ability to administer the DataMart.

Figure 52: DataMart Profile Page – Model Request Submission Rights

As shown in the figure, the DataMartAdministrators group is granted the right to view the request queue in the DataMart client application, execute the request, approve or reject it, and upload responses to the request. Additionally, the group has been granted access to run Audit Reports against the DataMart and to issue test queries to themselves without requiring approval.

5.10   Managing Users

User accounts in PMN determine the ability of the user to login and perform functions within the Portal and DataMart client. Each user is assigned a set of credentials, and optionally a X.509 certificate, used to authenticate the user. Additionally users as granted access rights directly or indirectly through inheritance or security groups as discussed in previous sections.

5.11   Create a User Account

Users must belong to a single organization, so once that organization is created, its users may be added to it. Administrators are granted access to add and modify user accounts via the Default User ACL panel in either the user's organization detail page or the Network/Access Control page.

Figure 53: Organization Profile Page – Manage User Rights

NOTE: Users always have the right to edit their contact information, notifications, and user password.

For administrators who have rights to create users, the user may be added via the Users panel on the Organization's detail page, or by navigating the Network/Users menu to list all users in PMN, by clicking the "Add User" button.

Figure 54: Organization Profile Page – Add User

Adding a user displays a blank User Detail form. The following sections describe the panels on this form.

5.12 User Contact Information

The Contact Information provides the user's name, email address, phone number, and the user's parent organization. Optionally, there's a field used to upload the user's X.509 certificate describes in a later section.

Figure 55: User Profile Page – Contact Information Panel

5.13 User Credentials

The user credentials consist of a Username and Password. The username must be unique across the network. The password must be at least 7 characters long and consist of at least one number, one symbol, and at least one upper case character. Users always have the rights to modify their password at any time. Password expire periodically based on a network-wide settings described in the Network Configuration section below.

Figure 56: User Profile Page – Credentials Panel

5.14 User Security Group Membership

Users belong to a single organization, but can take on multiple roles through membership in Security Groups. Administrators with access rights to manage user access control may select one or more security groups for which the user is a member. Membership grants the user all the rights in each security group added, as well as security groups for which the group is a member.
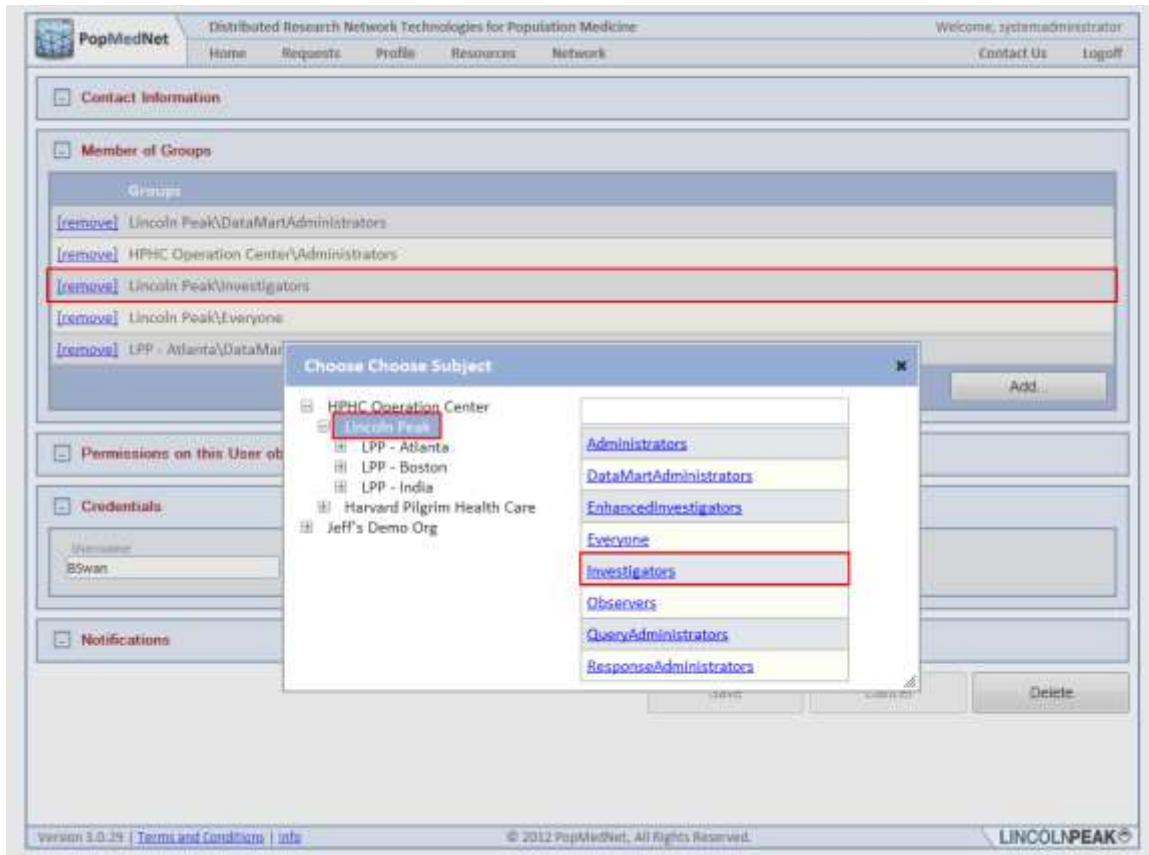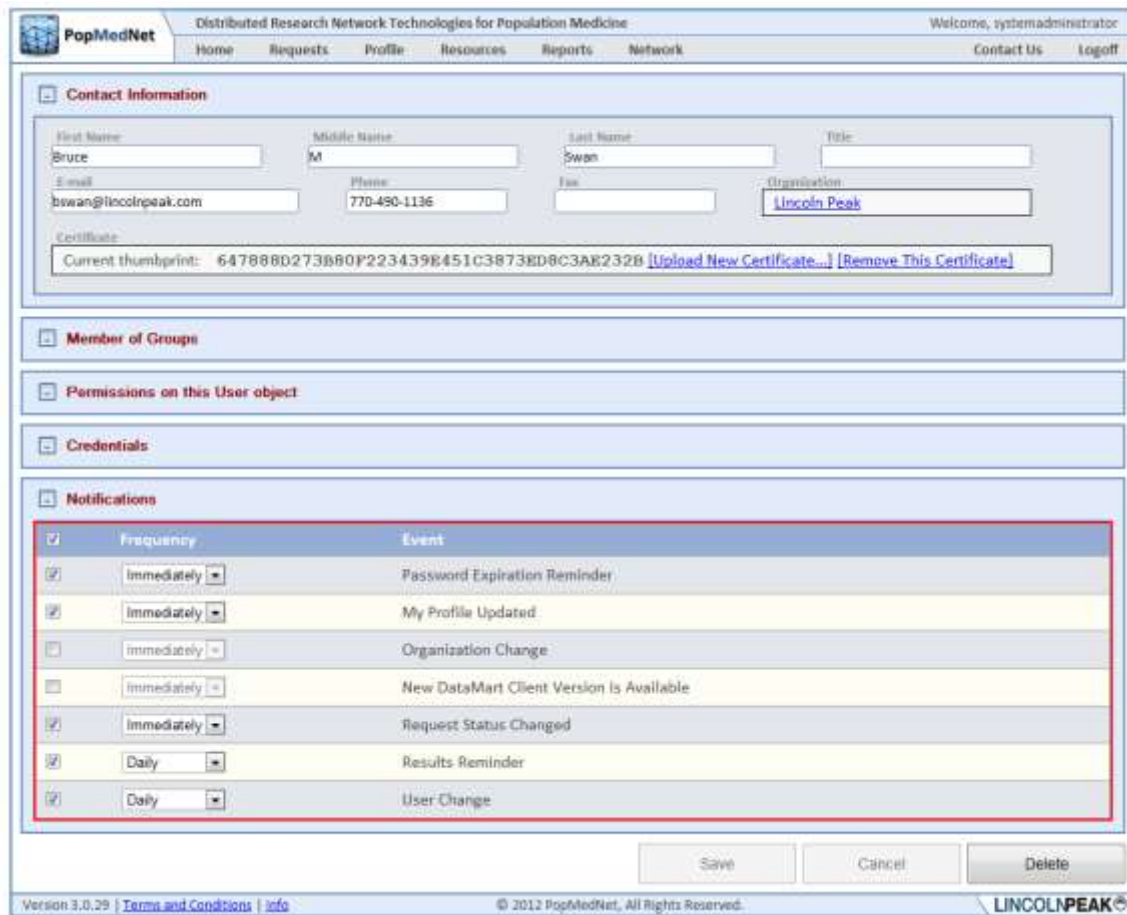
Figure 57: User Profile Page – Membership Panel and Dialog

Typically, users don't have the access rights to modify their own security profile. This right is intended for either site-wide "Root" administrators or administrators who are members of the user's organization.

5.15 Notification Options

Notification options allow the user to manage events that are triggered due to actions performed by the user or related to the user's role, such as a DataMart Administrator who is notified of an incoming requests created by other users. Users have the option of receiving notifications immediately when they are triggered, daily, weekly, or monthly. When choosing daily, weekly, or monthly, the notifications are batched together with other notifications on the same schedule in a single email.

Figure 58: User Profile Page – Notifications Panel

Note: Once the user has chosen to receive notifications, no matter what delivery frequency is selected, the notifications are displayed in the Notifications panel on the Home page.

5.16 Notification Event Reference

The following table lists each event that may be created in PMN along with a description.

Table 9: Notifications

Category	Event	Description
User	Password Expiration Reminder	Notifies the user that their password is about to expire.
	My Profile Change	Notifies the user there was an update to their profile.
	User Change	Notifies administrators there was a user added, deleted, or updated.
	New User Registration Submitted	Notifies administrators a new user request has been submitted.
	Registration Change	Notifies administrators there has been a change to a user registration request.

Category	Event	Description
Requests	New Request Submitted	Notifies DataMart administrators that a new request has been submitted.
	Request Status Changed	Notifies investigators and administrators that a change has been made to a request.
	Request Reminder	Reminds DataMart administrators there is a pending request that requires their attention.
	Results Reminder	Reminds administrators and investigators that results have been uploaded for their request.
	Results Viewed	Notifies administrators that a result has been viewed.
Organization	Organization Change	Notifies administrators that an organization has been added, updated, or deleted.
Group	Group Change	Notifies administrators that a group has been added, updated, or deleted.
DataMart	New DataMart Client Version is Available	Notifies DataMart administrators that a new version of the DataMart Client application is available.
	DataMart Change	Notifies administrators that a DataMart has been added, updated, or deleted.

5.17 Using X.509 Certificates

PopMedNet™ Release 3 introduced a security feature that uses a 2-factor authentication technique over a TLS secure connection to authenticate DataMart Administrators using the DataMart Client application. 2-factor authentication is an approach to authentication which requires the presentation of two or more of the three authentication factors: a *knowledge* factor ("something the user *knows*"), a *possession* factor ("something the user *has*"), and an *inherence* factor ("something the user *is*"). In the case of PopMedNet™, the user has a X.509 certificate installed on their machine and knows the password to their account which are both used together to authenticate the user.

Secondly, through the use of trusted client certificates, the connection PMN to DataMart connection is mutually authenticated. The following figure illustrates how this process is performed.
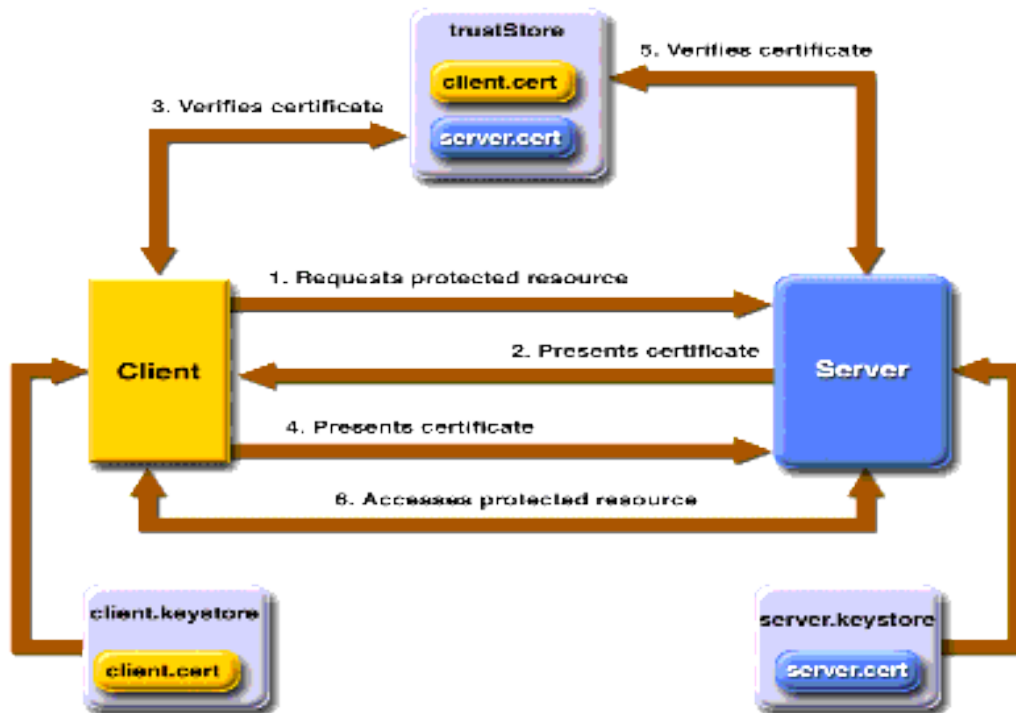
Figure 59: Mutual Authentication Scheme

In certificate-based mutual authentication, the following things occur:

1. A client requests access to a protected resource.
2. The web server presents its certificate to the client.
3. The client verifies the server's certificate.
4. If successful, the client sends its certificate to the server.
5. The server verifies the client's credentials.
6. If successful, the server grants access to the protected resource requested by the client.

To enable use of X.509 certificates, each DataMart administrator is issued a certificate that is issued by a certificate authority (CA) that is trusted by the PMN web server. The user installs the certificate in their local machine running the DataMart Client application, and uploads the certificate (in .CER format) to their user account as shown in the following figure:
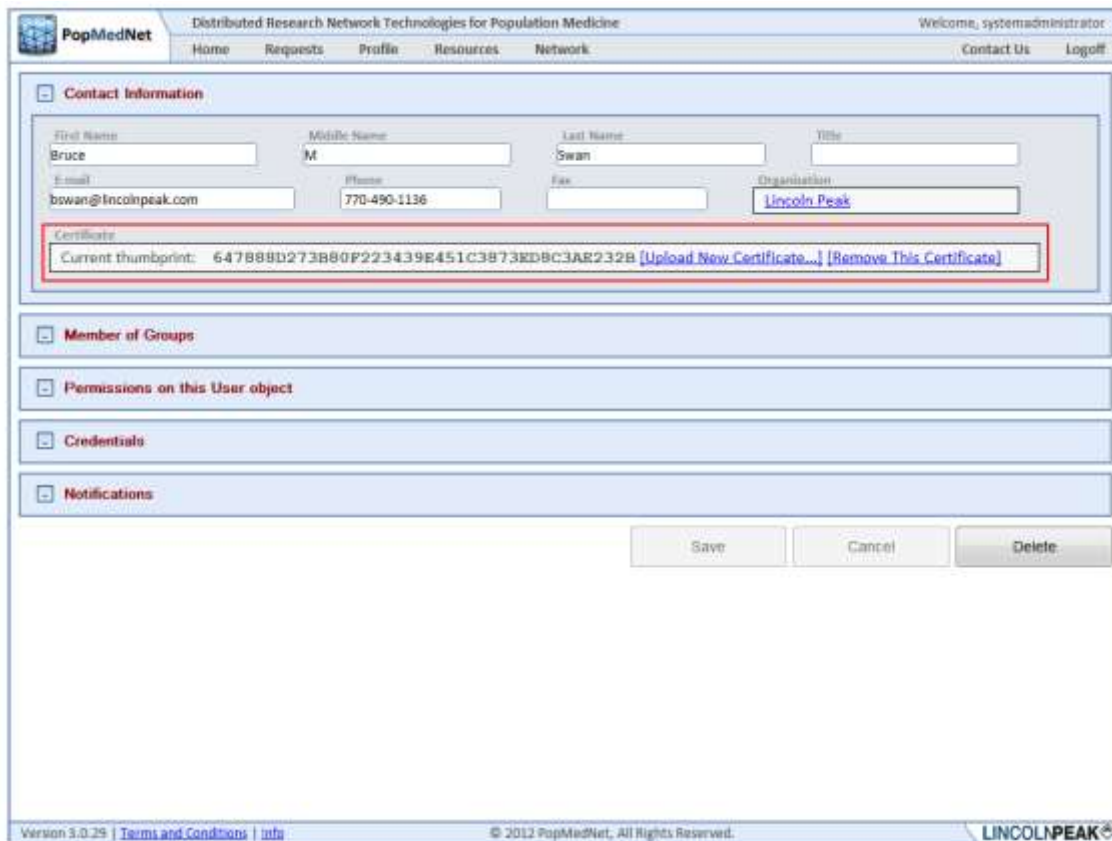
Figure 60: User Profile Page – X.509 Certificate Upload

This process associates the user's certificate thumbprint with the user's account used to validate the user during the authentication process.

5.18 Managing Groups

Groups are a collection Organizations that allow administrators to establish permissions and workflow across organizations that are not physically related. A Group may have one or more Organizations and an Organization may be a member of multiple groups. Groups allow the formation of **Sub-Networks**.

Sub-Networks allow deployment and operation of activities that can be isolated and managed within a secure environment through access control settings. For instance, there are a number of PopMedNet™ sites operating under PopMedNet™ Release 2. These sites could be hosted under a single network instance using groups to maintain their independence, security, and isolation among other sub-networks.

NOTE: The implementation of Groups is not complete in PopMedNet™ Release 3.1. This feature will be completed in a future release of PopMedNet™.

5.19 Viewing and Creating Groups

Groups can be added by navigating to the Network/Groups list page and clicking the "Add Group" button.
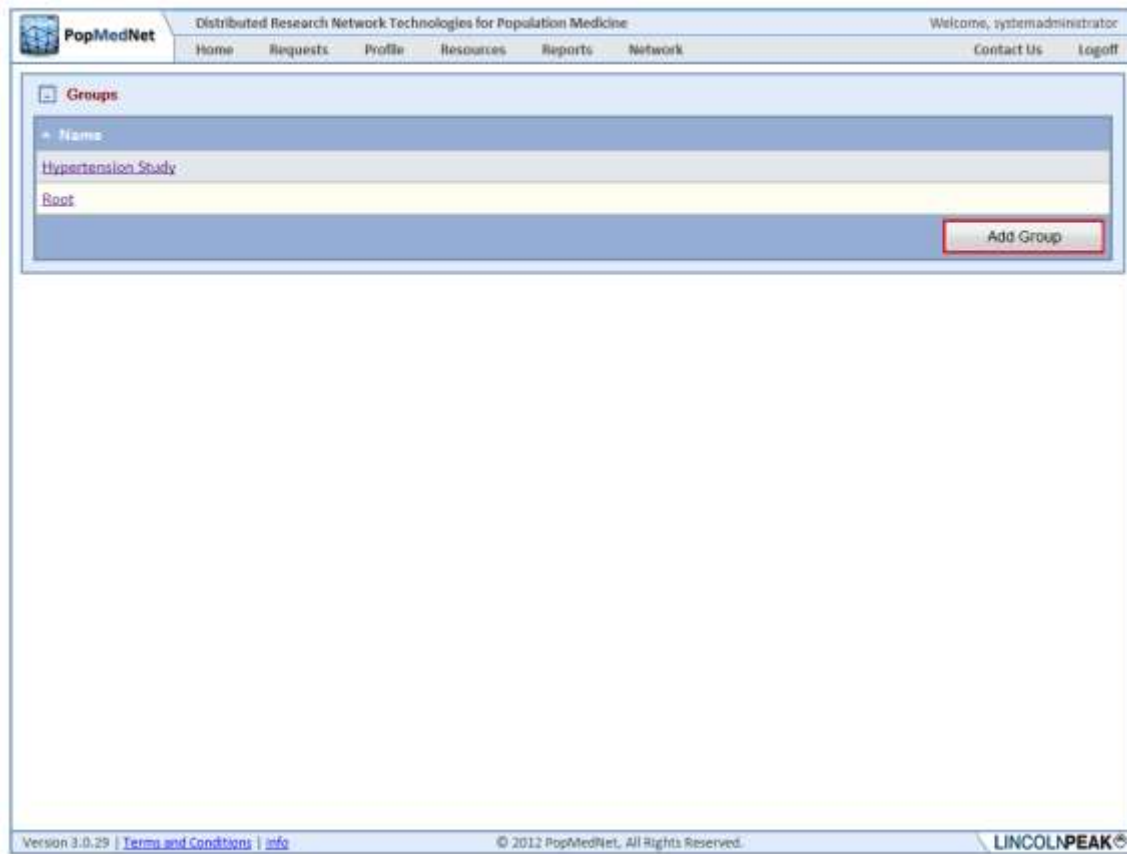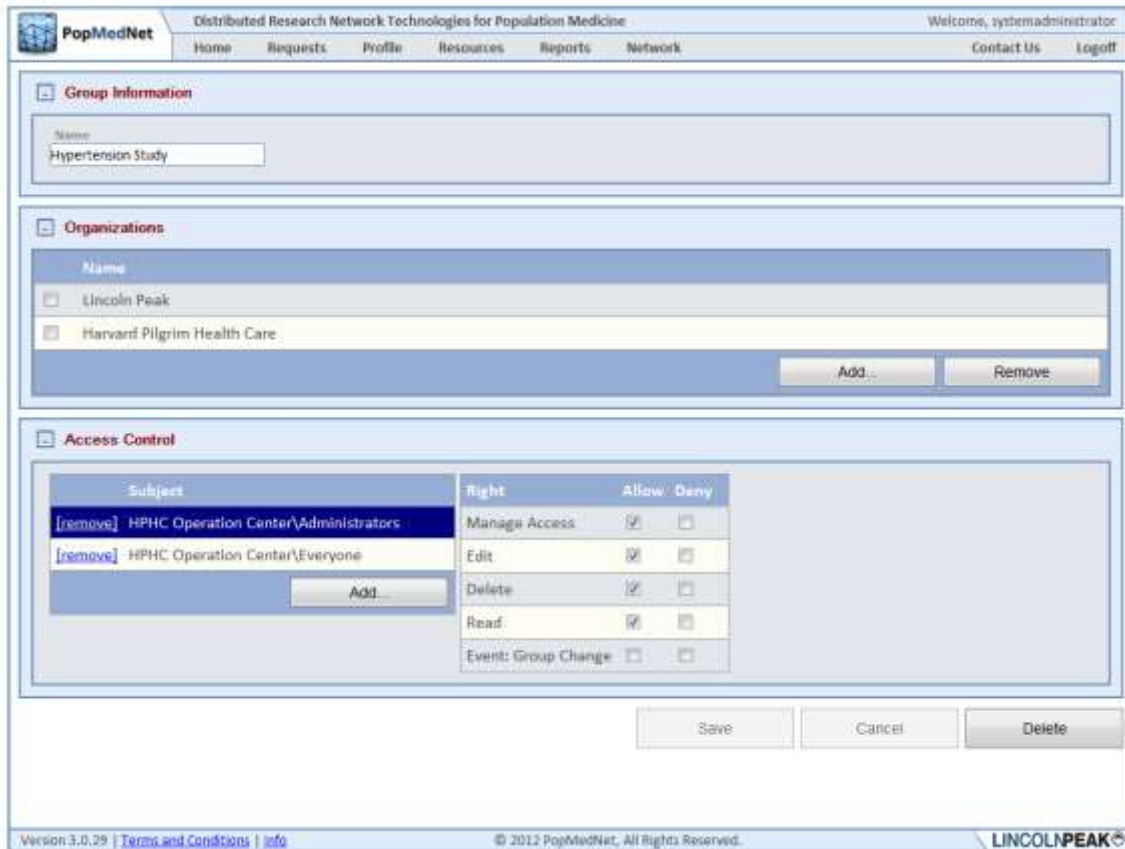
Figure 61: Group Page – Add Group

This displays the Group detail page shown in the following figure.

Figure 62: Group Profile Page

5.20 Managing Projects

One of the major enhancements in PMN R3.2 is the introduction of Projects. A project establishes security policies for composing, reviewing, and executing requests by users and DataMarts assigned to the project. Projects are created within an organizational group. Groups have one or more member organizations whose users and DataMarts may participate within projects owned by the group. The following figure shows a Group detail page along with a Group and Organizational structure displayed in the PMN Network Browser control.
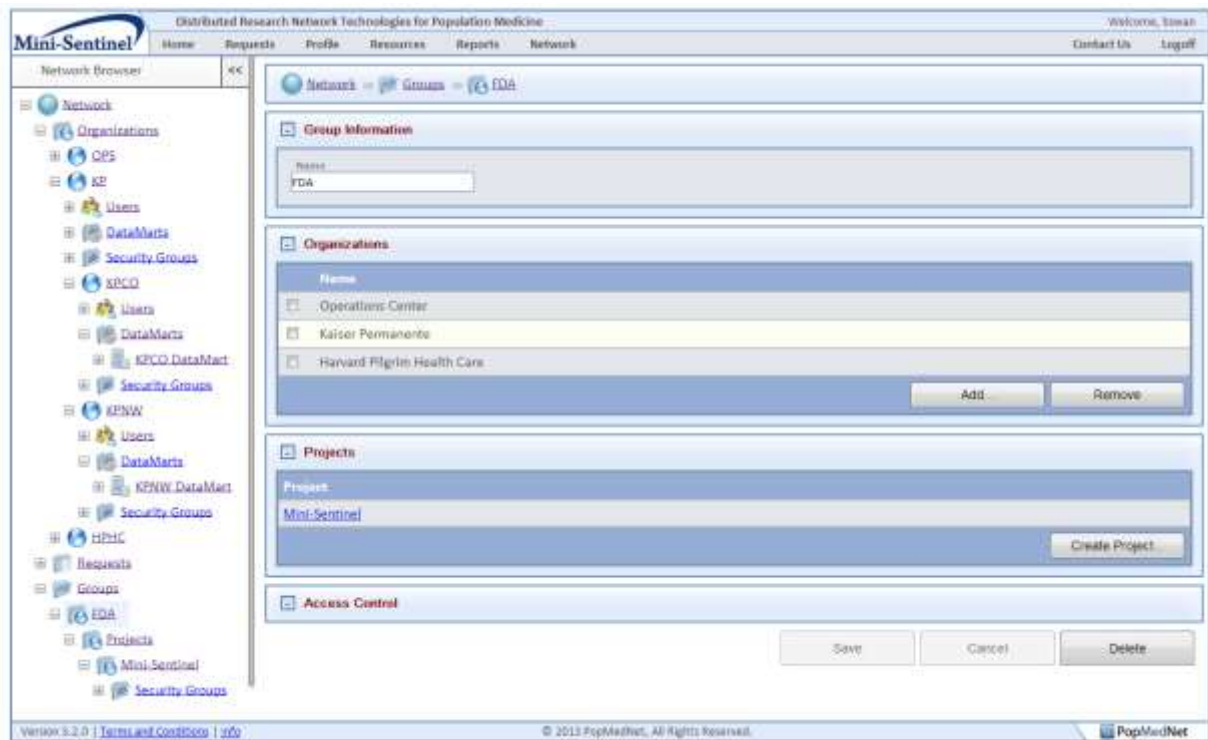
Figure 63: Group Profile Page

In this sample network, there is a single Group called FDA that contains three member organizations and a single project called Mini-Sentinel. Only users and DataMarts defined in each of the member organizations; Operations Center, Harvard Pilgrim Health Care, and Kaiser Permanente including its sub-organizations, may participate in Mini-Sentinel project owned by the FDA group.

Network administrators or users, such as Group and Project administrators, who have rights to modify and administer projects may grant access to a project and configure its security policies. Once a project is configured, users may begin submitting requests within the context of the project. See the PopMedNet Investigator's Manual for information on submitting requests within projects.

5.20.1   Creating a Project

Once a group is created one or more projects may be created by clicking the "Create Project" button in the Projects panel on the Group Profile Page displayed above.

5.20.2   Configuring Access Control

When the project is created, the administrator may configure the access control on the project that determines the policies in force for the project. The following figure shows a project detail page used to configure the security policies affecting users and DataMarts assigned to the project.

Figure 64: Project Profile Page

5.20.2.1 Project Information

The Project Information panel is used to enter a profile for the project; the project name, description, start and stop dates. The project start and end dates determine when a request may be issued within the project. Additionally, a project can be put on hold by removing the checkmark in the "Allow to submit requests to this project" checkbox.

5.20.2.2 Access Control

The Access Control panel allows the user to configure the base Access Control Lists (ACLs) for the project. The following table describes the rights for that may be granted to users or security groups for the project or the organizations who are members of the project's parent group.

Table 10: Project Access Controls

Right	Description
Manage Access	Allow editing ACLS for the project
Edit	Allow editing the project
Delete	Allow deletion of the project
Read	Allow viewing the project (note this right minimally allows users the ability to view the project profile, and the project organizations and DataMarts participating in the project)
List Requests	Allow project requests to be displayed in the requests grid on the home page or project tab
Event: New Request Submitted	Allow subscription to the "New Request Submitted" event that notifies the user whenever a new request has been submitted to the project
Event: Project Change	Allow subscription to the "Project Change" event that notifies the user whenever there has been a change to the project settings
Event: Project Assignment	Allow subscription to the "Project Assignment" event that notifies the user whenever an assignment has been made within the project

5.20.2.3 Default DataMart ACL

The Access Control panel allows the user to configure default ACLs for all DataMarts assigned to the project. The following table describes the rights for that may be granted to users or security groups for the project or organizations who are members of the project's parent group.

Table 11: Project DataMart Access Controls

Right	Description
See Request Queue	Allow viewing project requests issued to the DataMart within the DataMart Client application
Upload Results	Allow executing and uploading results for project requests issued to the DataMart within the DataMart Client application
Hold Requests	Allow holding project requests issued to the DataMart within the DataMart Client application
Reject Requests	Allow rejecting project requests issued to the DataMart within the DataMart Client application

Right	Description
Approve/Reject Responses	Allow review and approval of results uploaded by administrators within the DataMart Client application
Skip Response Approval	Allow results uploaded by administrations within the DataMart client application to be available to the submitter without review and approval
Group/Ungroup Responses	Allow users who review and approve results uploaded by administrators within the DataMart client application the ability to group multiple DataMart results into a single group or ungroup previously grouped results
Event: Uploaded Results Needs Approval	Allow subscription to the "Uploaded Results Needs Approval" event that notifies the user whenever a result has been uploaded that requires their approval

5.20.2.4 Request Types ACL

The Access Control panel allows the user to configure default ACLs for Request Types issued by users assigned to the project. The following table describes the rights for that may be granted to users or security groups for the project or organizations who are members of the project's parent group.

Table 12: Project Request Type Access Controls

Right	Description
Request Type Name (e.g. Pharmacy Dispensings By Generic Name, ICD-9 Diagnosis, ICD-9 Procedures, etc)	Allow user the right to issue a specific request type within the project. The list of rights displayed within this panel is dependent on the plug-ins installed in the DataMarts assigned to the project. Each plug-in may expose one or more request types for which the administrator may grant users the right to compose a request of the given type and submit it to authorized DataMarts. The administrator has the ability to determine whether the user has the right to execute the request Manually or Automatically when it is processed by the DataMart. Requests that are authorized to be processed automatically will do if and only if the given DataMart has been set to process requests automatically through the Automatic mode settings enabled at the DataMart.

5.20.2.5 Default Request ACL

The Access Control panel allows the user to configure default ACLs for all requests issued within the project. The following table describes the rights for that may be granted to users or security groups for the project or organizations who are members of the project's parent group.

Table 13: Project Request Access Controls

Right	Description
Edit	Allow editing requests assigned to the project
Delete	Allow deleting requests assigned to the project
Read	Allow viewing requests assigned to the project
Change Routings After Submission	Allow the ability to change the DataMart routings after the request has been submitted

Right	Description
View Submitted Requests Status	Allow viewing the requests detail DataMart status once it's been submitted
Approve/Reject Submission	Allow reviewing and approving requests submitted within the project that require approval
Skip Request Approval	Allow requests to be submitted to the project without requiring approval
View Results	Allow viewing the results for requests submitted within the project
View Individual Results	Allow viewing individual DataMart results for requests submitted within the project
View History	Allow viewing the history for requests submitted within the project
Event: Request Status Changed	Allow subscription to the "Request Status Changed" event that notifies the user whenever the status of a request is changed
Event: Submitted Request Needs Approval	Allow subscription to the "Submitted Request Needs Approval" event that notifies the user whenever a request has been submitted that requires their approval
Event: Results Viewed	Allow subscription to the "Results Viewed" event that notifies the user whenever a result has been viewed by users who have the right to view results
Event: Results Reminder	Allow subscription to the "Results Reminder" event that notifies the user whenever a result has been uploaded for which the user has rights to view. Note that the reminders are repeated based on a network wide interval until the user has viewed the result

5.20.2.6 Security Groups

The Security Groups panel lists the security groups defined by the project. A default set of groups is created when the project is created. These may be edited to alter the membership of a group and new groups may be created. The following table lists the default groups that are created.

Table 14: Project Security Groups

Security Group	Description
Administrators	Users who have rights to administer the project
DataMartAdministrators	Users who have rights to administer one or more DataMarts
EnhancedInvestigators	Users who have the rights to submit requests and view individual results
Everyone	Users who are members of the project
Investigators	Users how have the rights to submit request and view results
Observers	Users how have the rights to monitor requests being issued within the project and the processing of those requests
QueryAdministrators	Users who have the rights to Review and Approve requests

5.20.2.7 DataMarts

The DataMarts panel displays DataMarts that have been assigned to the project. Note that only DataMarts that are defined by organizations who are members of the project's parent group may be assigned to the project. Once assigned, the administrator may click the "ACL" link to

modify the access control lists for the use of the given DataMart within the context of the project. Note that DataMarts may be assigned to a project by default by ACLs within the DataMart detail page. Additionally, specific rights may be defaulted by ACLs configured in the project's Default DataMart panel described above or configured in the DataMarts detail page. The following figure displays the rights that may be assigned for each DataMart.

Figure 65: Project-Specific DataMart ACL

As was described above, administrators may use these ACLs to define rights in force for a given DataMart within the project including overriding the default or inherited rights.

5.20.2.8 Organizations

The Organizations panel displays organizations that have been assigned to the project. Note only Organizations who are members of the project's parent group may be assigned to the project. Once assigned, the administrator may click the "ACL" link to modify the access control lists for the given organization within the context of the project. Note the rights listed in the project organization panel may have default assignments granted within project based on the projects ACLs described above or through the organizations detail page. The following figure displays the rights that may be assigned for an organization assigned to the project.

Figure 66: Project-Specific Organizational ACL

5.20.3 Adding Users to Projects

Once the project has been configured, administrators may assign users to the project. This is performed by modifying the user's security group membership displayed in the user profile page. The following figure shows a user who has been granted rights to participate within the project.

Figure 67: User Profile Page - Security Group Membership Panel

In the figure above, the user has been modified to participate in sample Mini-Sentinel project as an Administrator, Enhanced Investigator, and a DataMart Administrator. These assignments grant the user rights granted to these security groups within the Mini-Sentinel project detail page as described in the sections above.

6   Technology Stack

PopMedNet™ is built on a Microsoft .NET 4 platform using best practices to ensure an extensible, scalable, and secure application. The following table lists the technology used:

Table 15: Technology Stack

OS / Application / Component	Description
Portal Operating System	Microsoft Windows Server 2008 R2
Website Manager	Microsoft Internet Information Server 7 (MS/IIS)
DataMart Web Services	Microsoft Windows Communication Foundation (REST or SOAP)
Portal Database Engine	Microsoft SQL Server 2008 R2
Plug-in Web Services	Microsoft Windows Communication Foundation (REST or SOAP)
Portal Webpage Framework	Microsoft ASP.NET MVC 3 with jQuery web client
Plug-in Framework	Microsoft Managed Extensibility Framework (MEF)
Object Relational Mapping Framework	Microsoft Entity Framework 4.2 (EF)
Scheduling Service	Quartz Scheduler (Open source)
DataMart Client Application Operating System	Microsoft XP, Vista, Windows 7
DataMart Client Application	Microsoft .NET 4 / C#
DataMart Model Processor Framework	Microsoft .NET 4

7   Configuration Settings

The following sections describe the settings used to configure the Portal site.

7.1   Web Configuration File Settings

The following are parameters that can be set within the PopMedNet™ web server application configuration file:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <configSections>
    <section name="entityFramework"
             type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSect
             ion, EntityFramework, Version=4.3.1.0, Culture=neutral,
             PublicKeyToken=b77a5c561934e089" />
    <section name="quartz" type="System.Configuration.NameValueSectionHandler,
             System, Version=1.0.5000.0,Culture=neutral,
             PublicKeyToken=b77a5c561934e089" />
    <section name="log4net"
             type="log4net.Config.Log4NetConfigurationSectionHandler,
             log4net" />
  </configSections>
  <quartz>
    <add key="quartz.scheduler.instanceName" value="ServerScheduler" />
    <!-- Configure Thread Pool -->
    <add key="quartz.threadPool.type" value="Quartz.Simpl.SimpleThreadPool,
```

```
                Quartz" />
    <add key="quartz.threadPool.threadCount" value="10" />
    <add key="quartz.threadPool.threadPriority" value="Normal" />
    <!-- Configure Job Store -->
    <add key="quartz.jobStore.type" value="Quartz.Impl.AdoJobStore, Quartz" />
    <add key="quartz.jobStore.dataSource" value="default" />
    <add key="quartz.jobStore.tablePrefix" value="QRTZ_" />
    <add key="quartz.jobStore.clustered" value="true" />
    <add key="quartz.jobStore.lockHandler.type"
            value="Quartz.Impl.AdoJobStore.UpdateLockRowSemaphore, Quartz" />
    <add key="quartz.jobStore.driverDelegateType"
            value="Quartz.Impl.AdoJobStore.SqlServerDelegate, Quartz" />
    <add key="quartz.dataSource.default.connectionString" value="data
            source=.;initial catalog=quartz;integrated
            security=True;MultipleActiveResultSets=True" />
    <add key="quartz.dataSource.default.provider" value="SqlServer-20" />
    <add key="quartz.jobStore.useProperties" value="true" />
    <add key="quartz.jobStore.misfireThreshold" value="60000" />
    <add key="quartz.scheduler.proxy" value="true" />
    <add key="quartz.scheduler.proxy.address"
            value="tcp://127.0.0.1:555/QuartzScheduler" />
</quartz>
<system.net>
  <mailSettings>
    <smtp deliveryMethod="" from="admin@dns3.local">
      <specifiedPickupDirectory pickupDirectoryLocation="c:\work\mail" />
      <network host="localhost" />
    </smtp>
  </mailSettings>
</system.net>
<appSettings>
  <add key="CurrentTheme" value="FDA" />
  <add key="ContactUsEmail" value="msullivan@lincolnpeak.com" />
  <add key="ConfiguredPasswordExpiryMonths" value="6" />
  <add key="PasswordExpirationNagDaysPrior" value="7" />
  <add key="PasswordExpirationNagPeriodDays" value="1" />
</appSettings>
<connectionStrings>
  <add name="Lpp.Dns.Model.DnsDomain" connectionString="data source=.;initial
            catalog=DNS3;integrated
            security=True;MultipleActiveResultSets=True;Connection Timeout=60"
            providerName="System.Data.SqlClient" />
  <add name="Lpp.Dns.HealthCare.HealthCareDomain" connectionString="data
            source=.;initial catalog=DNS3;integrated
            security=True;MultipleActiveResultSets=True;Connection Timeout=60"
            providerName="System.Data.SqlClient" />
  <add name="Lpp.Dns.HealthCare.Summary.SummaryDomain" connectionString="data
            source=.;initial catalog=DNS3;integrated
            security=True;MultipleActiveResultSets=True"
            providerName="System.Data.SqlClient" />
  <add name="Lpp.Dns.RedirectBridge.RedirectDomain" connectionString="data
            source=.;initial catalog=DNS3;integrated
            security=True;MultipleActiveResultSets=True"
            providerName="System.Data.SqlClient" />
  <add name="Lpp.Dns.HealthCare.ESPQueryBuilder.Data.ESPDomain"
            connectionString="data source=.;initial catalog=DNS3;integrated
            security=True;MultipleActiveResultSets=True"
            providerName="System.Data.SqlClient" />
```

```xml
    <add name="Lpp.Dns.HealthCare.FileDistribution.Data.FileDistributionDomain"
            connectionString="data source=.;initial catalog=DNS3;integrated
            security=True;MultipleActiveResultSets=True;Connection Timeout=60"
            providerName="System.Data.SqlClient" />
</connectionStrings>
<system.web>
  <httpRuntime maxRequestLength="32384" />
  <compilation debug="true" targetFramework="4.0">
    <assemblies>
      <add assembly="System.Web.Extensions.Design, Version=4.0.0.0,
                    Culture=neutral, PublicKeyToken=31BF3856AD364E35" />
      <add assembly="System.Design, Version=4.0.0.0, Culture=neutral,
                    PublicKeyToken=B03F5F7F11D50A3A" />
      <add assembly="System.Windows.Forms, Version=4.0.0.0, Culture=neutral,
                    PublicKeyToken=B77A5C561934E089" />
      <add assembly="System.Web.Abstractions, Version=4.0.0.0, Culture=neutral,
                    PublicKeyToken=31BF3856AD364E35" />
      <add assembly="System.Web.Helpers, Version=1.0.0.0, Culture=neutral,
                    PublicKeyToken=31BF3856AD364E35" />
      <add assembly="System.Web.Routing, Version=4.0.0.0, Culture=neutral,
                    PublicKeyToken=31BF3856AD364E35" />
      <add assembly="System.Web.Mvc, Version=3.0.0.0, Culture=neutral,
                    PublicKeyToken=31BF3856AD364E35" />
      <add assembly="System.Web.WebPages, Version=1.0.0.0, Culture=neutral,
                    PublicKeyToken=31BF3856AD364E35" />
    </assemblies>
    <buildProviders>
      <add extension=".rdlc" type="Microsoft.Reporting.RdlBuildProvider,
                    Microsoft.ReportViewer.Common, Version=9.0.0.0,
                    Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
    </buildProviders>
  </compilation>
  <pages validateRequest="false" enableEventValidation="false"
                        controlRenderingCompatibilityVersion="3.5"
                        clientIDMode="AutoID" />
  <customErrors mode="Off" />
  <authentication mode="Forms">
    <forms name=".ASPXAUTH" loginUrl="/login" protection="All" path="/"
              timeout="30" requireSSL="false" slidingExpiration="true"
              defaultUrl="~/" cookieless="UseDeviceProfile"
              enableCrossAppRedirects="false" />
  </authentication>
</system.web>
<system.webServer>
  <validation validateIntegratedModeConfiguration="false" />
  <modules runAllManagedModulesForAllRequests="true" />
  <handlers>
    <remove name="StaticFile" />
    <add name="StaticFile" path="*" verb="GET" modules="StaticFileModule"
            resourceType="File" requireAccess="Read" />
  </handlers>
</system.webServer>
<system.serviceModel>
  <serviceHostingEnvironment aspNetCompatibilityEnabled="true"
            multipleSiteBindingsEnabled="true" />
</system.serviceModel>
<entityFramework>
  <defaultConnectionFactory
```

```
        type="System.Data.Entity.Infrastructure.SqlConnectionFactory,
        EntityFramework">
        <parameters>
          <parameter value="Data Source=.\SQLEXPRESS; Integrated Security=True;
                          MultipleActiveResultSets=True" />
        </parameters>
      </defaultConnectionFactory>
    </entityFramework>
    <runtime>
      <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
        <dependentAssembly>
          <assemblyIdentity name="Common.Logging" publicKeyToken="af08829b84f0328e"
                          culture="neutral" />
          <bindingRedirect oldVersion="0.0.0.0-2.1.1.0" newVersion="2.1.1.0" />
        </dependentAssembly>
      </assemblyBinding>
    </runtime>
    <log4net debug="false">
      <appender name="HttpTraceAppender"
                type="log4net.Appender.AspNetTraceAppender">
        <layout type="log4net.Layout.PatternLayout">
          <conversionPattern value="%date %-5level - %message%newline" />
        </layout>
      </appender>
      <appender name="RollingLogFileAppender"
                type="log4net.Appender.RollingFileAppender">
        <file value="logs\" />
        <appendToFile value="true" />
        <maxSizeRollBackups value="10" />
        <maximumFileSize value="5MB" />
        <rollingStyle value="Date" />
        <datePattern value="yyyy-MM-dd.lo\g" />
        <staticLogFileName value="false" />
        <layout type="log4net.Layout.PatternLayout">
          <conversionPattern value="%date %-5level - %message%newline" />
        </layout>
      </appender>
      <root>
        <level value="DEBUG" />
        <appender-ref ref="HttpTraceAppender" />
        <appender-ref ref="RollingLogFileAppender" />
      </root>
    </log4net>
</configuration>
```

Figure 60 – Web Configuration File

The following table describes settings that the network administrator may change.

Note: It is not recommended to change that the other settings in the configuration file.

Table 16: Configuration Parameters

Area	Setting	Description
AppSettings	CurrentTheme	Web site theme name used to pick-up satellite assemblies that override default resources
	ContactUsEmail	Email address that is used in Contact Us link in header of Portal
	ConfigurePasswordExpiryMonths	Number of months before users passwords automatically expire
	PasswordExpirationNagDaysPrior	Number of days prior the password changing before we start sending expiration notifications to the user
	PasswordExpirationNagPeriodDays	Interval between sending password expiration nag messages
ConnectionStrings	Lpp.Dns.Model.DnsDomain	Connection string for the main POPMEDNET™ database
	Lpp.Dns.HealthCare.HealthCareDomain	Connection string for the healthcare plug-in common controls database, such as the ICD-9 selectors
	Lpp.Dns.HealthCare.Summary.SummaryDomain	Connection string for summary queries database
	Lpp.Dns.RedirectBridge.RedirectDomain	Connection string for the redirect plug-ins database
	Lpp.Dns.HealthCare.ESPQueryBuilder.Data.ESPDomain	Connection string for the ESPQueryBuider database
	Lpp.Dns.HealthCare.FileDistribution.Data.FileDistributionDomain	Connection string for the File Distribution plug-in database
Quartz Scheduler	Quartz.dataSource.default.connectionString	Connection string for the Quartz scheduler database
Application Logger	<file value="logs\" />	Location of the Log4Net log file; value is set of "logs" folder off the web site root folder
Notification Mail Server	`<smtp deliveryMethod="" from="admin@dns3.local"> <specifiedPickupDirectory pickupDirectoryLocation=" c:\work\mail" /> <network host="localhost" /> </smtp>`	Specifies the SMTP server settings, from email address used in outgoing emails to users, and the location of the folder where the mail is stored

7.2   Enabling X.509 Certificate Authentication

In the Managing Users section above, the process to enable the user of X.509 certificates is described for a given user; however the PMN web server needs to install the certificates of any root certificate authorities that have issued certificates used by PMN users. This allows the web server to validate the authenticity of the user's certificate.

To install the root CA certificates, open MMC and go into the Certificate Store under the computer account. Right click the Trusted Root Certificate Authorities folder and click All Tasks > Import. Then follow the Import steps to import the Root Certificate. Lastly, if the X.509 cert was not created off of a publically known CA such as Verisign, Go-Daddy, Digicert, etc., then change the registry key
"**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\ SendTrustedIssuerList**" from 1 to 0 and restart the server.

7.3   Application Log

PopMedNet™ uses Log4Net as the logging service. The location and logging information level of the log is specified in the PopMedNet web configuration file.

8 Scheduler Service

The Scheduler Service is a separate Windows Service based on the Quartz Scheduler engine (http://quartz-scheduler.org/) that is used to manage requests scheduling, notifications, and garbage cleanup within PMN. This service is installed on an application server and configured to connect to PMN to perform its work. The Scheduler can be installed using an install package that is part of the PMN solution. Once installed, follow the readme file in the scheduler install folder for instructions on how to configure it.

9   Theming and Branding PopMedNet

PopMedNet™ may be branded and its content changed through the user of a custom theme facility that is modeled after Microsoft's satellite DLL scheme used to translate web sites into different locales. Custom assemblies are developed with the embedded resource content to be used in lieu of the default content and given the same name as the base DLL it overrides with a special theme name extension. These satellite assemblies are copied into the binary folder of the web site containing the base assemblies they override, and the theme name is set using the "CurrentTheme" parameter in the web configuration file (See web configuration section above). Whenever a page is rendered, the rendering engine looks for an override for each of the resources used on the page, and if one is found, its content is used in lieu of the base assembly. See the readme file in the Web/Themes folder of the PMN solution files for details on building satellite assemblies.

10 Hosting Technical and Security Overview

This section provides a detailed description of the hosting, security, and support features of the PopMedNet™ application that is currently supporting several networks including the FDA Mini-Sentinel, AHRQ Scalable PArtnering Network (SPAN), and State of Massachusetts Department of Public Health Network (MDPHnet).

10.1 Hosting and Support Requirements

Each network is hosted separately in the same secure environment; there are separate portals and separate implementations of the system. The next two sections describe the system hosting infrastructure and security controls.

Hosting, Security and Support for the PopMedNet™ software application is provided by LPP and consists of:
✓ Hosting that is compliant with Federal Information Security Management Act (FISMA) requirements.
✓ Hosting through the full software development lifecycle (including design, implementation, unit testing, user acceptance testing and preparation for production).
✓ Deploying the system into production environment.
✓ Supporting all production versions of the applications.
  • This involves monitoring and maintaining the application and its operating environment as well as effectively responding to technical questions and issues encountered by the users.

The general requirements and detailed requirements are in Table 17 and 18:

Table 17: Hosting, Security & Support: General Requirements

Requirement	Description
General Requirements	
Multiple Hosting Environments	Separate Development / QA / UAT (User Acceptance Testing) and Production hosting environments are required to isolate active data partners from implementation and testing work being performed for the PopMedNet™ software or any other related activity.
System Software	Development and Production hosting environment each require Windows Server, IIS, .NET and SQL Server as the operating environment.
Production System Monitoring	Internal monitoring for hardware, system software, or application software failures and remediation.
Ticketing System	System for logging, tracking, and auditing resolution of all incidents detected via monitoring or due to support calls.

Requirement	Description

Technical Support	**Technical / Customer Service and Support Hotline / Process Overview**
	Anyone experiencing technical issues involving use of the systems may call the hotline for support. The specific process works as follows:
	
	1. **Call the Support Hotline:** (866) 624-2030 (Within the U.S.A) **/** (513) 768-3747 (International)
	
	   NOTE: ALL ISSUES THAT NEED IMMEDIATE ATTENTION MUST BE SUBMITTED VIA TELEPHONE.
	
	   The call center staff will enter a ticket and contact an "on-call" engineer. The on-call engineer will respond within 15 minutes.
	
	   Email Option for Non-Critical Support Needs
	   Non-critical issues can be submitted via email to: managedservices@lincolnpeak.com. A ticket will be entered into the tracking system. However, the call center will not notify the on-call engineer as these issues are not expected to be critical. On-call engineer will lead the technical support delivery team, keeping the Client Partner and Technical Lead aware of all issues.
	
	2. **For each support request, users will:**
	   1. Tell the call center customer representative which network (e.g., AHRQ, FDA Mini-Sentinel) they are calling about
	   2. Provide company name, your name, phone number and email address
	   3. Describe the issue

Software Patches	Application of software patches for the operating environment (Windows Server, IIS, .NET and SQL Server) and the PopMedNet™ Portal application will be applied on a regular basis during regularly scheduled maintenance windows. Publishing of updates to the DataMart will occur on a regular basis.

Table 18: Hosting, Security & Support: Detailed Requirements

Requirement	Description
Detailed Requirements	
Ping, pipe, power, connectivity, fire suppression, security.	Redundant TIER III level network connectivity at LAN and WAN, HVAC, fire suppression, and power along with physical and video security monitoring.
Servers, Virtual Machines	Web servers are hosted in private cloud based on Citrix XenServer with redundant physical servers supporting automated failover and load balancing. Database servers are clustered physical servers. All servers or VMs are connected to RAID 10 iSCSI SAN for storage and SAN based backup.
System software	Windows 2008 Server, IIS 6.0 / 7.0, .NET Framework 3.5 and SQL Server 2008.
Server maintenance	Regular maintenance windows to install system software and application software and to allow installation of patches and upgrades as well as server performance analysis.
Solution environment backup	Daily scheduled backup of the solution source and web server runtime environment.
Database backup	Full backup daily and incremental every 15 minutes. Stored onsite. The system will backup files or deleted queries on the disaster recovery database for 4 days and will automatically delete on day 5.
System event and SNMP trapping and notification	Trapping, alerting and responding to hardware, system software (operating system, database) and application software errors and notifications.

10.2 Hosting Design Overview

The hosting environment is operated at a data center provided by Carpathia Hosting, Inc. in Dulles, Virginia. Carpathia is a provider of FISMA/ SAS-70 private cloud services and operates TIER III datacenters (TIER III covers full system redundancy and redundant commercial connections to major backbones). Specifically, Tier III is comprised of multiple active power and cooling distribution paths, has redundant components, and is fault tolerant, providing 99.995% availability. Carpathia has facilities in many major US cities and around the world and provides: redundant HVAC, redundant fire suppression, redundant power with UPS and generator backup. The facility is secured with man-trap entrances, photo identification validation, manned armed security tours, and video surveillance 24 hours per day, 7 days per week. Figure 2 illustrates the system infrastructure.
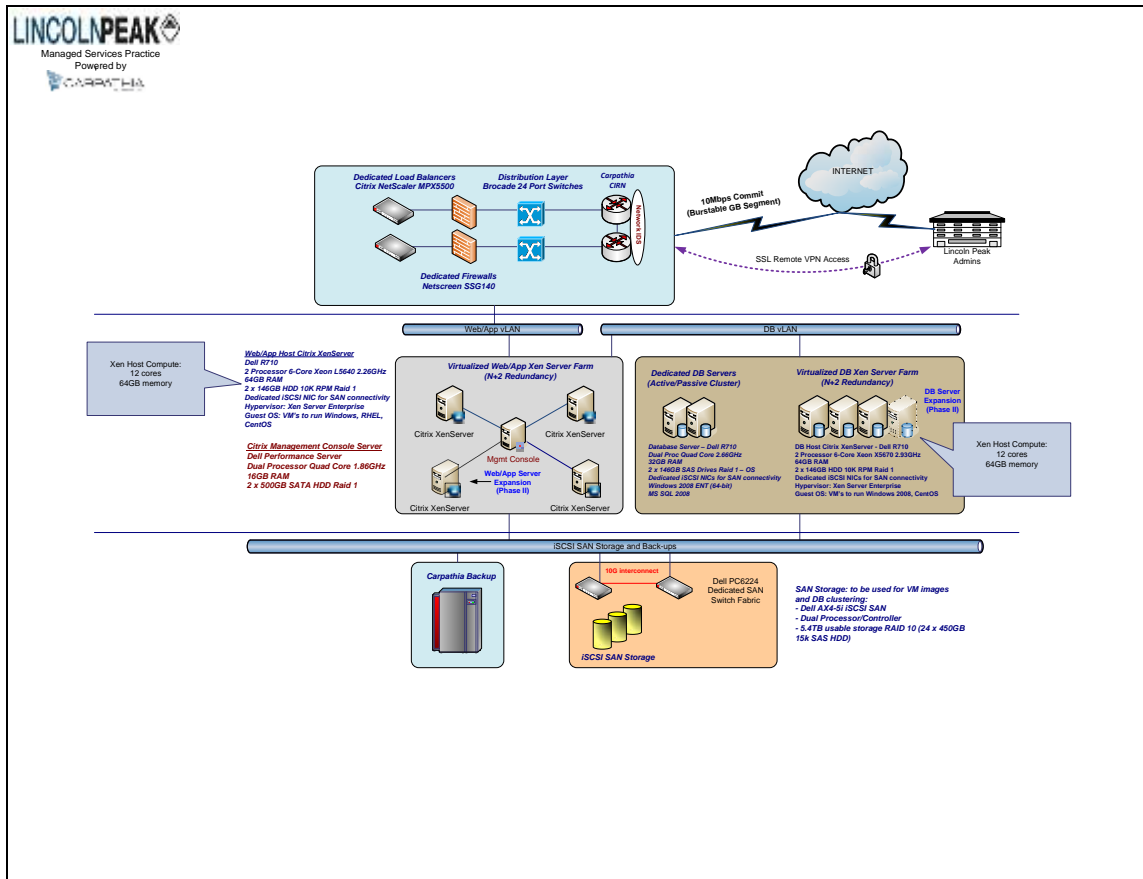
Figure 61 – Hosting System Infrastructure

LPP's systems connect to the internet via dual Juniper Router / Firewall / VPN concentrators that provide redundant connections to the internet with automatic failover. Each device has redundant power supplies connected to separate power circuits in the Tier III data center. The devices provide routing functions from the VLANs implemented on the redundant switches to the Internet. In addition to routing, the systems provide firewall and VPN functionality. Firewalls are configured to restrict inbound traffic to only HTTP (port 80) and/or port HTTPS (443) to the web servers. All clients are assigned dedicated web servers on virtual machines. No direct inbound web access is allowed to the database servers. All database traffic is routed through the firewalls and limited to the appropriate web server. VPN is dual authentication, requiring the use of an RSA token in addition to username/ password. The VLANs span the dual Ethernet switches and dual physical NICs are teamed on the servers for production data providing 2GB bandwidth and redundancy in the event of NIC or switch failure.

The Application Portal is hosted in a two server configuration, one server (Portal web Server) to run the application and to service all applications requests that come in via the Web. This server runs the Portal application under IIS and ASP .NET. The second server (Portal Database server) houses the Portal Database in a MS SQL Server 2008 instance. There will be no connection from the Portal Database server to the web. All requests will be made via the Portal Web server. Web servers are on virtual machines with support for load balanced web farms as utilization increases and database servers are physically clustered servers for FISMA compliance. Database server is replicated via log shipping to Carpathia Phoenix data center which is also FISMA compliant. Each server is hardened and performance tuned according to Microsoft best practice

documentation. A third Management Server (not open to the Web and only available via Virtual Private Network) will be used by Operations Administrators to monitor the health and tune the Portal Web Server and the Portal Database Server.

10.3 FISMA Controls per NIST SP 800-53 Security Controls

LPP has contracted Plante Moran (http:// http://www.plantemoran.com/) to review all Lincoln Peak's Standard Operating Procedures (SOP) pertaining to Managed Services to determine required enhancements for FISMA compliance. Specifically, the system is designed to meet FISMA Moderate Risk security controls as specified in the National Institute of Standards and Technology (NIST) Special Publication 800-53 (http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev3-final.pdf). The following is a list of applicable NIST SP 800-53 controls and a summary of Lincoln Peak's policies and procedures for each. These descriptions relate to internal LPP SOPs and policies, not those of the querying system.

Lincoln Peak Standard Operating Procedures per NIST SP 800-53 Security Controls
- I.   Lincoln Peak User Access Policy
    1. Provides policy to control who is allowed to access systems and how that access is managed.
    2. Logical Access
        - i.   New Hires/Terminated Users/Modifications/Contractors
            - a) Documentation and verification of all account requests
        - ii. User Access Review
            - a) Periodic review of accounts to eliminate unnecessary accounts
        - iii. Segregation of Duties
            - a) Limiting functional access by role to ensure only properly trained, authorized MSP personnel have access to production equipment.
        - iv. VPN Access
            - a) Policy for issuing and managed dual token SSL based VPN for accessing all systems
        - v.   Domain Policies
            - a) Active Directory and LDAP policies to control system access
            - b) Passwords - 7 character minimum, 100 characters maximum, strong password, quarterly change, enforce history
            - c) Lockouts – 5 failed attempts results in locked account requiring administrator intervention
    3. System Security
        - i.   Server/Network Configuration – security policies
            - a) DMZ
                - a. Web server and database server firewall configuration to prohibit external access to database servers and limit web server protocols/ ports
        - ii. Secure Data Transfer
            - a) FTP
                - a. Limited to behind firewall for authenticated VPN users only
            - b) Encryption

---

              a. All traffic behind traversing firewall is encrypted other than HTTP access to front end web servers by external users

      iii. Assessments and Certifications

          a) Penetration Testing

              a. Periodic testing of security

          b) Vulnerability Scanning

              a. Periodic scanning of ports and systems

      iv. Authorized Traffic

          a) Firewalls

              a. Firewall rules are created on a server by server basis to restrict inbound traffic to HTTP (port 80) and/or HTTPS (port 443) to web servers. Port 25 is available on request for SMTP. Additional ports are available if required and are documented through Change Management Process. Database servers have no direct inbound web traffic and are not NAT'd. DMZ firewalls limit access to each database server to the associated web server(s).

          b) Anti-Virus

              a. All servers must run NOD32 anti-virus

    v. Physical Access

          a) Third Party SAS70 Review

              a. Type II SAS-70 audit to be performed in Q4 2010.

4. Written Information Security Policy/Risk Policy – provides policy on high level controls for access and security monitoring as well as response in the event of an incident

    i. Protecting Data

          a) Both Physical and Electronic data are covered in this SOP.

    ii. Security Awareness Training

    iii. Incident Response

5. Business Continuity, Disaster Recovery Plan

    i. Policy and Plans for recovery of services in the event of data corruption/loss, component failure, system failure, site failure, and geographic failure (i.e., Natural disaster).

          a) Data corruption/loss is addressed via backup/recovery policy

          b) Component failure and system failure are addressed by in-device redundancy and overall redundant architecture of infrastructure providing near zero downtime for these conditions

          c) Site failure is addressed via cold site in Phoenix AZ that is FISMA compliant with log ship database replication and web server daily backup and copy to remote SAN allowing 72 hour configuration and recovery RTO and 15 minute RPO.

6. Change Management Policy

    i. Policy and procedure for reviewing and approving all change to production environment to ensure no unexpected results

    ii. Security Impact Analysis

    iii. Change requests

    iv. QA testing/end user testing
    v. System Backup
    vi. Change Approval prior to Implementation
 7. Software Development Life Cycle
 8. Maintenance Policy
    i. Policy for the control of system maintenance such as OS and application patches
    ii. Establishes maintenance schedule
    iii. Establishes resource and financial budgeting
 9. Vendor Management Policy
    i. Policy for the review, approval, and control of vendors as they pertain to managed services
 10. Human Resources Policy – Policy and procedure for review and approval of employee and contractor candidates
    i. Candidate screening including background and reference checks.
    ii. System security awareness policy/training

10.4 Security Specifications

The PopMedNet™ software system has undergone 3rd-party secure audit and passed a Harvard Pilgrim Health Care security audit and penetration test. The following list contains major system security governance specifications of the system.

- Enhanced system procedures
  - Securely store credentials as Salted Hashes
  - Use cryptographically secure random values for session IDs (.Net Type 4 GUID)
  - Cookies marked as 'SECURE', 'SESSION' & 'HTTPONLY' and the cookie domain
- Transmission
  - Require/force Secure Socket layer (SSL) for all communications
  - Enable strongest cipher suites and Transport Layer Security (TLS) versions
- Web Service and Portal Authorization
  - Ensure all submissions are performed via POST method
  - Do not publish WSDL
  - Limit the number and size of file submissions
- Users are required to select strong passwords with the following rules: at least 7 characters, maximum length of 100, at least 1 number, at least one nonnumeric character, at least one capital letter, at least one lower case letter. Passwords cannot contain the user name or any part of the user's full name.
- The system will force users to change their passwords every six months.
- Passwords cannot be re-used.
- The system will automatically log users off after thirty minutes of inactivity.
- The system will automatically delete all query results after one year.

- The system will automatically delete file transfers after 21 days.
- The system will backup files or deleted queries on the disaster recovery database for 4 days and will automatically delete on day 5.
- Network Administrators will verify user identities and email addresses before creating new user accounts.
- Users must use corporate email addressed for network communication.
- Only Network Administrator shall modify user email from user administration page on the portal.
- The system will audit all network activity (e.g., access, user ID changes, query initiation, results upload, etc.) and will regularly review audit logs to look for inappropriate system use.
- Antivirus software will run regularly on all system servers.
- DataMart Administrators will be notified of relevant changes within the system such as the addition of a new user or DataMart. DataMart Administrators will be able to create audit logs of all activity related to their DataMart; see screenshot below for an example audit report.

Figure 61 – DataMart Audit Report

11 Related References

Reports

- Brown J, *et al.*, Proof-of-principle evaluation of a distributed research network. Effective Health Care Research Report No. 26. (Prepared by the DEcIDE Centers at the HMO Research Network and the University of Pennsylvania Under Contract No. HHSA29020050033I T05.) Rockville, MD: Agency for Healthcare Research and Quality. June 2010. Available at: http://effectivehealthcare.ahrq.gov/reports/final.cfm; 2009, AHRQ.

- Brown J, *et al.*, Blueprint for a distributed research network to conduct population studies and safety surveillance. Effective Health Care Research Report No. 27. (Prepared by the DEcIDE Centers at the HMO Research Network and the University of Pennsylvania Under Contract No. HHSA29020050033I T05.) Rockville, MD: Agency for Healthcare Research and Quality. June 2010. Available at: http://effectivehealthcare.ahrq.gov/reports/final.cfm; 2009, AHRQ.

- Brown JS, *et al.*, Design specifications for network prototype and cooperative to conduct population-based studies and safety surveillance. Effective Health Care Research Report No. 13. (Prepared by the DEcIDE Centers at the HMO Research Network Center for Education and Research on Therapeutics and the University of Pennsylvania Under Contract No. HHSA29020050033I T05.), Agency for Healthcare Research and Quality: Rockville, MD. Available at: http://effectivehealthcare.ahrq.gov/reports/final.cfm; 2009, AHRQ.

- Brown JS, Lane K, Moore K, Platt R. Defining and Evaluating Possible Database Models to Implement the FDA Sentinel Initiative. Report to the U.S. Food and Drug Administration, Contract No. HHSF223200831315P; May 2009. Available at http://www.fda.gov/oc/initiatives/advance/sentinel.

Manuscripts

- Maro, J.C., *et al.*, Design of a national distributed health data network. Ann Intern Med, 2009. 151(5): p. 341-4.

- Brown, J.S., *et al.*, Distributed health data networks: a practical and preferred approach to multi-institutional evaluations of comparative effectiveness, safety, and quality of care. Med Care. 48(6 Suppl): p. S45-51.

Websites

- Mini-Sentinel.org
- PopMedNet.org

12 Development and Funding Statement

The **PopMedNet™** software application was developed as part of several contracts awarded by the Agency for Healthcare Research and Quality to the HMO Research Network (HMORN) Center for Education and Research on Therapeutics (CERT) DEcIDE Center housed in the Department of Population Medicine at the Harvard Pilgrim Health Care Institute (HPHCI). The software application has been enhanced using additional funding via the FDA Mini-Sentinel contract with Harvard Pilgrim Health Care. The system was developed by Lincoln Peak Partners under the direction of HPHCI.