**Diabetes Registry**

**Administrator Manual**

Version 2

March 16, 2017

Table of Contents

[1.0 Introduction 3](#_Toc478196811)

[1.1 Overview 3](#_Toc478196812)

[1.2 Purpose 3](#_Toc478196813)

[2.0 Administrative Functions 3](#_Toc478196814)

[2.1 Find Administrative Functions 3](#_Toc478196815)

[2.2 Update Clinic Details 5](#_Toc478196816)

[2.3 User Management 6](#_Toc478196817)

[2.3.1 Edit User 6](#_Toc478196818)

[2.3.2 Terminate User 6](#_Toc478196819)

[2.3.3 Reset Password 7](#_Toc478196820)

[2.3.4 User Audit 7](#_Toc478196821)

[2.4 Add a New User 7](#_Toc478196822)

[2.5 Password Reset Requests 8](#_Toc478196823)

[2.6 Email Reminder Management 9](#_Toc478196824)

[2.7 Quality Checklist Management 11](#_Toc478196825)

[3.0 Important Notes 11](#_Toc478196826)

[3.1 Security 11](#_Toc478196827)

[3.1.1 IP Address Filter 11](#_Toc478196828)

[3.1.2 Security Constraint 12](#_Toc478196829)

[3.2 Other Considerations 12](#_Toc478196830)

[3.2.1 Web Mail 12](#_Toc478196831)

# 1.0 Introduction

## 1.1 Overview

The administrative functions in the web application of the Diabetes Registry provide a way for the administrator to update clinic information, modify information used in the registry, and manage user access. The role of registry administrator is not set in the application interface; the role may only be set by direct database access.

## 1.2 Purpose

The goal of this manual is to explain and demonstrate the administrative functions provided by the application interface of the system. This manual describes the procedures for updating clinic information in the database, managing users, adding new users, reading password reset requests, managing email reminder messages, and managing quality checklist items.

# 2.0 Administrative Functions

## 2.1 Find Administrative Functions

A user with the role of administrator will have automatic access to administrative functions within the web application interface. To find the administrative section of the application, sign in to arrive at the home page. On this page and other pages of the application, a link for “Administration” can be found in the upper right corner. Click on this link to navigate to the administration main page.



Figure 1 Home Page

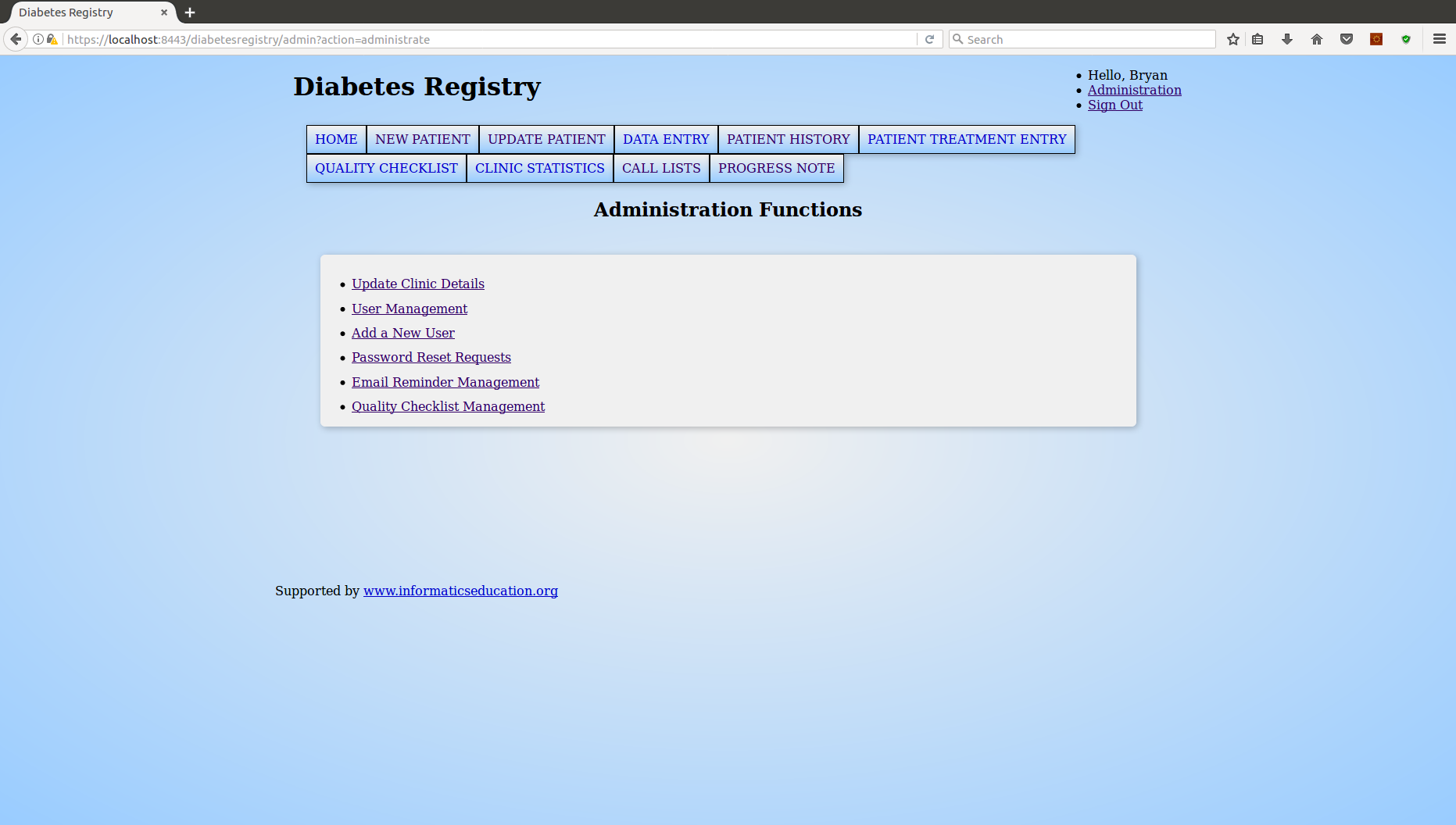


Figure 2 Administration Functions

## 2.2 Update Clinic Details

To find the form for updating clinic information, select the “Update Clinic Details” link from the administration functions menu. The update form will appear, populated with the clinic’s current information stored in the database as seen in the following figure. The clinic email address may be left blank, but it is required for functions in the registry associated with email messages, such as sending call list reminders, adding new registry users, and resetting user passwords.

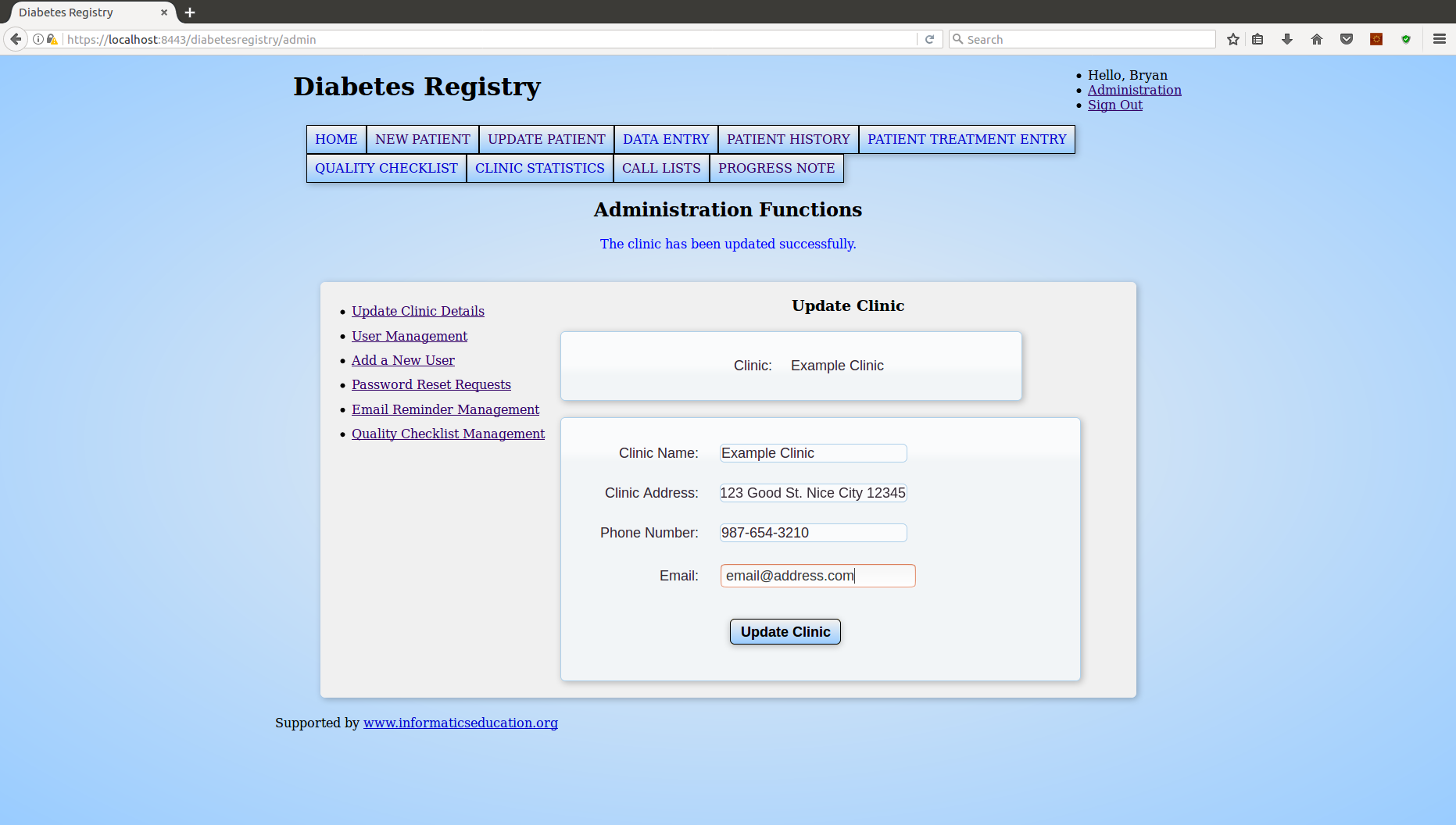


Figure 3 Update Clinic Form

When the information has been updated in the form, select the “Update Clinic” button at the bottom of the form to save the changes.

## 2.3 User Management

To manage users in the registry, click on the “User Management” link in the administration functions navigation menu. A drop-down selection is visible at the top of the form to choose the desired user. When a user is selected, options will be available for editing user details, terminating the user, resetting the user’s password, and viewing user activity.

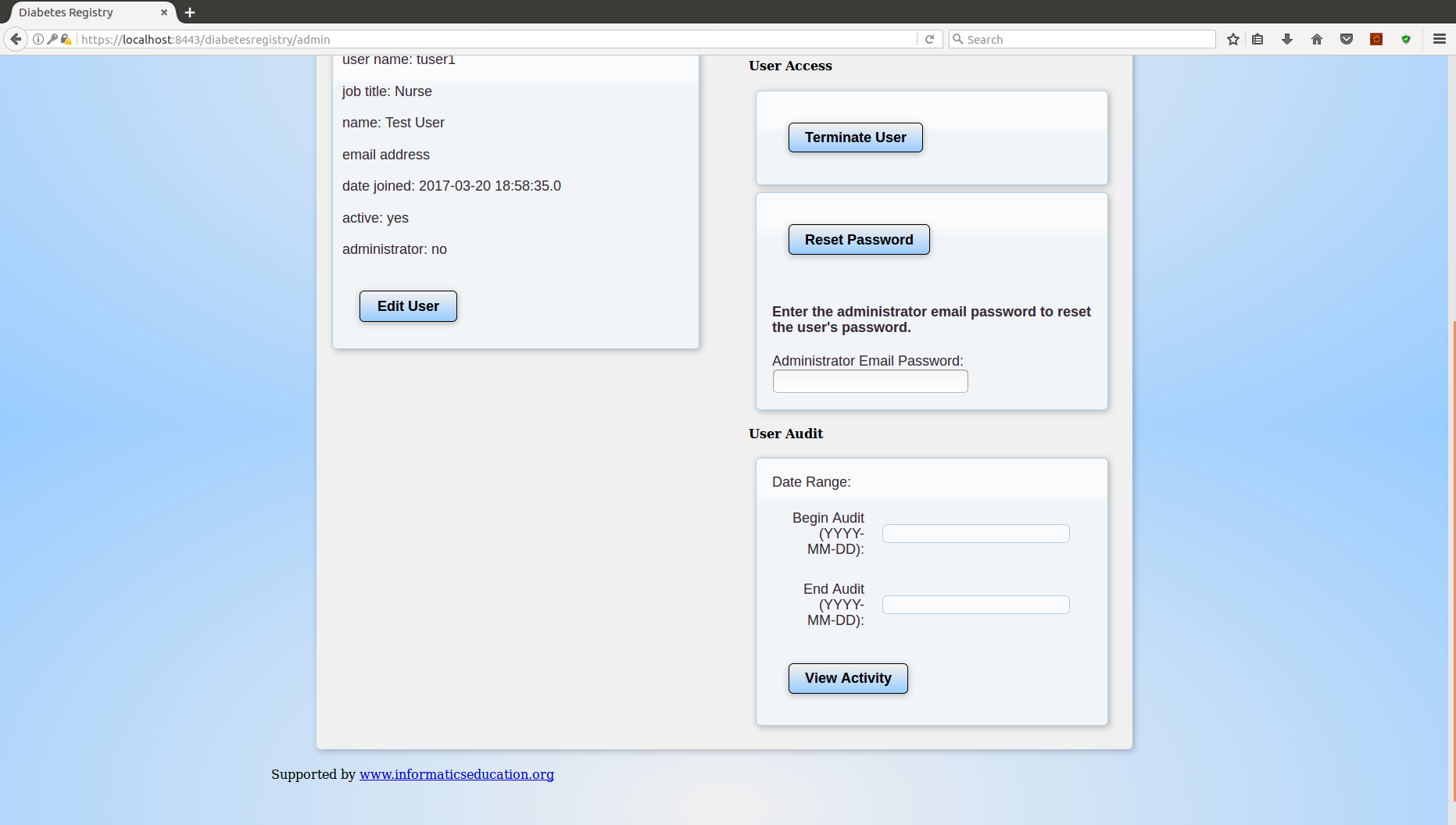


Figure 4 User Management

### 2.3.1 Edit User

The “Edit User” button, when clicked, will show a form where user first name, last name, job title, and email address may be modified. Upon clicking “Save” the new information will be written to the database. Clicking “Cancel” will hide the input form for editing the user.

### 2.3.2 Terminate User

The “Terminate User” button will set the selected user’s status to inactive, preventing any further sign in by the user. There is no administration function to revert this termination.

### 2.3.3 Reset Password

The “Reset Password” function will generate a new temporary password for the selected user and require new password creation by the user after successful sign in with the temporary password. To successfully reset the user’s password and receive the newly generated temporary password, the clinic email address must be stored and the email password must be entered into the input field labeled “Administrator Email Password”.

### 2.3.4 User Audit

User activity, such as a successful sign, in may be viewed by selecting a time frame in the “User Audit” section of the page. To view activities for the selected user, enter a start date and an end date and click the “View Activity” button. If any activity was recorded for the user, it will appear as a list at the bottom of the page.

## 2.4 Add a New User

To add new users to the registry, navigate to the new user form by selecting the “Add a New User” link from the administration navigation menu. The clinic email address attribute must be stored and the email password must be provided when adding new users. When a user is successfully added to the registry, the user ID and temporary password are generated and sent to the clinic email address.

The new user form contains input fields for first name, last name, job title, and email address. The email address field is optional and is only intended for organizational email accounts which are under the control of the administrator. It is inadvisable to store any private email address for a user as this address will also receive sign-in IDs and temporary passwords when generated.

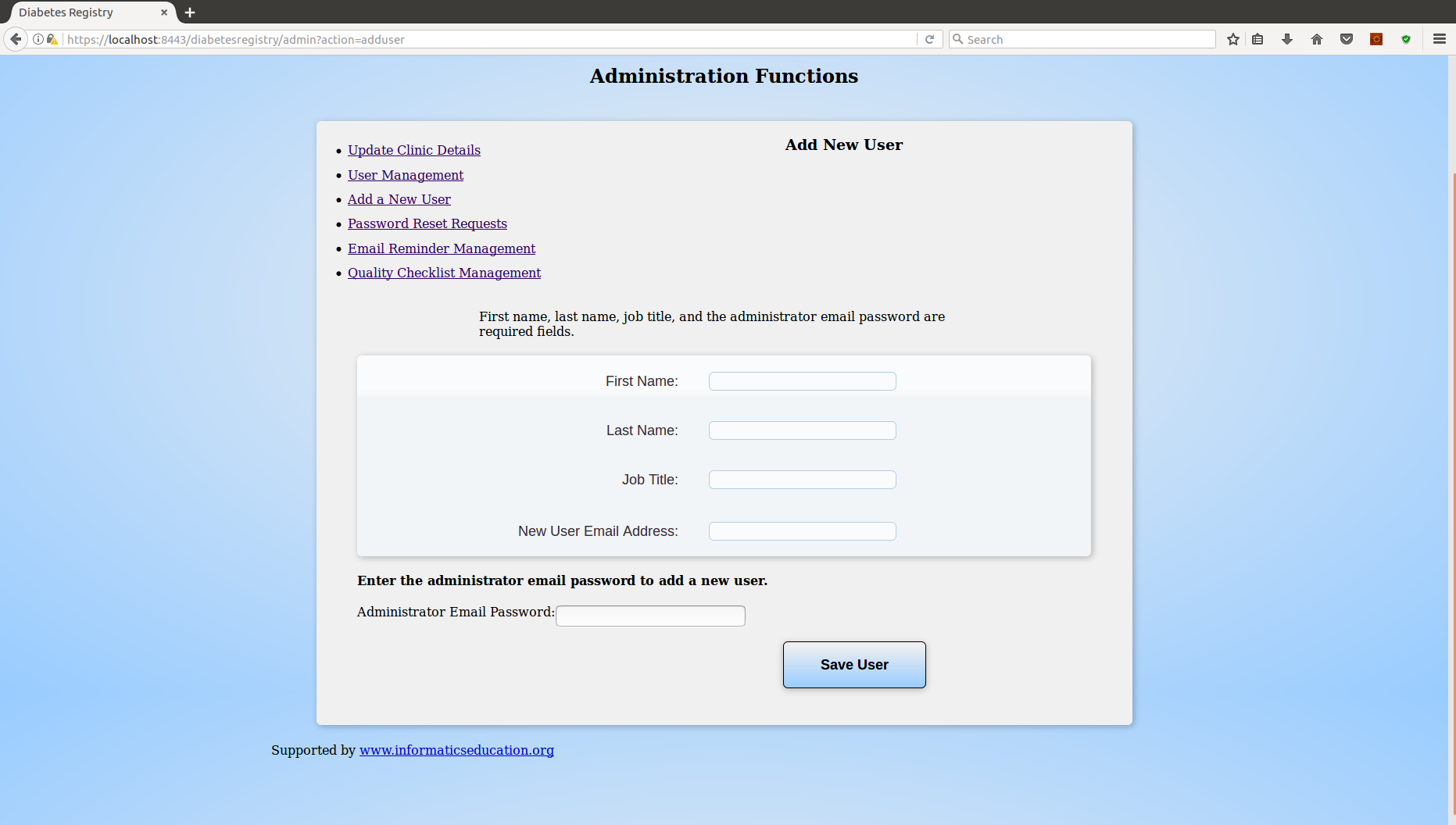


Figure 5 Add New User

## 2.5 Password Reset Requests

To view requests by users for password resets, select the navigation option for “Password Reset Requests”. Requests that have not been marked as read will appear as a list on the page. Select the checkbox of the item in the “Mark as Read” column and click the “Save” button to mark a request as read.

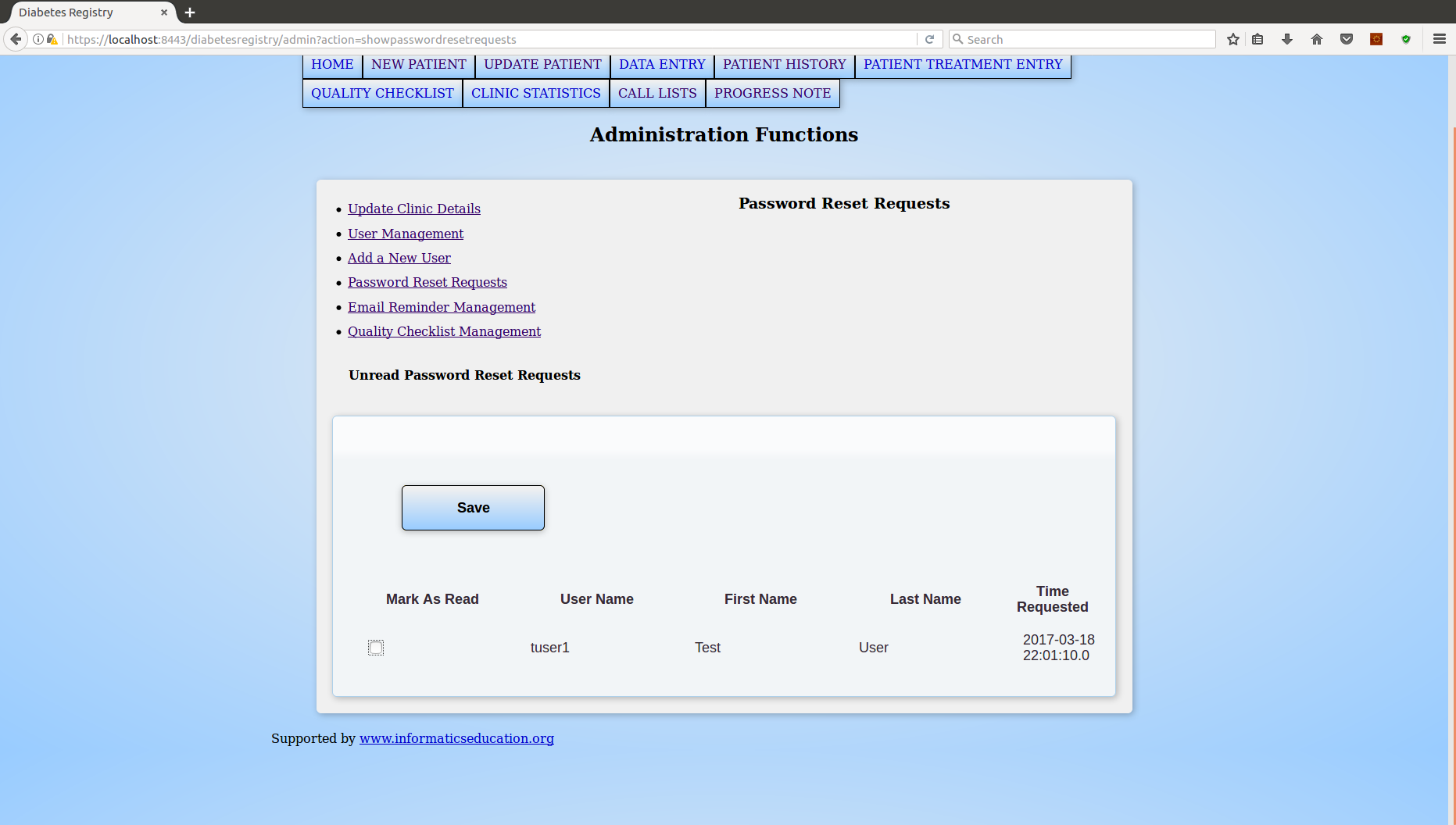


Figure 6 Password Reset Request

## 2.6 Email Reminder Management

Select the “Email Reminder Management” link in the administration navigation menu to show a selection menu to choose to edit an existing email reminder or create a new one. The selection menu is shown in the following figure.

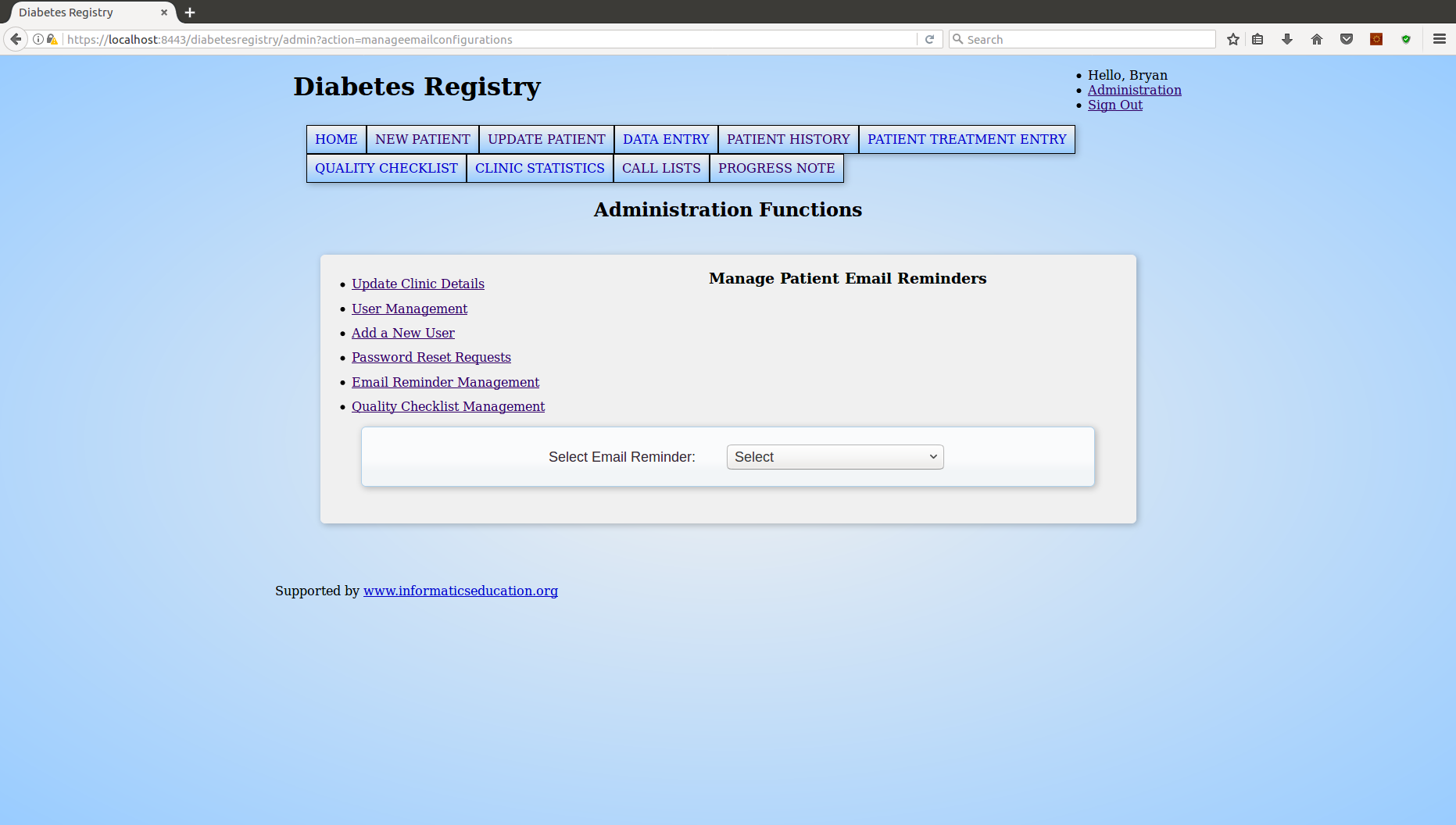


Figure 7 Select Email Reminder

The form for editing an existing email reminder will allow for modification of the email message while all other attributes of the reminder remain unchanged. When creating a new email reminder, the form requires input for subject, language, and patient filter in addition to the email message. The patient filter is in place to determine which patients will populate the call list on the call list page when the subject is selected.

Each email reminder must have a unique subject and language combination, so, when creating a new email reminder sharing the subject of another reminder, the language must be distinct from the existing reminder. Each subject has only one filter, so a subsequent subject-sharing reminder must adopt the same filter adopted by the initial subject-sharing reminder. Any duplicate subject-language combination or non-matching filter selection will result in an error message.

If an email reminder is no longer needed or mistakes were made in the creation of a reminder, the form allows for the deletion of the selected reminder.

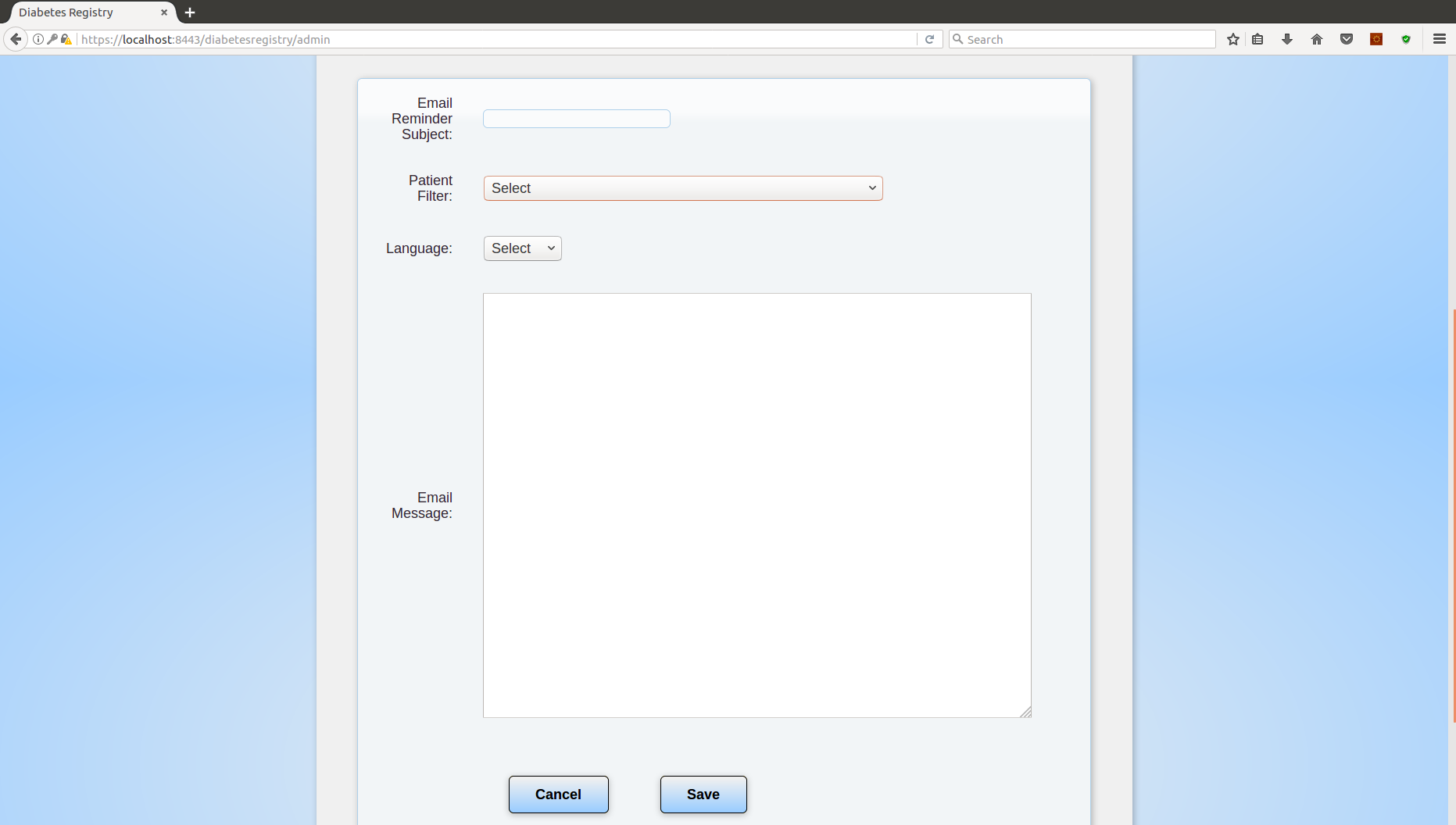


Figure 8 New Email Reminder Form

## 2.7 Quality Checklist Management

To manage the checklist items used by healthcare providers to document accomplished tasks, click the link for “Quality Checklist Management” in the administration navigation menu. A seen in the following figure, a role selection menu appears from which a quality role or all roles may be selected to show the list of corresponding responsibility items.

Activated items may be deactivated to no longer show on the quality checklist page and deactivated items may be re-activated to appear on the quality checklist page. Below the list, an option for creating a new checklist item is available. A new item must not have a responsibility exactly matching the responsibility of an existing item.

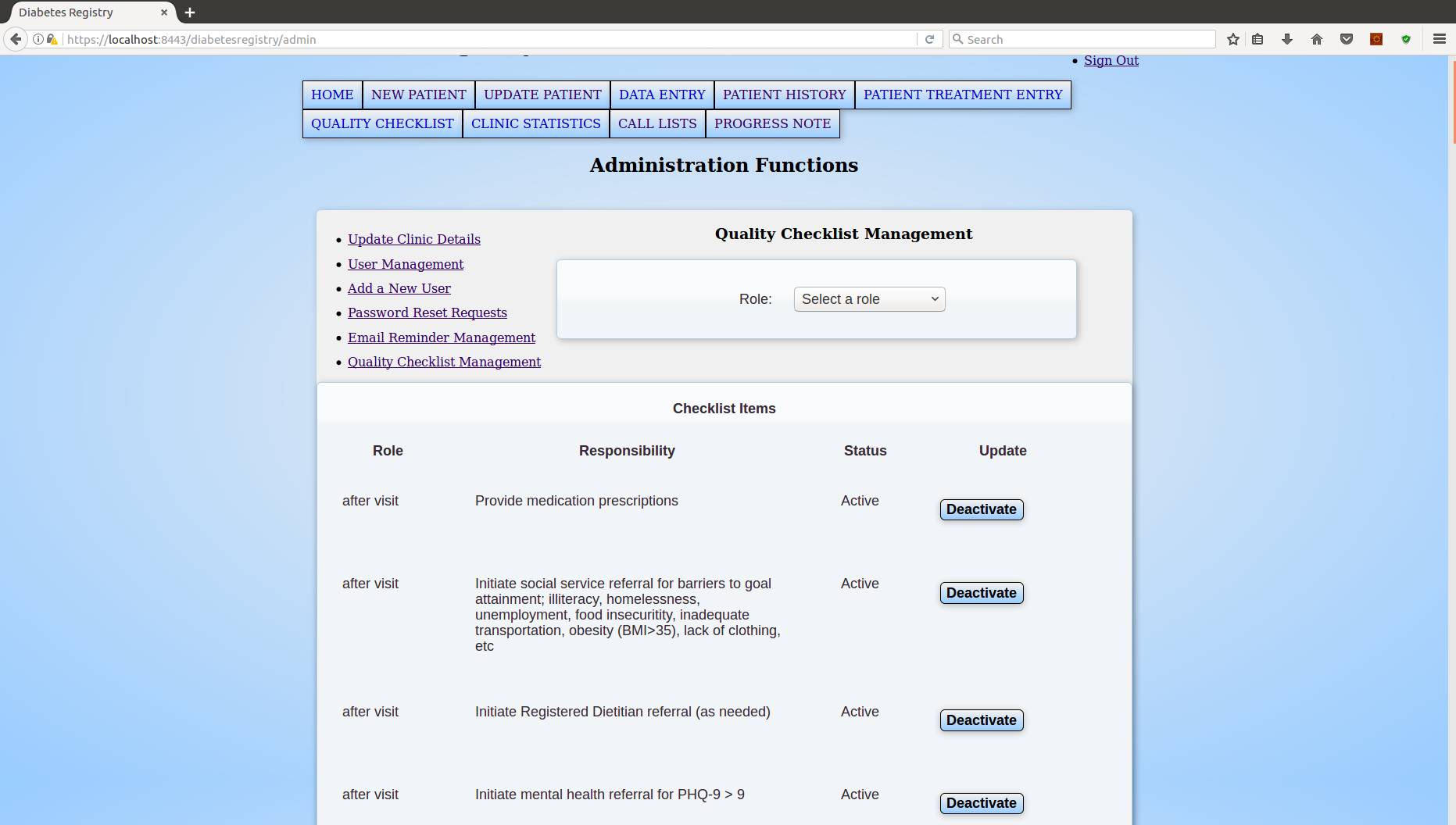


Figure 9 Quality Checklist Management

# 3.0 Important Notes

## 3.1 Security

### 3.1.1 IP Address Filter

The Remote Address Filter is contained in the Tomcat configuration file WEB-INF/web.xml. Only specify IP addresses in the “param-value” element of the Remote Address Filter which are needed by authorized users for access to the registry. If an address is temporarily added to the filter, remove it after use.

### 3.1.2 Security Constraint

The web.xml file contains a security constraint specifying that data transport is confidential; meaning that implementation of SSL or TLS is required. When deployed, the server must be configured with an SSL certificate. To run this program on a local, isolated machine, a self-signed certificate may be created to comply with the security requirement. The procedure for creation of a self-signed certificate is outside the scope of this document.

## 3.2 Other Considerations

### 3.2.1 Web Mail

The Simple Mail Transfer Protocol (SMTP) server utilized by the email functions of the call list page and the administration tasks is specified in the XML file, WEB-INF/mail.xml. A deployment necessitating a different web host will require updating the mail.xml file to hold the correct SMTP host name.