Software Requirements Specification for

Strengthening the password policies

(Security Module Enhancement)

Version 1.0

By Visolve ViCare Team

Prepared by

ViSolve Inc.,

Contact: 408.666.4320

EMail: vicare_engg@visolve.com

www.visolve.com

25th November 2009

Revision History

Version	Date	Author	Reviewed By
1.0	11/25/09	ViCare Team	Team

Table of Contents

1. Introduction

The purpose of this document is to describe the technical requirements of strengthening the password policies under HIPAA in OpenEMR.

2. Strengthening the Password Policies

(a) Password must be eight character length or more and must contain just 3 of the following 4 items:
- a lowercase letter
- an uppercase letter
- an integer
- a special character

How

The password is validated by checking whether the password contains minimum of eight characters and must contains any of the three items from the following four items:

- a lowercase letter
- an uppercase letter
- an integer
- a special character

- If the entered password is invalid an alert message is displayed ("The password must be at least 8 characters, and should contain at least three of the four following items:

  - A number

  - A lowercase letter

  - An uppercase letter

  - A special character (not a letter or number).

  For example: healthCare@09")

- If the password text box is empty an alert message displayed ("please enter the password').

Where

User Addition and Modification

Password change place

(b) Passwords need to be changed on a regular basis (every 6 weeks to 3 months) and the grace login period must be given for another 30 days to reset the password.

- While adding new users in "**User Administration**", the value for "Password Expiration Duration" is also obtained (default value is 180). 'Password Expiration Date' is then calculated (current date + Password Expiration Duration). The above items are taken care in while editing the User details in "**User Administration**" and in the "Password Change" page also.
- After successful login by user, the 'Password Expiration Date' is compared with the current date. if the user logins, prior to <7 days of 'Password Expiration Date, the warning message "Welcome <<UserName>>, Your Password Expires on <<YYYY-MM-DD>>. Please change your password" is displayed.
- If the current date is equal to password expiration date then "Welcome <<UserName>>, Your Password expires today. Please change your password" message is displayed.
- If the user doesn't change his/her password with in the password expiration period, the user got the grace login period of about 30 days. During the grace login period the warning message, "Welcome <<UserName>>, You are in Grace Login period. Please change your password before <<YYYY-DD-MM>>".
- If the "Password Expiration Date" is date empty or default value of "0000-00-00". The warning message "Welcome <<UserName>>, Your Password Expired. Please change your password" is displayed.
- If the user does not change his/her password during the Grace Login period, their user account is locked and the user will not be able to login and user account is moved to 'Inactive' state.
- Later, the admin can activate his/her account by moving the "'InActive'" state to "Active" and change the user password in **"User Administration**" page .
- All above warning messages are displayed in new page. This new page is loaded only once at the top frame (instead of calendar) after a successful login by user.

(c) The system should log the last three passwords and prevent reuse:

- When user password is changed in **"User Administration**" or "**Password Change**" pages, entered password is compared with last three passwords of same user.
- If the entered password is any of the last three passwords user is alerted with "Recent three passwords are not allowed."

3. Database Fields Introduced

Following fields are introduced in "users" table

Password Expiration Duration => pwd_exp_duration

Password Expiration Date => pwd_expiration_date

Password History 1 => pwd_history1

Password History 2 => pwd_history2

4. How to migrate an existing OpenEMR to this feature

Step 1: Move to OpenEMR directory.

Step 2: Patch the given patch file by executing the following comment:

```
Patch –p1 –i patch_file.txt
```

Step 3: Access http://<Openemr installed location>/sql_upgrade.php in web browser, choose 3.1.0 from version list and click 'Upgrade Database'.

Step 4: After successful login by any user (Example: admin) on the top frame a message displayed

and request the user to change his/her password.

Step 5: Change his/her password in “Password Change” page and re-login.