Developing a HIPAA Compliant EMR System: TigerPlace Case Study

A Thesis presented to the faculty of the Graduate School

University of Missouri—Columbia

In Partial Fulfillment
Of the Requirements for the Degree

Master of Science

BY:-

SAURAV GARG

Dr. Yang Gong, Thesis Supervisor

May - 2012

The undersigned, appointed by the Dean of the Graduate School, have examined the thesis titled:

Developing a HIPAA Compliant EMR System: TigerPlace Case Study

Presented by Saurav Garg,

a candidate for the degree of master science, and hereby certify that, in their opinion, it is worthy of acceptance.

Dr. Yang Gong, Faculty Advisor

Dr. Mihail Popescu, Assistant Professor

Academic Supervisor

Dr. Lori L. Popejoy, Assistant Professor

ACKNOWLEDGEMENTS

I would like to express my gratitude to all those who supported me to complete this thesis. I would like to thank the Health Management and Informatics Department of the University of Missouri-Columbia, for giving me the opportunity to commence this thesis in the first instance, and to do the necessary research work, a vital foundation for my future career.

I am deeply grateful to my academic advisor, Assistant Professor, Dr. Yang Gong, whose help, valuable suggestions, ideas, and encouragement assisted me in writing of this thesis during the time of research. I really enjoyed working with Dr. Yang Gong, as he was a very good listener and was always open to new ideas and suggestions. The successful completion of this thesis lies in the strength of encouragement and guidance that I gained at regular intervals whenever needed from my academic advisor, Dr. Yang Gong.

I would also like to thank my project supervisor, Dr. Mihail Popescu, and Dr. Marilyn Rantz, who gave me an opportunity to work on the TigerPlace EMR project when I started my master's program in Health Informatics. This is the sole opportunity that helped me in formulating the idea for the thesis and I believe this thesis could not have been written without this opportunity, encouragement, guidance, and valuable input that I gained throughout the process of this research from Dr. Mihail Popescu.

Finally, I would like to express my sincere gratitude to Dr. Lori L. Popejoy and Dr. Lanis Hicks, whose advice, motivation, and guidance facilitated me to complete my research work.

Table of Contents Page No.

Chapters

LIST OF FIGURES

Figures Page No.

LIST OF ABBREVIATIONS

ADL	Activities of Daily Living
AJAX	Asynchronous JavaScript and XML
CA	Certification Authority
CMS	Centers for Medicare and Medicaid Services
CSRF	Cross Site Request Forgery
CSS	Cascaded Style Sheet
CXR	Chest X-Ray
DAC	Discretionary Access Control
DME	Durable Medical Equipment
EMR	Electronic Medical Record
ER	Emergency Room
ERA	Elopement Risk Assessment
HCFA	Health Care Financing Administration
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HTML	Hyper-Text Markup Language
HTTP	Hyper Text Transfer Protocol
JS	JavaScript
IADL	Instrumental Activities of Daily Living
ICD-9	International Statistical Classification of Diseases, Version 9
ID	Identification Number
IDS	Intrusion Detection System
IPS	Intrusion Protection System

IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LTC	Long-Term Care
NIST	National Institute of Standards and Technology
MAC	Mandatory Access Control
MD5	Message Digest
MU	University of Missouri
NHIS	Nursing Home Information System
PC	Personal Computer
PHP	Hypertext Pre-Processor
PPD	Purified Protein Derivative
RBAC	Role Based Access Control
SF	Short Form
SQL	Structured Query Language
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
VPN	Virtual Private Network
WWW	World Wide Web
XHTML	Extended Hyper-Text Markup Language
XSS	Cross Site Scripting

INTRODUCTION

Healthcare organizations are complex, with a number of diverse stakeholders that include healthcare professionals and consumers. One patient may be linked to many providers, and one doctor is linked to many patients. It is, therefore, critical for the healthcare team to have access to accurate, complete, and reliable medical data and information in order to provide effective, timely care. It is equally important to protect medical record information from misuse by unauthorized persons. With the evolution of electronic medical record (EMR) systems, it has become very easy for healthcare providers to access medical information outside of the healthcare organization. This access makes it imperative to protect the privacy of patient's records from misuse by unauthorized users.

The rapid evolution of Information Technology (IT) systems and their application is seen in nearly every aspect of modern society, including banking, education, and entertainment. The healthcare industry is also taking advantage of these information technologies. IT technologies in healthcare have shown improvement in processes and organizational efficiencies, provide access to information and help in relation to a wide range of health and health-related issues to healthcare consumers. Simultaneously, information technology has also produced many problems related to consumer protection and satisfaction, identity protection, interoperability between systems, harmonization (universal standards), quality control, intellectual property rights, and investment strategies (Bashshur, 2002).

TigerPlace is a for-profit independent living long-term care facility for adults age 65 and above. The healthcare team at TigerPlace includes nurse care coordinators, nurses, physicians, social workers, and aides. The primary goals of TigerPlace are to help senior citizens feel

independent, comfortable, active, and healthy. To achieve these goals, TigerPlace has been continuously involved with various IT projects, such as smart home technology and nursing information systems, such as the EMR, to record early signs of illness and provide effective and efficient healthcare to residents.

The purpose of this project was to develop a secure and HIPAA-compliant EMR system in TigerPlace. According to HIPAA rules and regulations, any covered entity (e.g., healthcare providers, health plans, system vendors) that maintains or transmits electronic medical records from one system to another must develop, implement, and maintain reasonable and appropriate safeguards (administrative, physical, and technical) to ensure integrity, confidentiality, and availability of patient information and protect it from unauthorized use or disclosure.

Any information that is processed over the network or internet is exposed to various security threats. Malware infections can easily infect the user system when the user is browsing the web, and this malware or virus can be potentially harmful to the vital information processed by the user system. In order to protect and secure the TigerPlace EMR system from unauthorized access and misuse by hackers/malicious users, and to ensure the compliance of the EMR system with HIPAA requirements, security measures and protocols within the web application were implemented.

This project involved the development of an easy to use and sophisticated information (EMR) system for TigerPlace, analysis and evaluation of security needs for this EMR system, implementation of various security safeguards to ensure integrity, availability, and confidentiality of residents’ medical records and, finally, suggestions for the improvement and enhancement of the security of this application.

This thesis contains seven chapters, starting with the TigerPlace Background outlined in Chapter 1. The TigerPlace EMR system is described in detail in Chapter 2. Literature review, methods and concepts, limitations and recommendations are presented in Chapter 3. Some of the challenges associated with development of the TigerPlace EMR system are summarized in Chapter 4. The various methods for dealing with security concerns that are used within the current web-based EMR application are explained in the chapter 5. The results obtained with the implementation of various security measures and various recommendations are mentioned in Chapter 6. Last but not least, conclusions from this research are presented in Chapter 7.

CHAPTER 1

ORGANIZATION BACKGROUND

TigerPlace is a for-profit independent living long-term care facility for seniors (age 65 and above) designed and developed as a result of collaboration between the Sinclair School of Nursing, Columbia, Missouri, and Americare Systems, Inc., of Sikeston, Missouri. TigerPlace uses an Aging in Place philosophy of care. Senior citizens who move to one of the 54 apartments in TigerPlace do not need to move again, regardless of any change in their care needs. TigerPlace provides patient-centered long-term and equitable health care delivery to all residents and helps them to stay active, healthy, and independent. TigerPlace has a 27 member staff (clinical and non-clinical) to accommodate the needs of seniors and make TigerPlace an attractive and comfortable place to live. The clinical staff includes Registered Nurses (RN), Licensed Practitioner Nurses (LPN), Nursing Aides, and Para-professionals. The non-clinical staff includes an administrator, a finance manager, maintenance staff, contractors, transportation staff, and restaurant staff. About 90% of the residents at TigerPlace suffer from chronic diseases, like diabetes, vascular disease, Alzheimer's dementia, and many other health problems. The clinical staff is responsible for providing care to all residents whenever needed (24 hours a day and 7 days a week).

The increase of the older adult population in the past decade has demanded more supervised care due to their diminishing capability to manage themselves (Scharlach, 2008). In older adults (age 65 years and above) a simple fall can result in major injuries and even permanent disability (Schiller et al., 2007). It has become very important to keep the growing population of older adults healthy, safe, and independent. In order to meet these challenges, TigerPlace has been continuously involved with various IT projects to address the needs of the aging population. Various pilot projects, such as smart home technology, and information systems, such as the EMR system are deployed by TigerPlace to record early signs of illness and provide effective and efficient healthcare to residents at an earlier stage. These projects will not only provide effective healthcare but will also serve to reduce cost associated with long term chronic diseases or injuries, reduce workload of the healthcare team, and help the older adult community to live more safely and healthily (Aud et al., 2007). The smart home technology pilot project that is currently deployed in TigerPlace uses various sensors (motion sensor, video sensor, and bed sensor) to capture pulse rate, respiratory rate, and restlessness during sleep (Mack et al., 2006). This technology allows the healthcare team to identify early signs of illness, and change in functional ability of the residents, so that early interventions can be made. Figure 1 explains how network sensors can help to improve the functional ability of the TigerPlace residents over time.

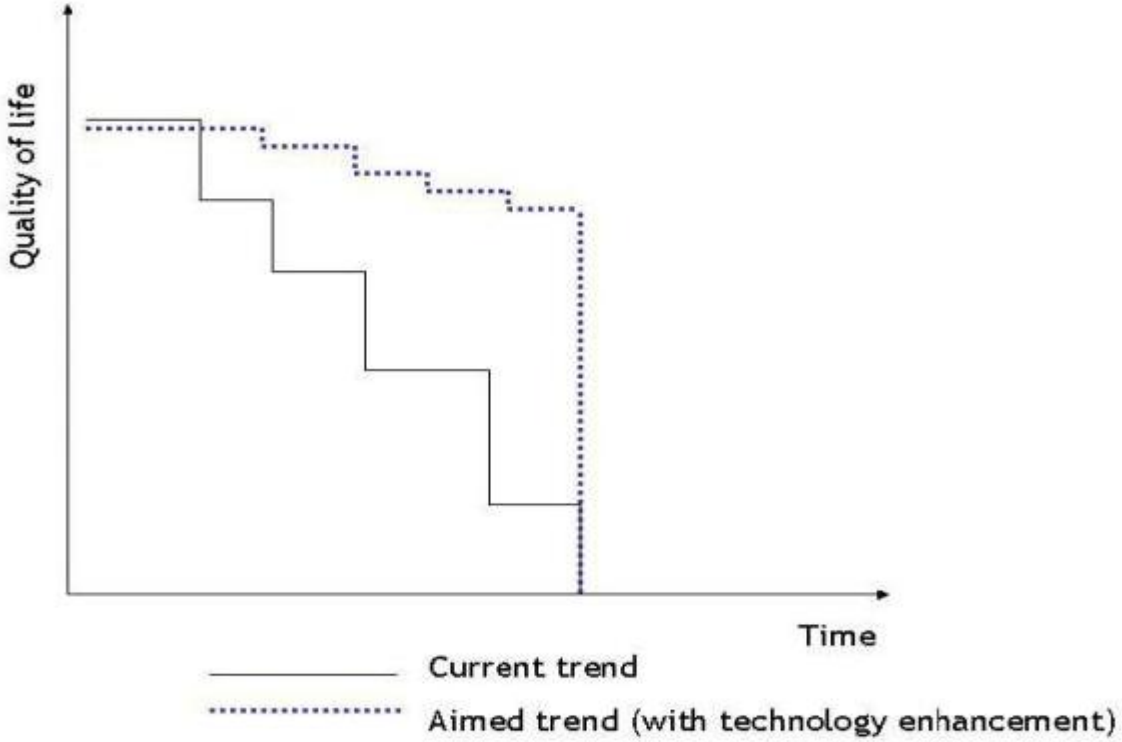


Fig 1 - The Trajectory of Functional Decline (Rantz et al., 2005)

The black solid line shows the routine trend decline in physical and cognitive health and the dotted blue line shows the targeted change in the trajectory when using smart home technology.

Further, the use of a comprehensive EMR system for recording detailed medical and health information about TigerPlace residents can make a real difference in the way healthcare services are rendered. EMR systems can be very useful to calculate quality measures, performance, and quality improvement efforts (Alexander, 2009). Numerous studies have illustrated the benefit of using EMR systems to deliver effective and timely care to patients. According to the American Health Care Association, it has been estimated that adoption of sophisticated IT systems can save up to $140 billion per year (Lourde, 2009). Although a web-based EMR system offers benefits, patient privacy in web-based applications remains a primary concern. The implementation of security measures for EMR systems has not been found to be very promising due to the increased number of attacks in the past decade (Lorence, 2005). This will always leave open the question of how secure the EMR systems are, even after the implementation of various security tools. Figure 2 below illustrates the IT infrastructure at TigerPlace. The IT infrastructure includes six components: physiological sensor (motion sensor, stove sensor, bed sensor), video sensor (which records fall events), behavior reasoning component (which combines the input of physiological sensor and video sensor and generates alerts), activity databases that store the output of behavior reasoning component, EMR database that records various medical and health-related information, and secure web application for displaying data to researchers, clinicians, residents, and their family members (Rantz et al., 2010).

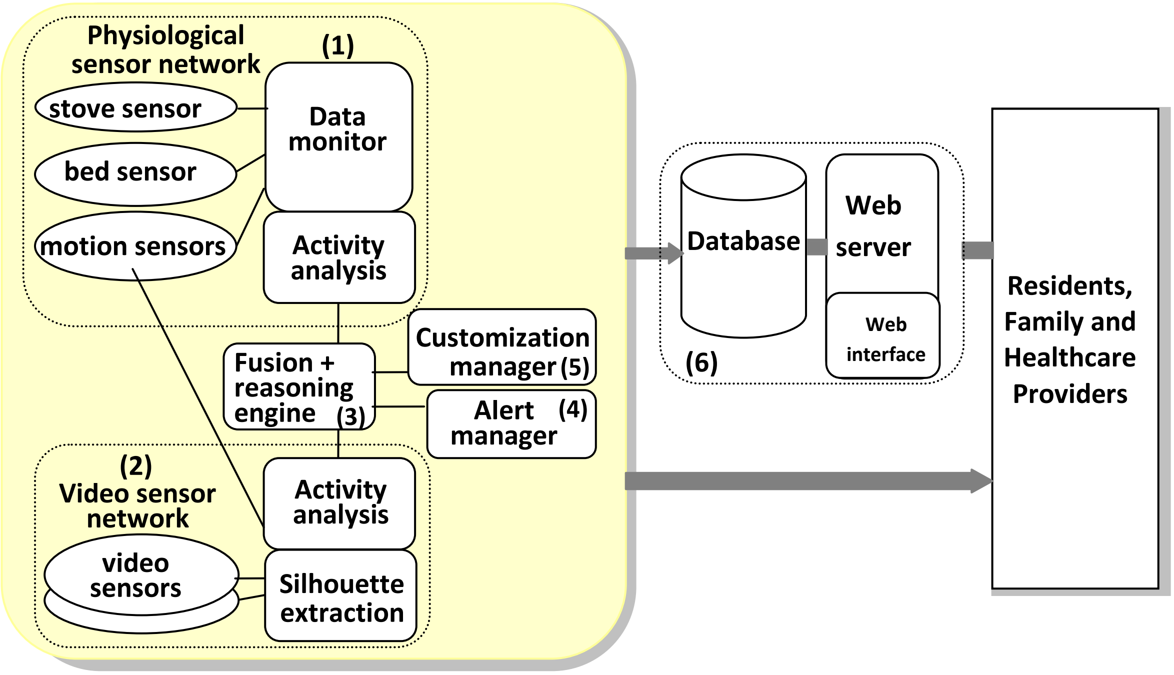


Fig 2 - The Integrated IT Infrastructure at TigerPlace (Rantz et al., 2010)

CHAPTER 2

TIGERPLACE EMR SYSTEM

TigerPlace had previously used the CareFacts™ medical record system. The system was designed for use in community home healthcare settings. CareFacts™ provided programs to complete federally mandated home healthcare assessments, and used the Omaha system taxonomy as the basis for clinical assessment and care plan development. In 2008, they decided to replace the existing EMR, as many components of the system were no longer needed. The decision was made to develop a simpler EMR for TigerPlace, which became the backbone of its information system. The database is aimed at storing and retrieving detailed medical information of residents in an efficient and effective manner, which includes on-going assessment, early illness recognition, and health promotion activities. With the evolution of advance technologies and techniques, it has become possible for healthcare researchers and providers to monitor and detect chronic illness in older adults at an earlier stage and begin medical treatment before problems become serious **(**Starren et al., 2005**)**. This resident-specific data and information will be used by the nurses, doctors, and other medical staff members to provide effective and timely care to TigerPlace residents.

The current EMR system is web-based and allows for storage, retrieval, and modification of medical records of TigerPlace residents. Previously, nurses and other members of the healthcare team needed to incorporate assessments used for evaluating residents’ health, but these assessments were not part of the CareFacts™ documentation system (Rantz et al., 2010).

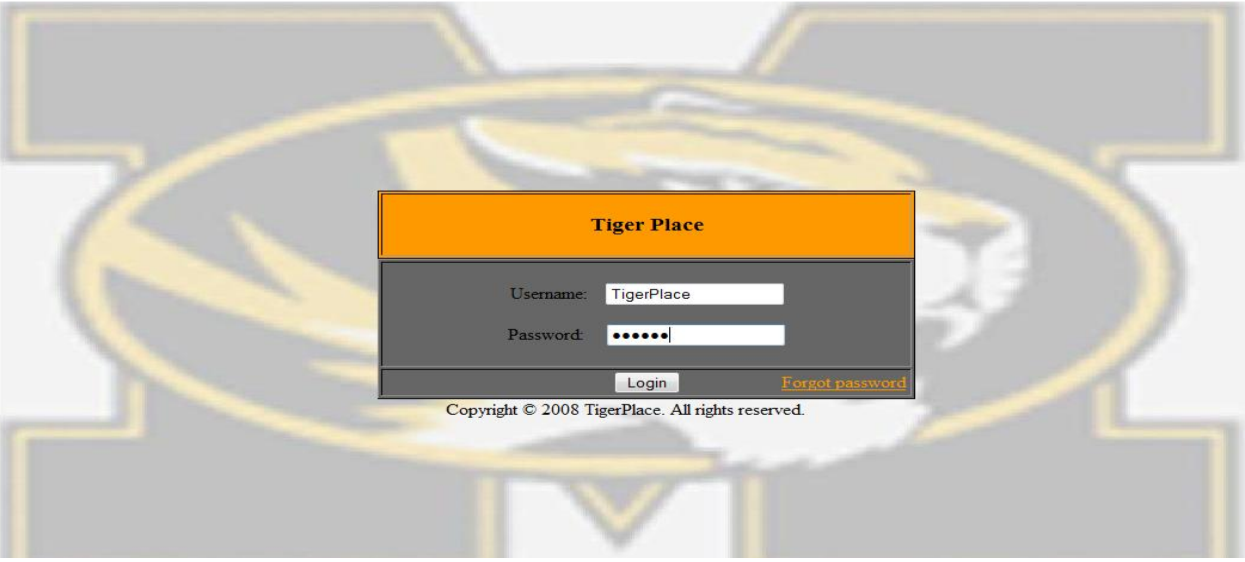
CareFacts™ was a stand-alone application that had to be installed on every personal computer (PC). Since it was a stand-alone application that could only be used on an installed system (laptop or PC), it was believed to waste a lot of nursing time that could be used in delivering care to the residents. TigerPlace was not a home healthcare agency and the features of CareFacts™ that work well in home healthcare were not needed in TigerPlace, effectively making the cost of the program prohibitive. There was a strong need to develop a system or application that could streamline the workflow of nursing care and be easily integrated with sensor technology for effectively and efficiently delivering healthcare to the TigerPlace residents. The web application allows the capability to integrate various different IT systems, applications, and servers, forming the multi-complex systems (Cimino et al., 1998).

The TigerPlace EMR system was designed and developed using PHP, HTML, Ajax, CSS, Javascript and MYSQL as a database. With the evolution of web services, web-based applications are becoming more common, allowing multiple people simultaneous access and providing easy access to information whenever needed **(**Szydlowski, et al., 2007**)**. Due to the interoperability limitation and ease of accessing various EMR systems, the research group has suggested the use of a Web application that uses World Wide Web (WWW) technology (Kohane et al., 1996). PHP is a widely-used general-purpose scripting language that is especially suited for web development, production of dynamic web pages, and can be easily embedded into HTML (Hyper-Text Markup Language). It generally runs on a web server, which is configured to take PHP code as input and create web page content as output. It can be deployed on most web servers and on almost every operating system and platform without any cost. HTML is the predominant markup language for web pages. It provides a means to create structured documents by denoting structural semantics for text, such as headings, paragraphs, and lists, as well as for links, quotes, and other items. It allows images and objects to be embedded and can be used to create interactive forms. It is written in the form of HTML elements consisting of "tags" surrounded by angle brackets within the web page content. It can include or can load scripts in languages, such as JavaScript, which affect the behavior of HTML processors like Web browsers, and Cascading Style Sheets (CSS) that defines the look and layout of text and other material written in HTML (markup language). The use of CSS is stimulated due to its presentational markup (World Wide Web Consortium, 2008). JavaScript is a scripting language used to enable programmatic access to objects within other applications. It is primarily used in the form of client-side JavaScript for the development of dynamic websites. The separation of CSS and HTML can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics, enable multiple pages to share formatting, and reduce complexity and repetition in the structural content (such as by allowing for table-less web design). CSS can also allow the same markup page to be presented in different styles for different rendering methods, such as on-screen, in print, or by voice (when read out by a speech-based browser or screen reader) (World Wide Web Consortium , 2008). MYSQL, also called "My Structured Query Language," is a relational database management system (RDBMS). The program runs as a server providing multi-user access to a number of databases. A relational database stores data in separate tables rather than putting all the data in one big storeroom. This adds speed and flexibility. The SQL also called “Structured Query Language is the most common query language that is used to access databases (Ramakrishnan and Gehrke, 2009). To add, access, and process data stored in a computer database, we need a database management system such as MYSQL Server.

The TigerPlace EMR application represented the client-server model, where the client machine (end user) sends requests to the server, and after processing the request, the server responds back to the client machine. The TigerPlace EMR system contains diverse medical components (EMR information, reports, elopement forms, and clinical forms) that record the residents' health status and helps nurse care coordinators and other members of the healthcare team in making informed clinical decisions. Furthermore, the data are easily accessible and are displayed in a meaningful way.

2.1 EMR Login Interface

To access the TigerPlace EMR system, the user first types the application URL in the browser (IE, Google Chrome, Firefox, etc.), the user will then encounter the MU login page where he/she must enter the MU login credentials. Once the MU login credential is authenticated, the user will be directed to the application login page, where he or she will again enter the username and password created for this particular application to access the application for charting and viewing previous records. Figure 3 below shows the login interface of the TigerPlace EMR application.



Tiger Place

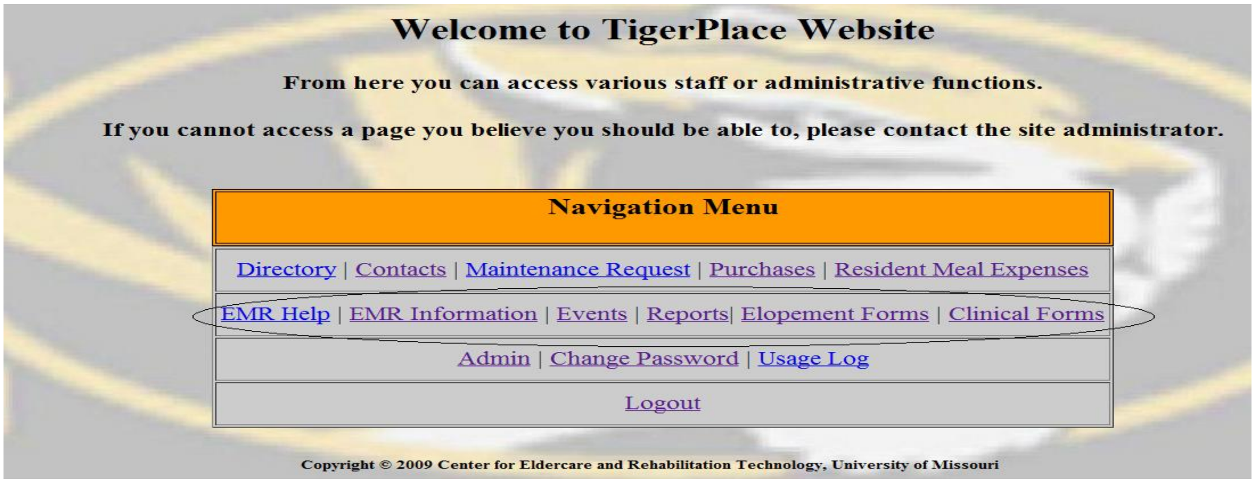
Username: TigerPlace

Password: ••••••

Copyright © 2008 TigerPlace. All rights reserved.

Fig 3 - Login Interface of TigerPlace EMR System

Upon successful authentication of login credentials on the login interface, the user will be directed to the navigation menu that constitutes all modules of the EMR system. Figure 4 below shows the main/navigation page of the EMR system that healthcare teams can access for charting the medical records of the TigerPlace residents.



Welcome to TigerPlace Website

From here you can access various staff or administrative functions.

If you cannot access a page you believe you should be able to, please contact the site administrator.

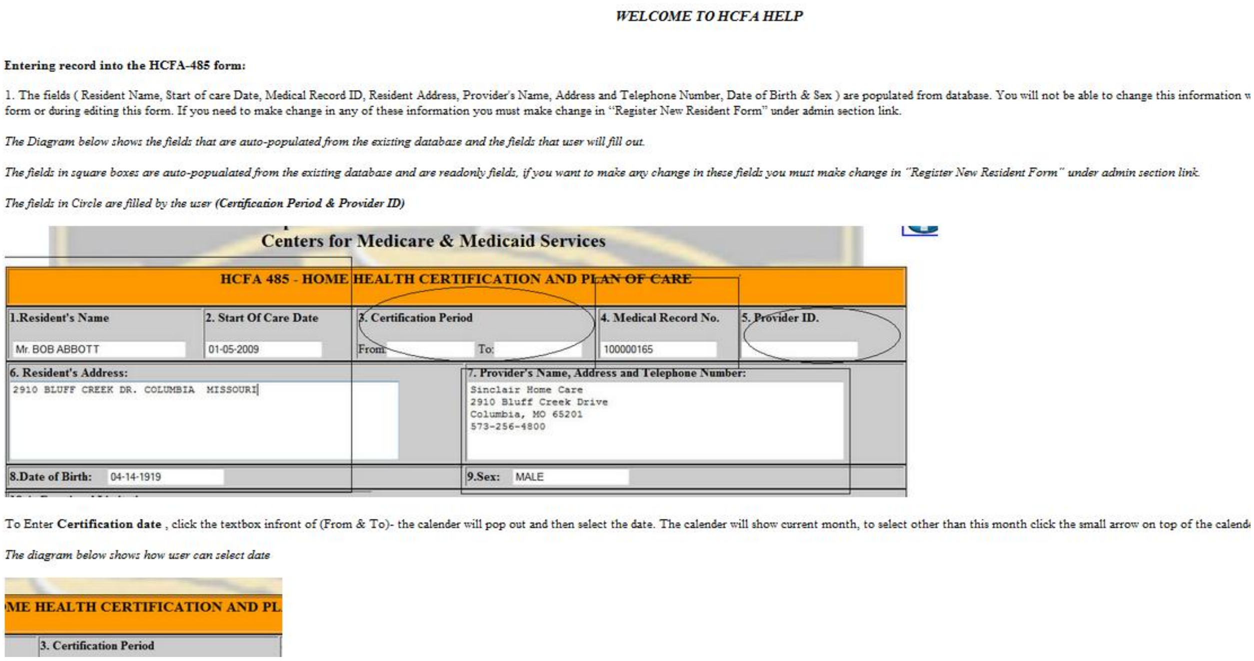
Navigation Menu
Directory | Contacts | Maintenance Request | Purchases | Resident Meal Expenses
EMR Help | EMR Information | Events | Reports| Elopement Forms | Clinical Forms
Admin | Change Password | Usage Log
Logout

Copyright © 2009 Center for Eldercare and Rehabilitation Technology, University of Missouri

Fig 4 - Navigation Menu

2.2 EMR Help Module

The EMR Help Module contains the documentation, including step-by-step screenshots of each and every module. The purpose of designing and integrating this module was to assist and guide the end users (clinical staff) about how to use each and every web form of the EMR system for charting care. Figure5 below illustrates the example of EMR Help module.



WELCOME TO HCFA HELP

Entering record into the HCFA-485 form:

1. The fields (Resident Name, Start of care Date, Medical Record ID, Resident Address, Provider's Name, Address and Telephone Number, Date of Birth & Sex) are populated from database. You will not be able to change this information w form or during editing this form. If you need to make change in any of these information you must make change in "Register New Resident Form" under admin section link.

The Diagram below shows the fields that are auto-populated from the existing database and the fields that user will fill out.

The fields in square boxes are auto-popualated from the existing database and are readonly fields, if you want to make any change in these fields you must make change in "Register New Resident Form" under admin section link.

*The fields in Circle are filled by the user **(Certification Period & Provider ID)***

Centers for Medicare & Medicaid Services

HCFA 485 - HOME HEALTH CERTIFICATION AND PLAN OF CARE

1.Resident's Name: Mr. BOB ABBOTT

2. Start Of Care Date: 01-05-2009

3. Certification Period: From: To:

4. Medical Record No.: 100000165

5. Provider ID.:

6. Resident's Address:
2910 BLUFF CREEK DR. COLUMBIA MISSOURI

7. Provider's Name, Address and Telephone Number:
Sinclair Home Care
2910 Bluff Creek Drive
Columbia, MO 65201
573-256-4800

8.Date of Birth: 04-14-1919

9.Sex: MALE

To Enter **Certification date** , click the textbox infront of (From & To)- the calender will pop out and then select the date. The calender will show current month, to select other than this month click the small arrow on top of the calend

The diagram below shows how user can select date

ME HEALTH CERTIFICATION AND PL

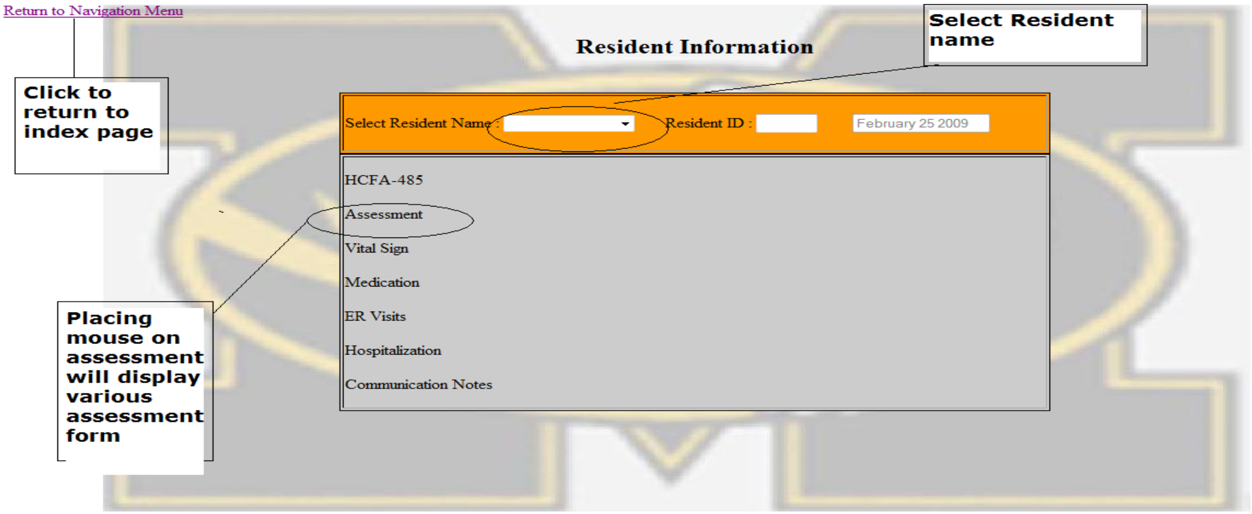
3. Certification Period

Fig 5 – Help Section

2.3 EMR Information Module

The EMR information module is one of the main modules of the entire EMR system developed for TigerPlace to record most patient-related medical information. This module contains HCFA-485 form, Assessment forms (SF-12, Mood scale, Fall Assessment, Mini-Mental State Exam), and Vital Signs, Medications, Hospitalization, Emergency Room (ER) Visits, Communication

Notes, Activities of Daily Living (ADL), and Instrumental Activities of Daily Living (IADL) forms. Figure 6 below shows the detailed EMR information module.



Click to return to index page

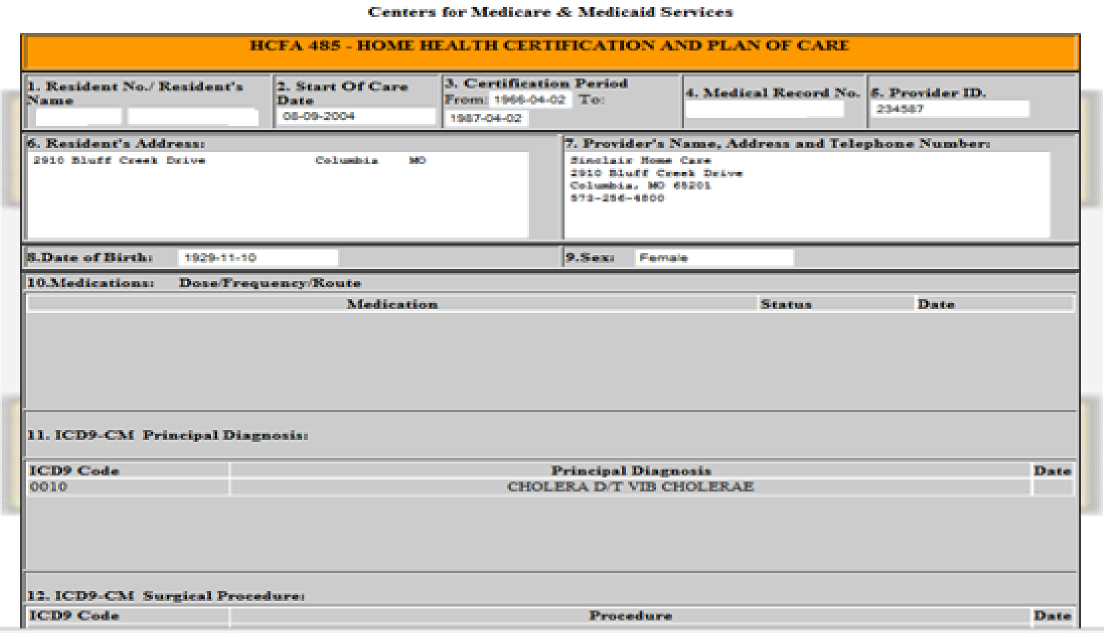
Select Resident name

Placing mouse on assessment will display various assessment form

Fig 6 - EMR Information Module

The HCFA-485 form is used for home health and plan of care certification and re-certification. Information recorded in this form is categorized under four sections; resident's detail, medication detail, health status, and provider information.

Resident detail includes resident name, resident ID, sex, date of birth, start of care date, and resident address. Medication details include International Statistical Classification of Diseases codes (ICD-9), durable medical equipment (DME) and supplies, safety measures, nutritional requirements, and allergies. Health status of resident includes information about functional limitations, such as hearing, paralysis, speech etc; activities permitted, such as wheel chair, walker, cane, crutches, etc; mental status, such as oriented, forgetful, and agitated; and prognosis, such as poor, fair, good, etc. Finally, the provider section of this form includes provider information, including provider name, address, phone number, ID Number, and the signature of the provider. Figure 7 below shows the interface of the HCFA-485 form.



Centers for Medicare & Medicaid Services

HCFA 485 - HOME HEALTH CERTIFICATION AND PLAN OF CARE

1. Resident No./ Resident's Name

2. Start Of Care Date: 08-09-2004

3. Certification Period From: 1966-04-02 To: 1987-04-02

4. Medical Record No.

5. Provider ID. 234587

6. Resident's Address:
2910 Bluff Creek Drive Columbia MO

7. Provider's Name, Address and Telephone Number:
Sinclair Home Care
2910 Bluff Creek Drive
Columbia, MO 65201
573-256-4800

8.Date of Birth: 1929-11-10

9.Sex: Female

10.Medications: Dose/Frequency/Route

Medication	Status	Date

11. ICD9-CM Principal Diagnosis:

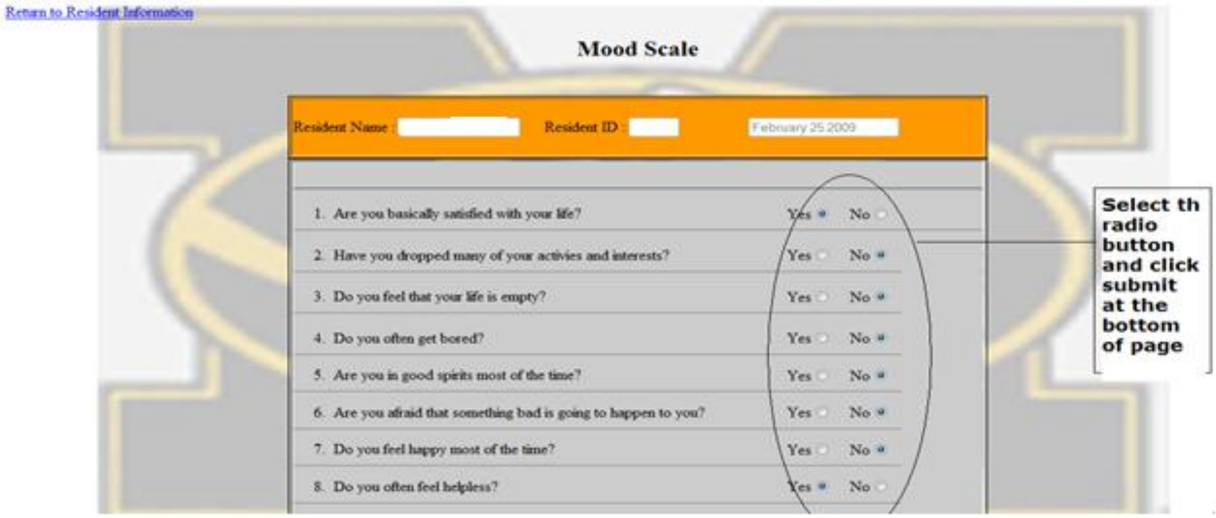
ICD9 Code	Principal Diagnosis	Date
0010	CHOLERA D/T VIB CHOLERAE	

12. ICD9-CM Surgical Procedure:

ICD9 Code	Procedure	Date

Fig 7 - HCFA- 485 Form

Assessment forms (Short Form -12, Mood Scale, Fall Assessment, and Mini-Mental State Exam) are designed to determine the physical and mental health status of the residents. For instance, mood scale forms concentrate on the cognitive aspects of functioning, including questions about the patient's mood or such abnormal experiences as confusion. Cognitive performance scales are used most often to evaluate older adults for delirium, dementia, detect cognitive decline, follow the course of the resident's illness, and monitor responses to treatment. These assessment forms contain sets of questions and options (radio buttons, checkboxes, and textbox) for answering each question. Whenever clinical staff selects options and submits the form, it calculates the scores based on the values and formula set for each option. These scores are then used by the healthcare team to determine residents' current health status and to develop the care plan to address healthcare needs, incorporating assessment modules in the EMR system that assess physical and cognitive health changes to assist the healthcare team in early detection of potential problems. Figure 8 and Figure 9 below show how the Mood Scale assessment form works.



Return to Resident Information

Mood Scale

Resident Name : Resident ID : February 25 2009

1. Are you basically satisfied with your life? Yes ● No ○

2. Have you dropped many of your activies and interests? Yes ○ No ●

3. Do you feel that your life is empty? Yes ○ No ●

4. Do you often get bored? Yes ○ No ●

5. Are you in good spirits most of the time? Yes ○ No ●

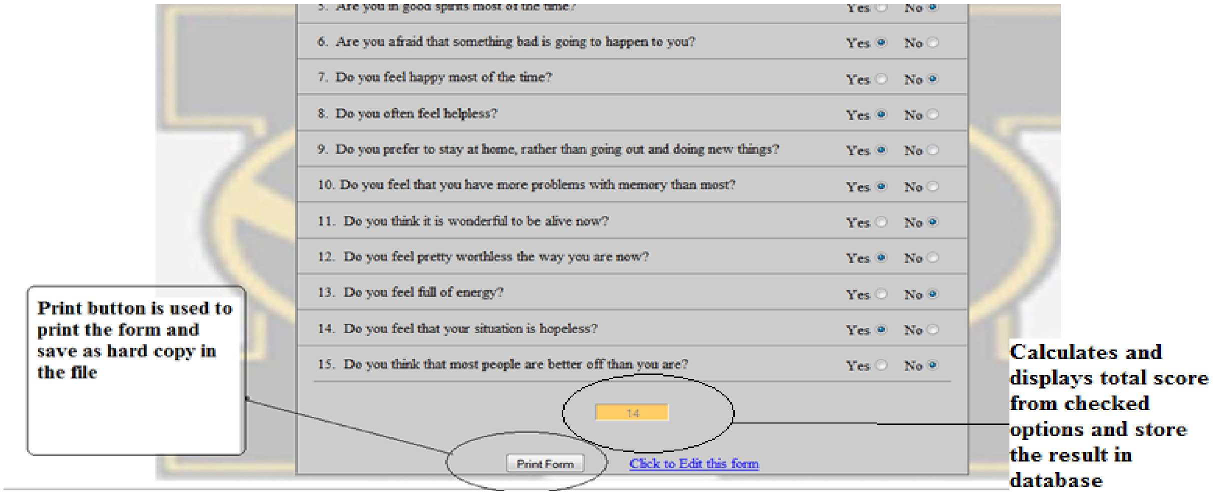
6. Are you afraid that something bad is going to happen to you? Yes ○ No ●

7. Do you feel happy most of the time? Yes ○ No ●

8. Do you often feel helpless? Yes ● No ○

Select th radio button and click submit at the bottom of page

Fig 8 – Mood-Scale (Before Survey)



5. Are you in good spirits most of the time? Yes ○ No ●

6. Are you afraid that something bad is going to happen to you? Yes ● No ○

7. Do you feel happy most of the time? Yes ○ No ●

8. Do you often feel helpless? Yes ● No ○

9. Do you prefer to stay at home, rather than going out and doing new things? Yes ● No ○

10. Do you feel that you have more problems with memory than most? Yes ● No ○

11. Do you think it is wonderful to be alive now? Yes ○ No ●

12. Do you feel pretty worthless the way you are now? Yes ● No ○

13. Do you feel full of energy? Yes ○ No ●

14. Do you feel that your situation is hopeless? Yes ● No ○

15. Do you think that most people are better off than you are? Yes ○ No ●

14

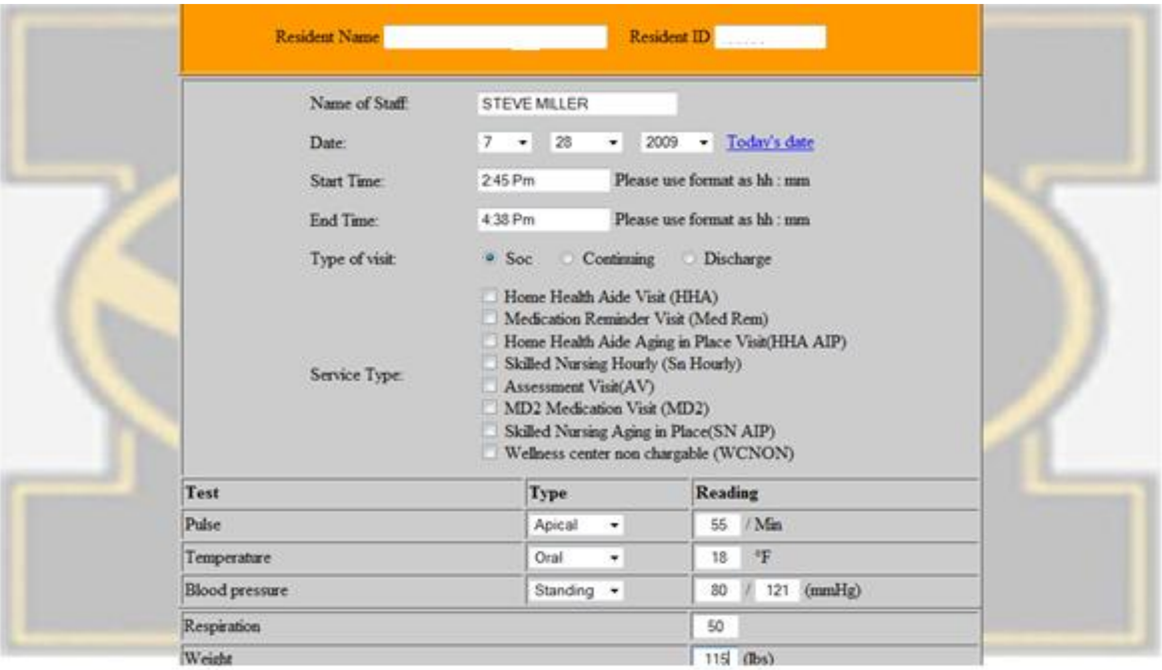
Print Form Click to Edit this form

Print button is used to print the form and save as hard copy in the file

Calculates and displays total score from checked options and store the result in database

Fig 9- Mood-Scale (After Survey)

Vital Signs are measurements of the body's most basic functions. The seven main vital signs routinely monitored by the healthcare team are incorporated in the Vital Signs form. In this form, the seven vital signs are under the heading “Test” column. The medical professionals can also select type associated with test under the heading “Type” and can enter the reading in the text box under the “Reading” column. The temperature is measured in Fahrenheit, weight is measured in pounds, and the pain reading scale is entered from the drop down list under the “Reading” column. In addition to these elements, also documented are name of visiting staff, date, time, type of visit, and service type. There is also a set of questions related to vital signs with radio button options. Figure 10 shows the Vital Signs web interface to record the vital signs for each resident in the TigerPlace.



Resident Name Resident ID

Name of Staff: STEVE MILLER

Date: 7 28 2009 Today's date

Start Time: 2:45 Pm Please use format as hh : mm

End Time: 4:38 Pm Please use format as hh : mm

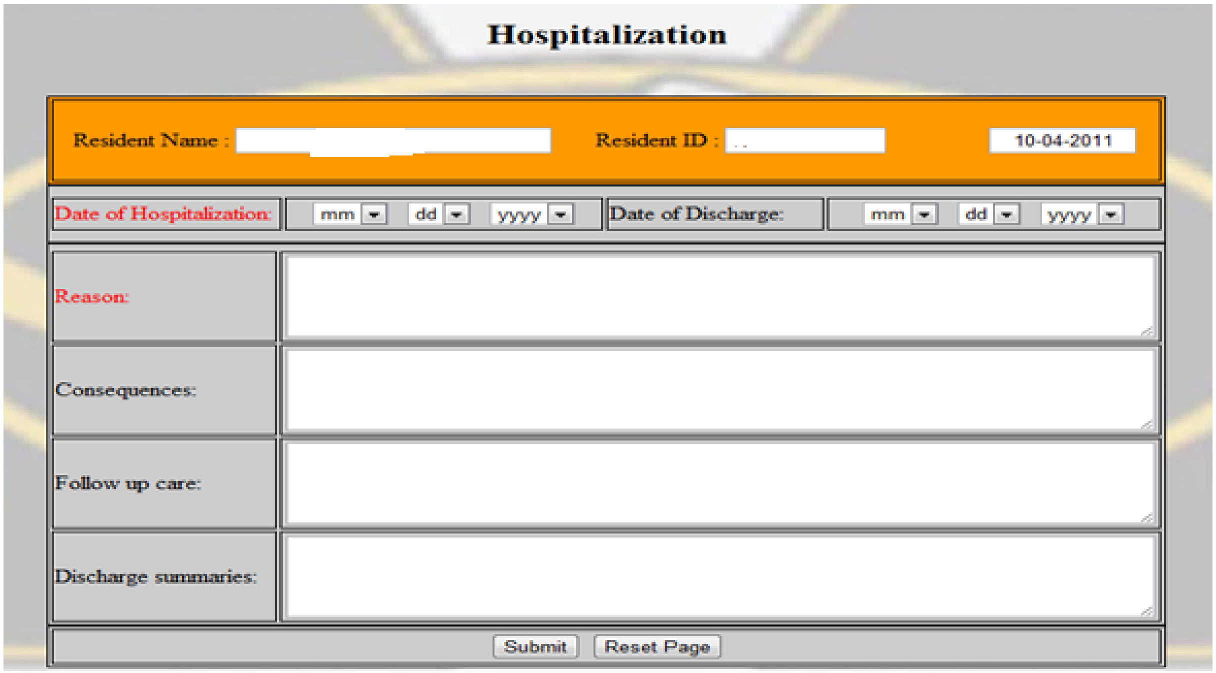
Type of visit: ● Soc ○ Continuing ○ Discharge

Service Type:
□ Home Health Aide Visit (HHA)
□ Medication Reminder Visit (Med Rem)
□ Home Health Aide Aging in Place Visit(HHA AIP)
□ Skilled Nursing Hourly (Sn Hourly)
□ Assessment Visit(AV)
□ MD2 Medication Visit (MD2)
□ Skilled Nursing Aging in Place(SN AIP)
□ Wellness center non chargable (WCNON)

Test	Type	Reading
Pulse	Apical	55 / Min
Temperature	Oral	18 °F
Blood pressure	Standing	80 / 121 (mmHg)
Respiration		50
Weight		115 (lbs)

Fig 10 - Vital Signs Form

ER visit/Hospitalization forms are designed to keep track of the resident who is admitted to the hospital or ER. The information that is recorded in these forms includes reason for admission, consequences, orders for follow up care, dates of hospitalization, and discharge. The date of visit and reason field was validated using JavaScript function, so that the end user cannot skip this vital piece of information as it is necessary to record for future reference. Figure-11 displays the interface of the hospitalization form with mandatory fields marked in red text.



Hospitalization

Resident Name :

Resident ID :

10-04-2011

Date of Hospitalization: mm dd yyyy

Date of Discharge: mm dd yyyy

Reason:

Consequences:

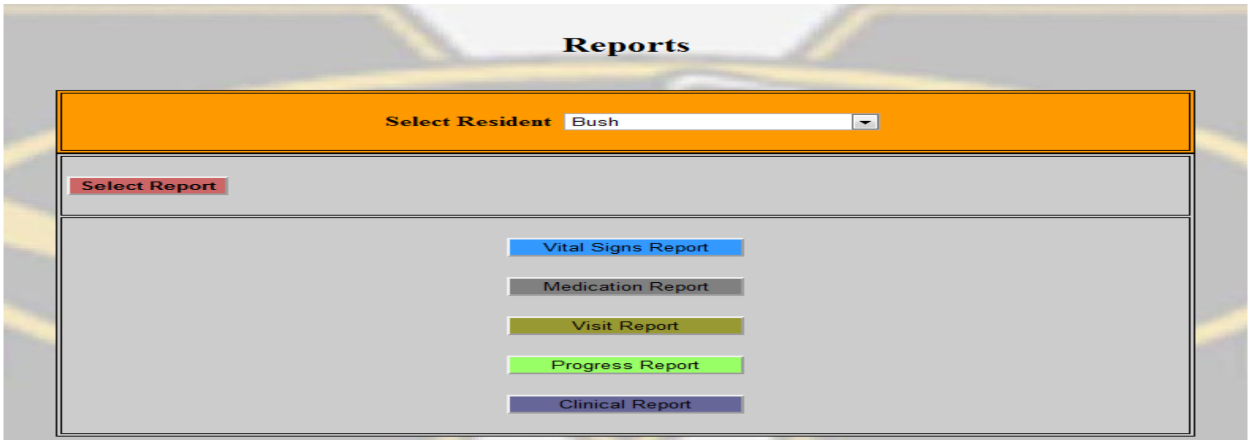
Follow up care:

Discharge summaries:

Fig 11 – Hospitalization Web Interface

2.4 Report Module

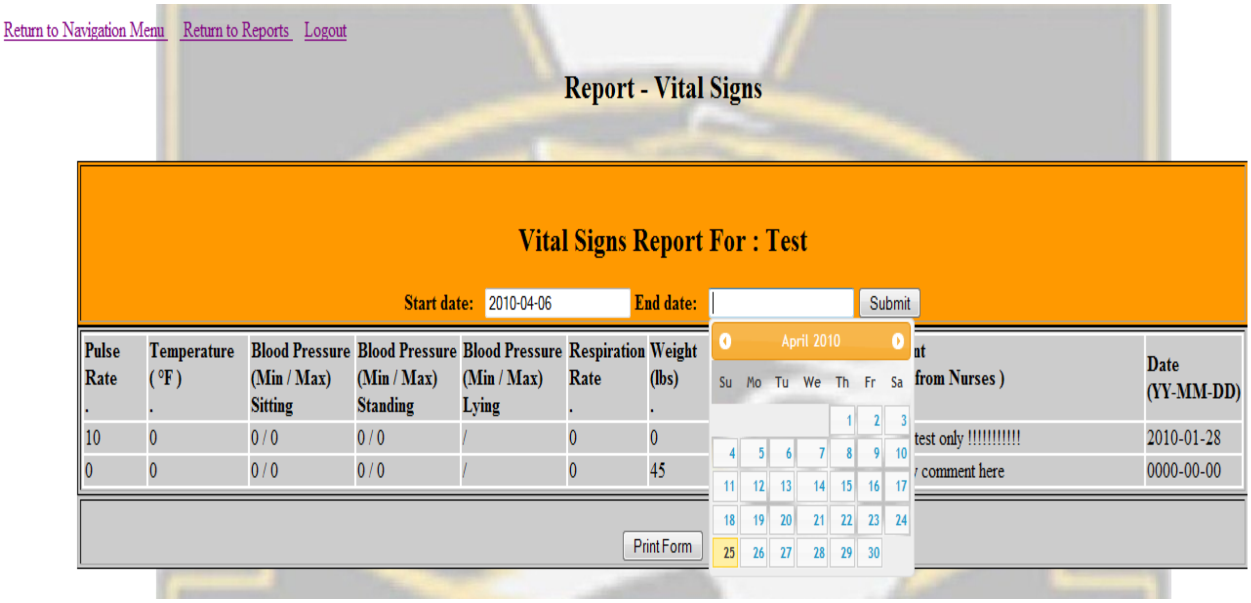
Whenever clinical staff needs to view the report of a particular resident, the first user will select the name of the resident from the drop down list on this report module (Figure 12), and then the user will select the name of the report that they wish to see. Figure 13 displays how the report looks when the user selects the vital signs report after selecting the resident's name.



Reports

Select Resident: Bush

Fig 12- Report Module



Report - Vital Signs

Vital Signs Report For : Test

Start date: 2010-04-06 End date:

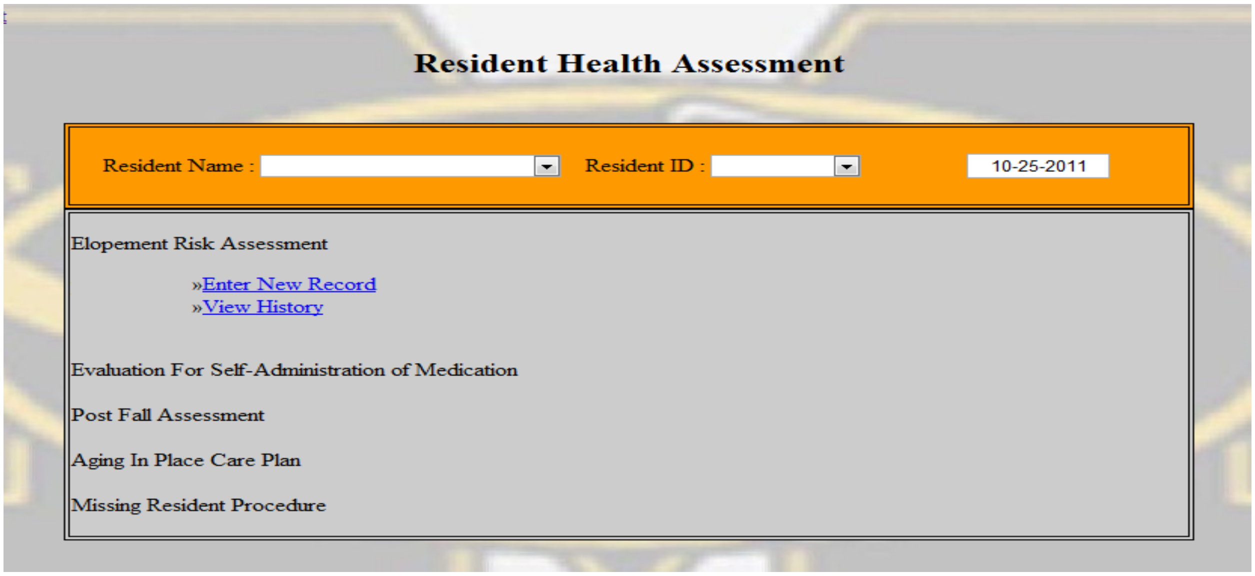
Pulse Rate .	Temperature (°F) .	Blood Pressure (Min / Max) Sitting	Blood Pressure (Min / Max) Standing	Blood Pressure (Min / Max) Lying	Respiration Rate .	Weight (lbs) .	nt from Nurses)	Date (YY-MM-DD)
10	0	0 / 0	0 / 0	/	0	0	test only !!!!!!!!!!	2010-01-28
0	0	0 / 0	0 / 0	/	0	45	comment here	0000-00-00

Fig 13 - Vital Signs Report

In these reports, the end user can also filter the records by selecting the start and end date. For instance, if the user would like to check the vital signs for resident "X" for a specific date range, on clicking the mouse in the start date field, the calendar will appear where the user can select the day/month/year and, similarly, on clicking the mouse in the end date field, another calendar will appear where the user can select the day/month/year. On hitting the "Submit" button, all the vital signs recorded within this date range will be displayed. The purpose of incorporating the calendar was to improve the end user visualization of the resident’s medical records by filtering the records.

2.5 Elopement Module

The “Elopement Module,” also called “Resident Health Assessment Module,” contains five forms that are designed to record and assess the resident’s health and medical condition. Figure 14 below displays the structure of the “Elopement” Module.



Resident Health Assessment

Resident Name :

Resident ID :

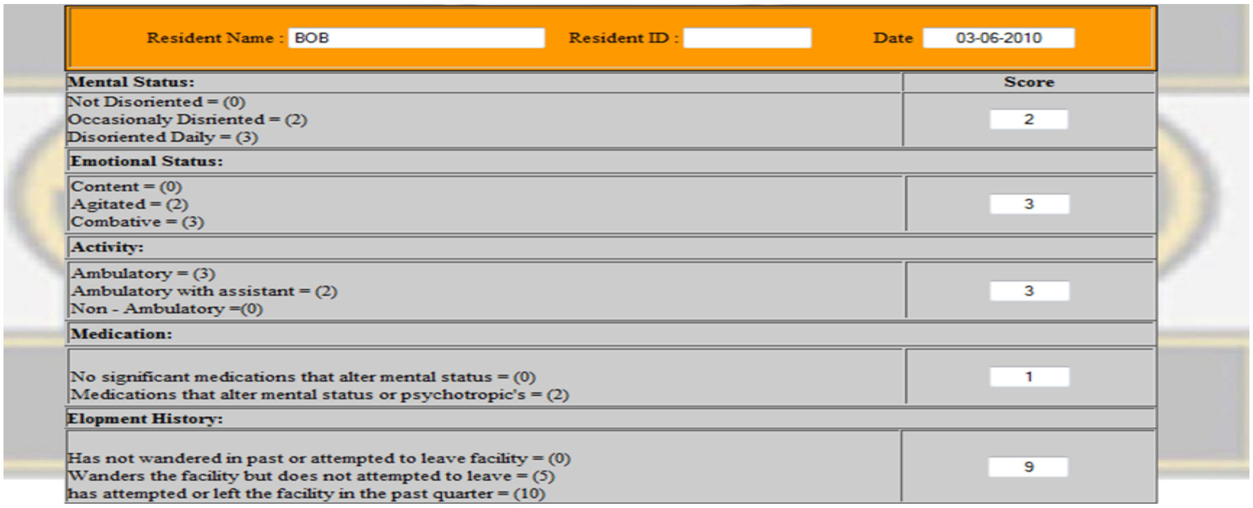
10-25-2011

Elopement Risk Assessment
»Enter New Record
»View History
Evaluation For Self-Administration of Medication
Post Fall Assessment
Aging In Place Care Plan
Missing Resident Procedure

Fig 14 - Elopement Module/Resident Health Assessment Module

The five forms that were designed under the elopement module include:

Elopement Risk Assessment: Elopement risk assessment captures the information of the resident regarding mental status, emotional status, activity, medication, and elopement history. This form consists of a set of questions, with a value associated with each question that evaluates and determines the Tiger Place resident’s health. Figure 15 below displays the web interface of the “Elopement Risk Assessment” form.



Resident Name : BOB Resident ID : Date 03-06-2010

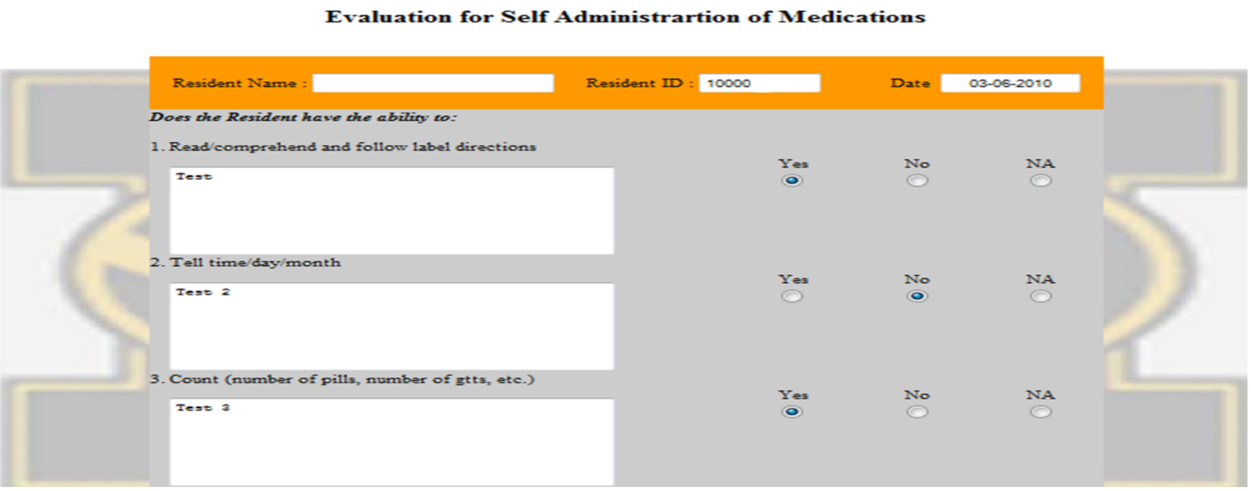
Mental Status:	**Score**
Not Disoriented = (0) Occasionaly Disriented = (2) Disoriented Daily = (3)	2
Emotional Status:	

Content = (0)
Agitated = (2)
Combative = (3)
	3

Activity:	
Ambulatory = (3) Ambulatory with assistant = (2) Non - Ambulatory =(0)	3
Medication:	
No significant medications that alter mental status = (0) Medications that alter mental status or psychotropic's = (2)	1
Elopment History:	
Has not wandered in past or attempted to leave facility = (0) Wanders the facility but does not attempted to leave = (5) has attempted or left the facility in the past quarter = (10)	9

Fig 15 - Elopement Risk Assessment Form

<u>*Evaluation of Self Risk Assessment:*</u> This form was designed to capture the information about the resident's ability to self-administer medications. For instance, "Does the resident have the ability to read and follow label directions?" Figure 16 below displays the structure of the "Evaluation of Self Risk Assessment" form.



Evaluation for Self Administrartion of Medications

Resident Name : Resident ID : 10000 Date 03-06-2010

Does the Resident have the ability to:

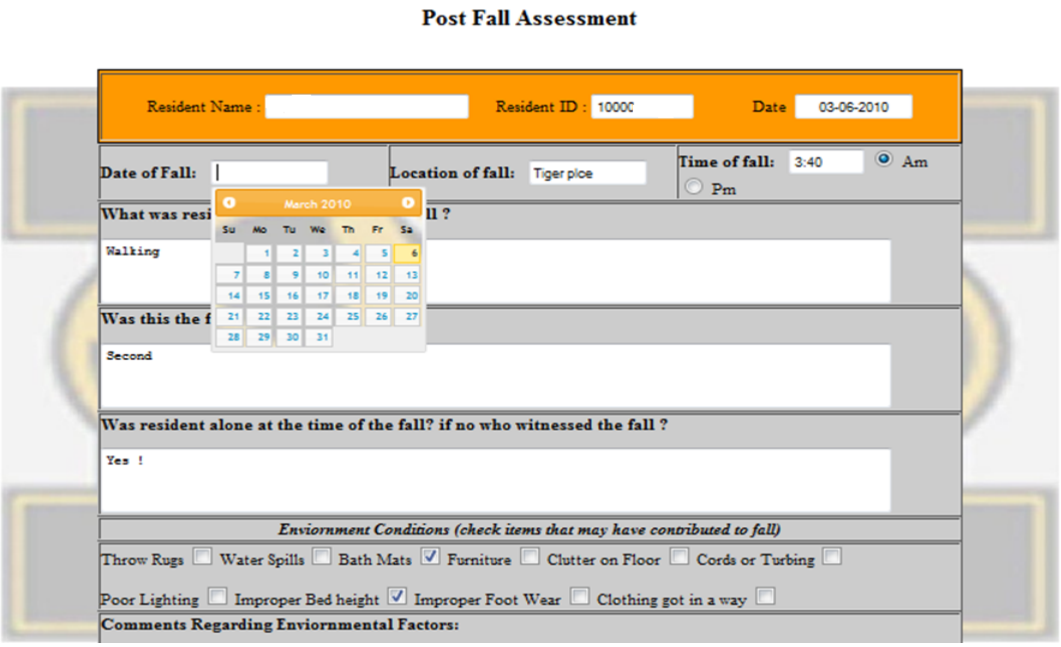
1. Read/comprehend and follow label directions — Test — Yes ● No ○ NA ○

2. Tell time/day/month — Test 2 — Yes ○ No ● NA ○

3. Count (number of pills, number of gtts, etc.) — Test 3 — Yes ● No ○ NA ○

Fig 16 - Evaluation for Self Risk Assessment Form

<u>Post Fall Assessment:</u> This form was designed to track and record the resident's fall event. This form is designed in such a way that it can record multiple fall events on a single day. Figure 17 below shows the interface of the "Post Fall Assessment" form.



Post Fall Assessment

Resident Name :

Resident ID : 1000(

Date 03-06-2010

Date of Fall: |

Location of fall: Tiger ploe

Time of fall: 3:40 ● Am ○ Pm

What was resi… ll ?

Walking

Was this the f…

Second

Was resident alone at the time of the fall? if no who witnessed the fall ?

Yes !

Enviornment Conditions (check items that may have contributed to fall)

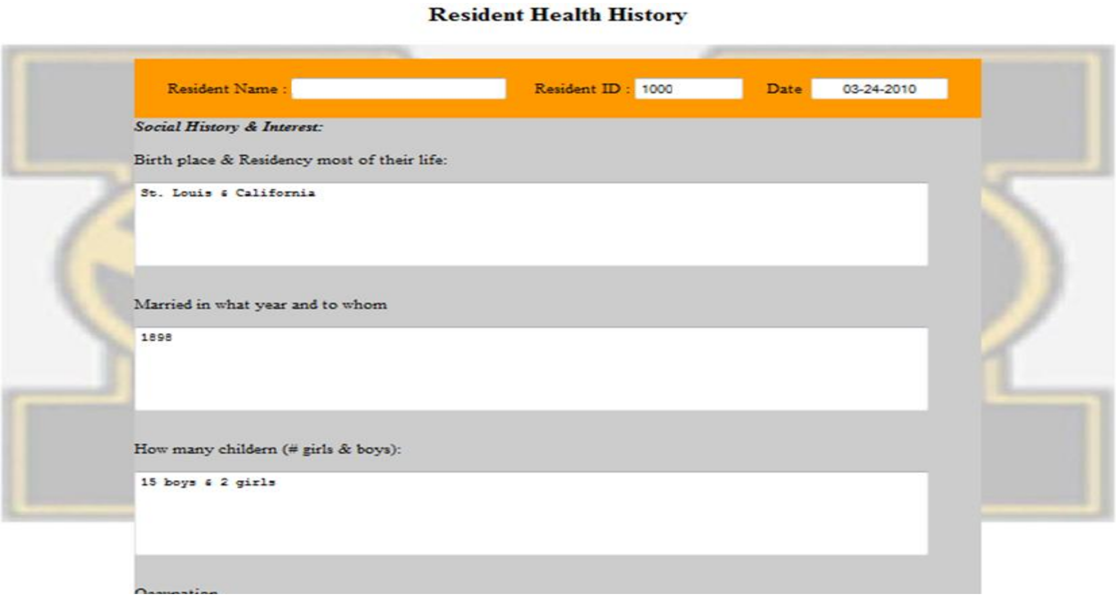
Throw Rugs □ Water Spills □ Bath Mats ☑ Furniture □ Clutter on Floor □ Cords or Turbing □

Poor Lighting □ Improper Bed height ☑ Improper Foot Wear □ Clothing got in a way □

Comments Regarding Enviornmental Factors:

Fig 17 – Post Fall Assessment

<u>Resident Health History</u>: This form was designed to record the personal and health history of all residents at TigerPlace. This form records information about residents' current ability to self-administer medicine or the ability to read, comprehend, and follow the label directions. Knowing this information will assist nurses and other medical staff members in determining their current status and providing effective and timely care to residents. Figure 18 below displays the structure of the "Resident Health History" form.



Resident Health History

Resident Name :
Resident ID : 1000
Date 03-24-2010

Social History & Interest:

Birth place & Residency most of their life:

St. Louis & California

Married in what year and to whom

1898

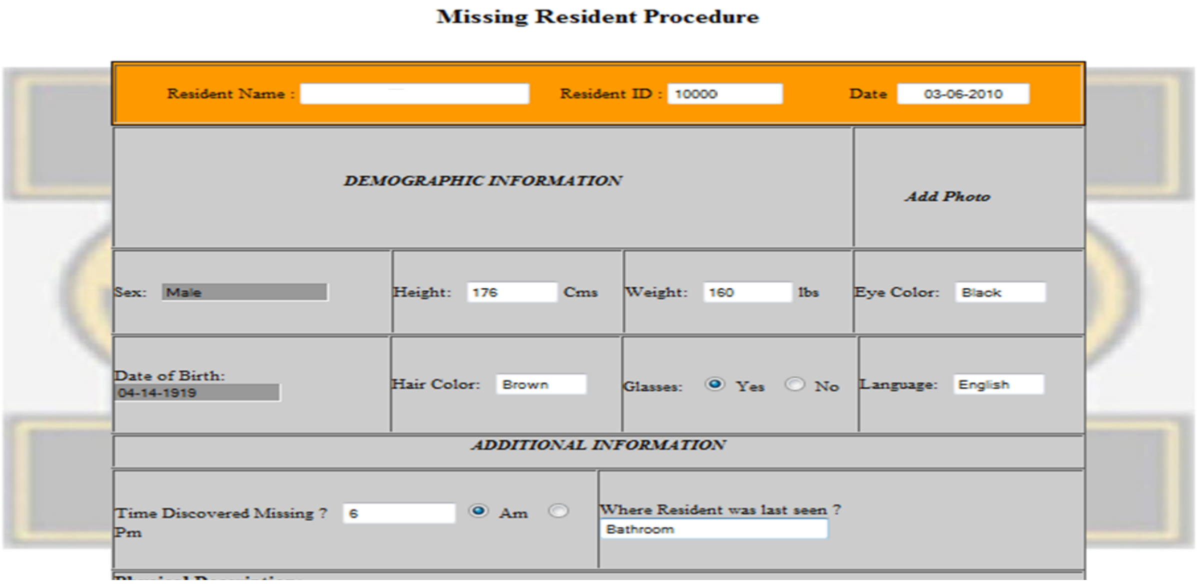
How many childern (# girls & boys):

15 boys & 2 girls

Occupation

Fig 18 – Resident Health History Interface

Missing Resident Procedure: This form was designed to record and keep track of residents who might become missing from TigerPlace. It records information related to the physical appearance of the resident (eye color, weight, height, hair color, wore glasses, etc.), and also includes the language they speak, date/time when they were found to be missing, and other pertinent information that can assist staff to recover the missing resident. Figure 19 below displays the structure of the "Missing Resident Procedure" form.



Missing Resident Procedure

Resident Name : Resident ID : 10000 Date 03-06-2010

DEMOGRAPHIC INFORMATION	*Add Photo*

Sex: Male	Height: 176 Cms	Weight: 160 lbs	Eye Color: Black
Date of Birth: 04-14-1919	Hair Color: Brown	Glasses: ● Yes ○ No	Language: English

ADDITIONAL INFORMATION

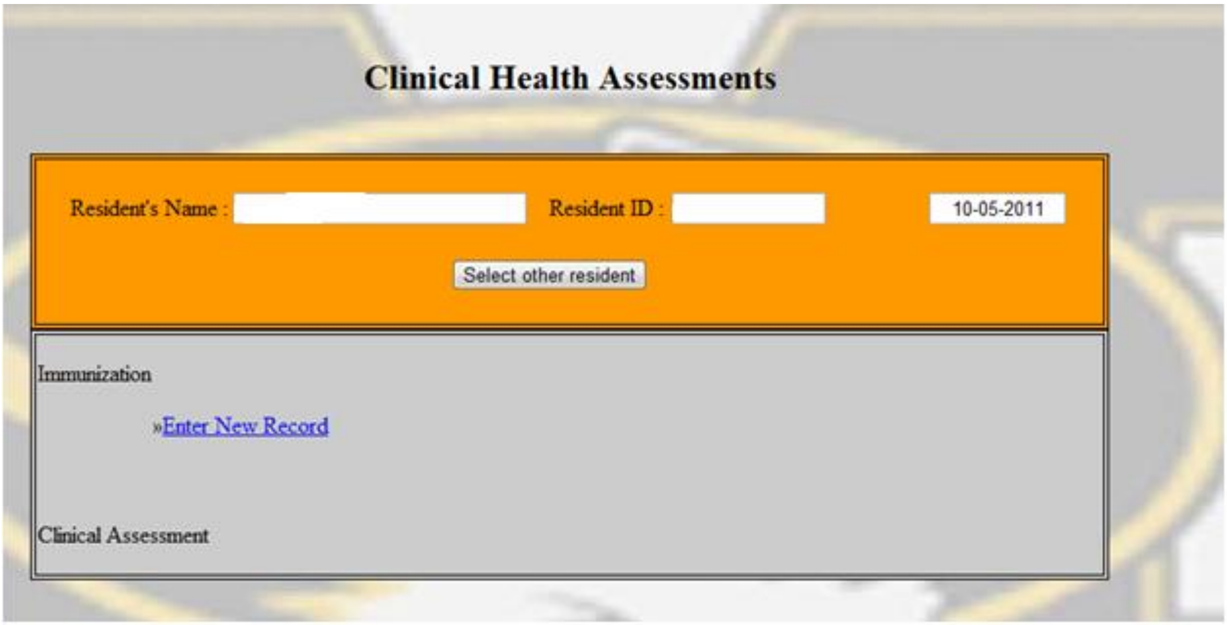
Time Discovered Missing ? 6 ● Am ○ Pm	Where Resident was last seen ? Bathroom

Physical Description

Fig 19 – Missing Resident Procedure Form

2.6 Clinical Forms Module

The Clinical Forms Module was designed and developed to record the immunizations/screening tests and other clinical assessments of TigerPlace residents. Figure 20 displays the structure of Clinical Forms Module. The Immunization and Screening form is used by clinical staff to record residents' immunizations, e.g., influenza, H1N1, and tetanus. It is also used to document screening tests, such as mammogram, chest x-ray (CXR), colonoscopy, vision, hearing, and dental. The results of immunization and screening tests are entered in the text field along with the date. Figure 21 displays the structure of the Immunization and Screening web form. The clinical assessment form is used by the staff to record lab results associated with diagnostic tests. Figure 22 displays the structure of the Clinical Assessment form.



Clinical Health Assessments

Resident's Name :

Resident ID :

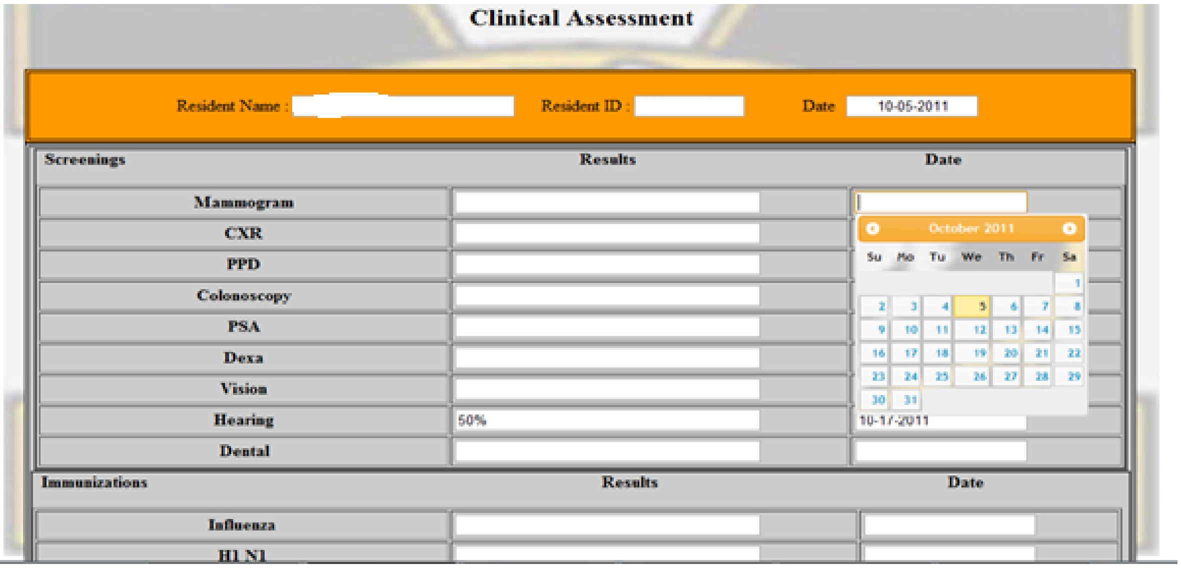
10-05-2011

Immunization

»Enter New Record

Clinical Assessment

Fig 20 - Clinical Health Module



Clinical Assessment

Resident Name :

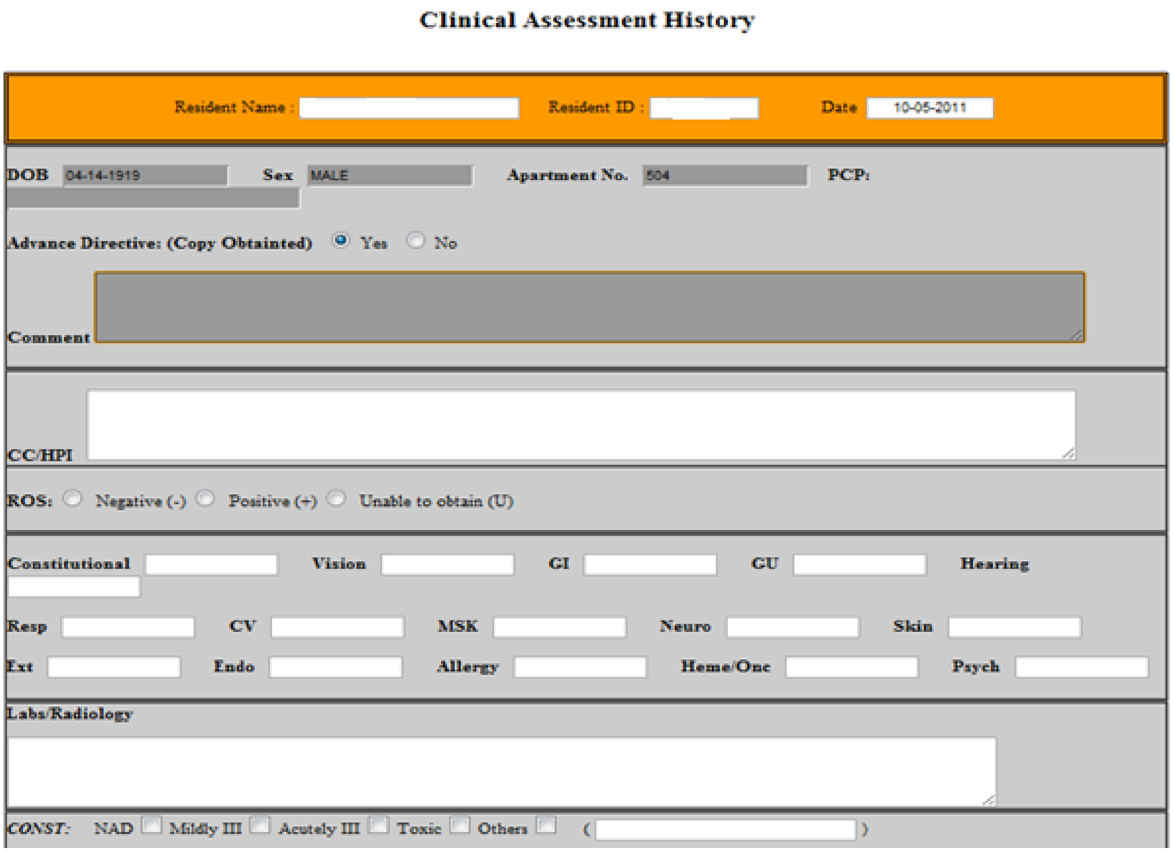
Resident ID :

Date 10-05-2011

Screenings	Results	Date
Mammogram		
CXR		
PPD		
Colonoscopy		
PSA		
Dexa		
Vision		
Hearing	50%	10-17-2011
Dental		

Immunizations	Results	Date
Influenza		
H1 N1		

Fig 21 – Immunization and Screenings Form



Clinical Assessment History

Resident Name : Resident ID : Date 10-05-2011

DOB 04-14-1919 Sex MALE Apartment No. 504 PCP:

Advance Directive: (Copy Obtainted) ● Yes ○ No

Comment

CC/HPI

ROS: ○ Negative (-) ○ Positive (+) ○ Unable to obtain (U)

Constitutional Vision GI GU Hearing

Resp CV MSK Neuro Skin

Ext Endo Allergy Heme/Onc Psych

Labs/Radiology

CONST: NAD □ Mildly Ill □ Acutely Ill □ Toxic □ Others □ ( )

Fig 22 - Clinical Assessment Form

Screenshots of other clinical web forms are included in the appendix section.

2.7 Flowchart of EMR System

The flowchart below (Figure 23) describes the functioning or the algorithm that is used for one of the modules of the TigerPlace EMR system. The arrows represent the flow of control (how the web forms are linked to each other) and boxes represent the operations (medical forms) that are performed. Whenever any clinical staff members want to access the EMR, the first window encountered is the login page, where they will be asked to enter their login credentials and, if username and password are correct, they will be granted access to all the EMR modules for charting and viewing/editing the previous records. If the login credential is invalid, they will be prompted with an error message and will be re-directed to the login page.

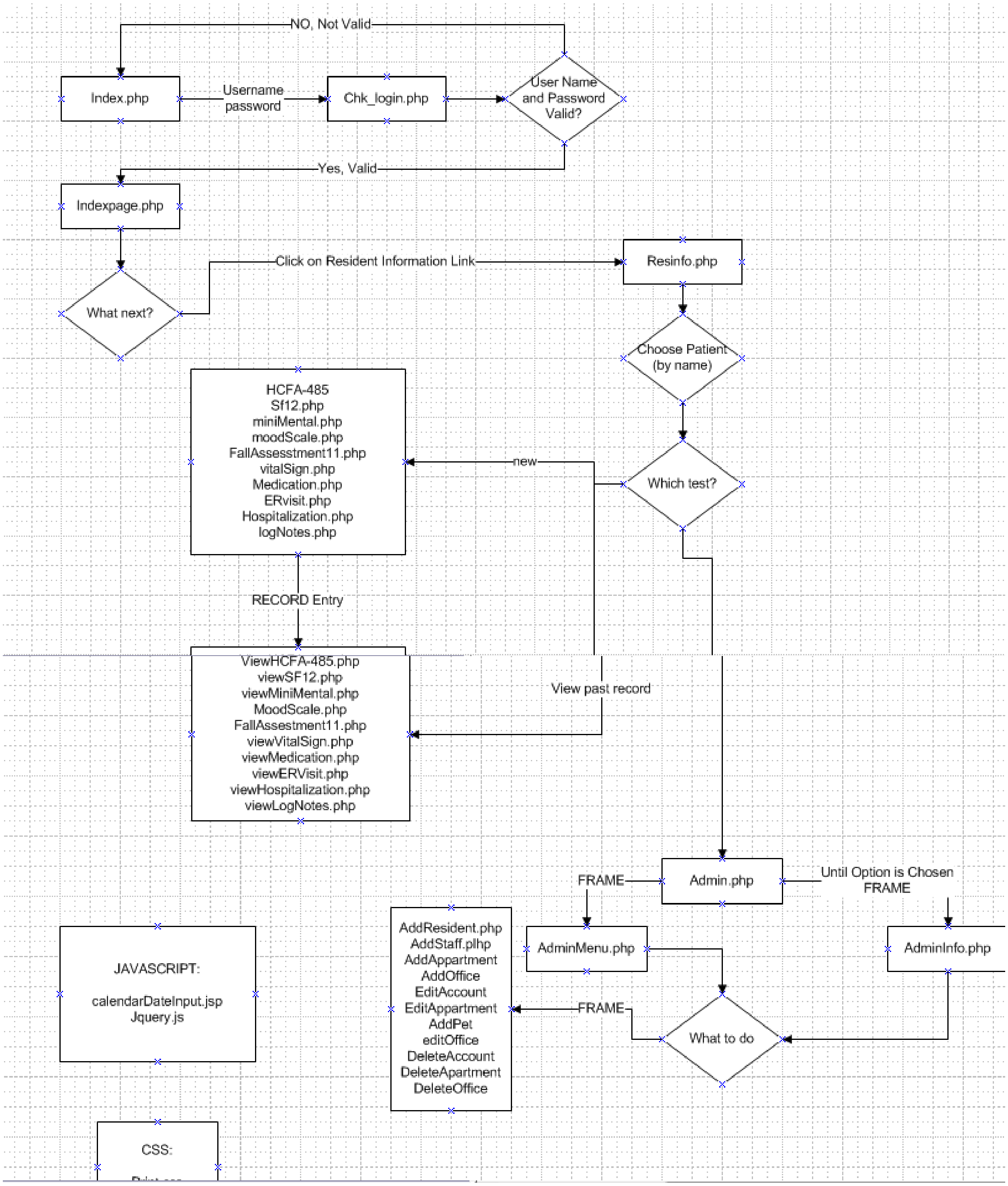


Fig 23 - Flowchart of EMR System

CHAPTER 3

LITERATURE REVIEW

3.1 Literature Review Methodology

The literature review methodology section is composed of six parts: Health Insurance Portability and Accountability Act (HIPAA) rules and regulations on use of EMR systems, importance of information system security in healthcare settings, need for TigerPlace EMR security, web application vulnerabilities, database security and concerns, and security programs. A review of the HIPAA Federal requirements was done to identify issues specific to the protection and security of web-based EMRs. In addition to this, research specific to web application security tools, methods to identify security concerns associated with web applications, and common security measures that can be integrated in the web application to protect it from malicious users were identified. To cover the scope and content of the research topic, COMPENDEX, ACM Digital Library, MEDLINE, CINAHL, Google, OVID, and PubMed databases, using the keywords and phrases EMR, confidentiality, information security, privacy, web security, information systems, HIPAA, security needs, web application vulnerabilities, access control, authorization, authentication, and web EMR benefits, were used. To filter the results obtained from these keywords and phrases, and to search for more precise results, “AND” and “OR” operators were used to combine keywords and phrases. The COMPENDEX, MEDLINE, and CINAHL databases were used to obtain information about information technology, security concerns related to web applications, compliance issues, and patients’ privacy. COMPENDEX database mainly contains engineering and technology research literature, so IT related articles were more retrieved from COMPENDEX, and MEDLINE database mainly contains biomedical literature, so the recall for healthcare articles were more when this topic was exploded. The Google database was used to retrieve basic security related concerns within the web application, and the results obtained from the Google database were searched against various medical databases to retrieve more precise and accurate information. The OVID, PubMed, and ACM Digital Library databases were used to search for the HIPAA compliance rule for EMR systems and security risks.

I started my search with breaking down this search topic into smaller units or keywords and combining the keywords to narrow down the search results. First, I used the keywords and phrases EMR, confidentiality, information security, information systems, health information privacy, web security, information systems, HIPAA, security needs, web application vulnerabilities, access control, authorization, authentication, and web EMR benefits. When I searched for the keyword HIPAA, the search produced me a return of 2605 results. Then I narrowed this search result by exploding the HIPAA topic and selecting only the health information privacy and this search returned me with 55 results. Then I turned to the next keyword security, this search resulted me with 58112 articles. In the 3rd search, I turned too looked for word EMR confidentiality and this returned me with 118. To narrow down the search again, I combined the keywords EMR confidentiality and HIPAA and it produced me with 2 results with AND operator and 425 results when search with OR operator. In 4th and 5th search I searched for keyword web application and access control, it resulted me 836 and 522 article respectively. For the 6th search I turned to the next keywords authentication, I found many subject headings 2346, however I narrowed my search strategy by choosing combining these 2 keywords and I found 5 articles. After combining these 2 keywords, my 8th search was information security and again I was awarded with 345 articles. In the next search, I combined the term HIPAA and information security and it results me with 654 articles. In the 10th search I combined the term HIPAA, web application and security with the aim of finding the relationship between HIPAA regulation and security need for EMR system and this search produced me with 63135 articles. Finally, I looked for keywords Information system and nursing home to determine the usefulness of IT systems in nursing home and this search produced me 216 articles on combining with AND operator. After analyzing the results from various databases, 21 articles were selected that were most appropriate to the research topic.

3.2 HIPAA Rules and Regulations

According to HIPAA rules and regulations, any covered entity (healthcare providers, health plans, system vendors) that maintain or transmit electronic medical records of the patients from one system to another must develop, implement, and maintain reasonable and appropriate safeguards (administrative, physical, and technical) to ensure integrity, confidentiality, and availability of the patient information and to protect from unauthorized personnel the use or disclosure of the information. Confidentiality means the protection of information from unauthorized access by person, process, or system. Integrity refers to protecting the integrity of information, which includes the implementation of policies, processes, and technology that prevent or detect unauthorized modification of data. Availability refers to the ability of authorized users to access patients' records when and where they need (Department of Health and Human Services, 2003). "The rule requires covered entities to protect against reasonably anticipated security threats, to safeguard against reasonably anticipated violations of privacy, to ensure workforce compliance with the rule, and to periodically review and modify security measures in order to comply" (Department of Health and Human Services, 2003: 8334-8338).

3.2.1 Administrative Safeguards

The administrative safeguards outlined by HIPAA rules and regulations are categorized in two groups: required or addressable implementation specification. The required specification implies that covered entities are obligated to meet certain specifications, which include risk analysis and management, sanction policy, information system activity review, data backup plan, disaster recovery plan, response, and reporting. The addressable implementation specification allows covered entities additional flexibility with respect to compliance with security standards. The covered entity has flexibility to decide whether it is reasonable to deploy the addressable implementation specification and appropriate security measures to apply within the security framework. Some of the addressable implementation specifications include authorization/supervision, access authorization, log-in monitoring, password management, and testing and revision procedures (Department of Health and Human Services, 2003).

3.2.2 Technical Safeguards

With the increased use of sophisticated IT technologies in healthcare settings, technical safeguards are very important to ensure integrity, confidentiality, and privacy of patients' vital information from unauthorized personnel. Healthcare organizations face various risks from internal and external sources, due to which the Office for Civil Rights has enforced technical safeguards that need to be addressed by covered entities to minimize the risk to EMR systems. The various technical safeguards mentioned in HIPAA rules and regulations include access control, audit trails, integrity, transmission security, and person or entity authentication. Access control is the way of ensuring that only the privileged entity has access to that part of information that is needed to perform the required operation, while blocking access to unauthorized entities. Audit control mechanisms examine and log all activities associated with the information system that can be used at a later stage for evaluating use of the entire information system by authorized users. Integrity of data is the addressable specification mentioned in HIPAA rules and regulations to ensure data are always in a consistent state and are not altered or destroyed by unauthorized personnel. Person or entity authentication is marked as a required feature that needs to be addressed by covered entities dealing with EMR systems. It includes features like automatic system logoff during idle state and unique user identification while accessing the system. Transmission security is another addressable implementation specification that deals with protecting data and information from unauthorized personnel, while transferring over communication lines or networks. The covered entity must use some type of encryption methodology when transferring vital data from one terminal or location to another (Department of Health and Human Services, 2003).

3.2.3 Physical Safeguards

To ensure data integrity, confidentiality, and availability of electronic health records, the HIPAA rules and regulations have proposed physical safeguards as necessary requirements. Physical access control can be achieved by a human (guard), through mechanical means, such as locks and keys, or through technological means. The physical safeguards include securing workstation location, physical access controls, media and equipment control, assigning security responsibilities, and policies and guidelines on use of workstations. Securing workstations ensures that EMR systems and equipment residing in a building are safe from natural and environmental hazards, and unauthorized users. The formal policies and procedures on use of workstations describe how to keep track of the physical use of electronic devices (media and equipment) by authorized users while limiting unauthorized use. Also described is the proper disposal of electronic equipment, such as destroying the hard drive before dumping into the trash, regular data backups and storage at secure locations (Department of Health and Human Services, 2003).

HIPAA requires a covered entity to ensure proper implementation of administrative, technical, and physical safeguards for the safe and secure transmission of patients'-related information between the systems in order to prevent disclosure of information from the unauthorized users. In addition to this, it also requires encrypting the patient-related information that is processed over the network (intra or internet). Since TigerPlace EMR system is a web-based application (which means all the information related to patients is exchanged or transmitted among the systems over the web) and HIPAA requires safe and secure transmission of patient-related information among the systems, various web-related security threats are evaluated and discussed in detail under the web security vulnerability section. To address the web-related vulnerabilities and secure the patient-related information from being misused by the unauthorized users, various methods and techniques (such as Fortify Scan to identify SQL injections, encryption, authorization and authentication mechanism, firewalls, backups, etc.), that are implemented within the TigerPlace EMR system are discussed in detail in chapter 5.

3.3 Security

Security refers to protecting vital and confidential data and information from unauthorized and malicious users. Information security plays a very important role in any setting. Most internationally renowned organizations have successfully implemented some kind of information security to protect data and information. Information security is a way of protecting computer-based information systems from demolition, alteration, and disclosure. There is a huge amount of personal and other information that flows from one network to another network or one device to another that needs to be secured from malicious users. Data and information can be protected from unauthorized access in a number of different ways. Some techniques for securing the information involve the use of software and hardware applications. One of the examples of software applications involves the use of antivirus software, which protects the computers from worms, viruses, and other harmful programs that can corrupt the data and information in the computer systems. Hardware-based security is more powerful in protecting information from unauthorized access, as it restricts the read and write access to the data and information. One of the examples of hardware-based security involves setting robust login credentials and setting the different levels of access/privileges. The setting of login access will block malicious users from accessing the information, thus preventing the information from theft and modification actions. Although software applications provide an immense range of security to data and information, still it is not adequate in providing effective and efficient protection to information from malicious users. So, it is very important to incorporate both the components (software and hardware-based security) into the systems to ensure reliability.

3.3.1 Importance of Information System Security

In recent years, the US healthcare industry has emphasized EMR security systems more than paper based records. With the increased use of EMR systems, a large amount of patient information (including personal, medical, billing, and other patient-related information) is being stored in computer systems on a daily basis, and is communicated/shared inside and outside the organization among physicians, nurses, other medical staff members for providing better and timely healthcare to the healthcare consumers. This has led to many security concerns and increased use of Information Security (IS) systems in the healthcare field for protecting vital patient data and information from unauthorized access and malicious users (Dennis, 2000).

Some of the reasons for securing patient records are:

1. Private insurers use patient personal and medical data to target customers for health care plans.

2. Pharmaceutical/ drug companies use patient medical data to promote their drug to the health care providers by knowing the medical conditions of the patients.

In order to ensure security and privacy of patients' data and information, HIPAA Privacy and Security rule has been enforced by the Health and Human Services (HHS) Office for Civil Rights. The violation of HIPAA rules and regulations by health care providers can result in penalties which includes large fines up to $250,000 and up to five years in prison (Frank, 2002). It has, therefore, become very important for any healthcare organization to have an effective layer of security for their computer systems that protect vital patient data and information from misuse by unauthorized individuals, and also to remain safe from the penalties of HIPAA Privacy and Security Act.

There is a number of security features incorporated into TigerPlace EMR. These features will be described in the next section.

3.4 Need for TigerPlace EMR Security

The need for incorporating security tools into the TigerPlace EMR systems arose because of two main factors. First, the TigerPlace EMR system is a web application that is designed and developed using PHP, JavaScript, HTML, Ajax and MYSQL as a database. Web-based information systems are exposed to many types of security risks and threats, since the information is processed on the web and any individual can access the website via the URL and can maliciously manipulate the code in the application. According to the 2002 Computer Crime and Security Survey, more than $320,000,000 has been lost through web application incidents in 2001. Figure 24 shows the trend of web application vulnerability from 2000 – 2010, as reported by HP DVLabs team. Figure 25 shows the web application vulnerability by type from 2000 – 2010, as reported by HP DVLabs team.

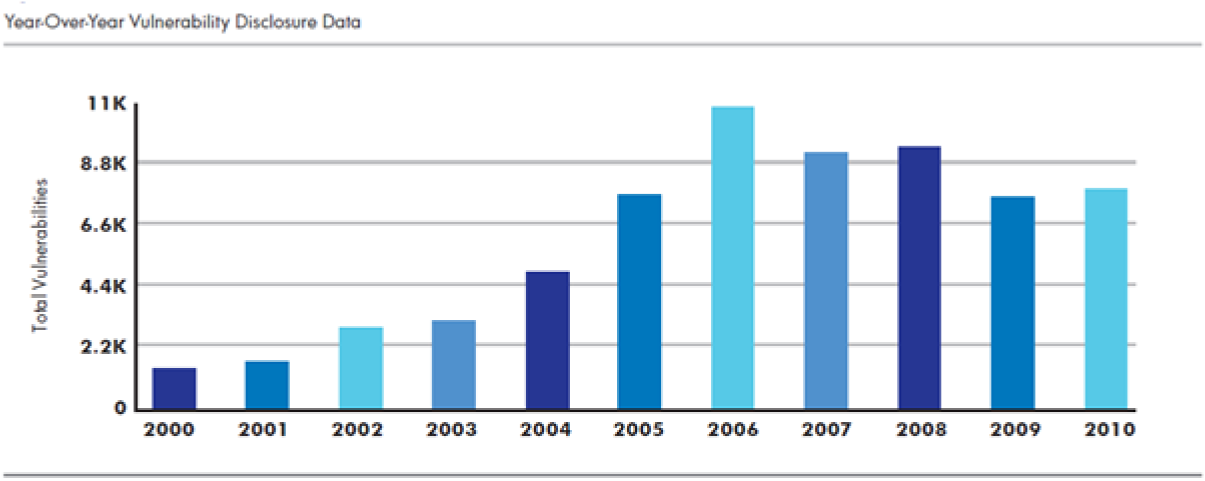


Fig 24 - Web application vulnerability from 2000 – 2010 (HP DVLabs)

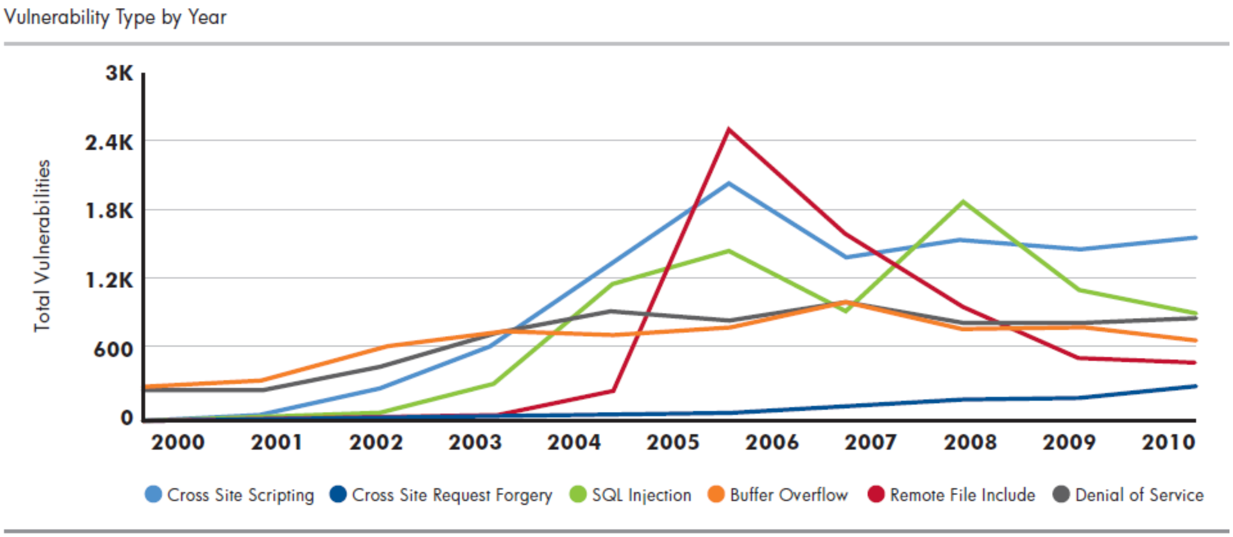


Fig 25 **- Web application vulnerability types from 2000 – 2010**

In the web-based EMR system, patient-related medical and other pertinent information is transmitted over the web, allowing free passage to anyone on the web. Maintaining the confidentiality of medical records that are shared over the Internet and the World Wide Web has become a serious concern (Rind et al., 1997). Secondly and most importantly, HIPAA rules and regulations are strictly enforced on any covered entity that deals with processing of any patient's EMR to administer proper security safeguards (administrative, technical and physical) that ensure protection of patients' medical records from unauthorized users.

3.5 Web Application Vulnerability

Web applications vulnerabilities are the security risk or threats to the web application due to weak coding standards in the application. The below are the some of the most common web application vulnerabilities.

3.5.1 SQL Injections

SQL Injection is one of the common types of database attack that allows a malicious individual to execute arbitrary SQL code on your server. SQL injections are the MYSQL statements that can be placed in the user input by malicious users to corrupt the entire database. The SQL injection mainly occurs when a user is asked to enter input in the form. For instance, when a user enters some input data in the form, instead of the input data, the SQL query is constructed literally from the input data by the malicious users, and this SQL statement is executed on the database. The SQL injections can result in addition of new data to the database, modification of previous data, and access to system capability by retrieving the username and password (PHP Security Consortium, 2005).

Example of SQL Injections:

Suppose a web application has a simple HTML page that contains a textbox called customer ID and a submit button for customers to enter their customer ID to retrieve all of their current order information. On submitting the form, the following SQL query is executed:

```
SELECT *
FROM Orders
```

```
WHERE CustomerID = Customer_ID
```

During a normal customer inquiry, this form works quite well. Suppose person X visits the page and enters his customer ID (140000). The following query would retrieve his results:

```
SELECT *
FROM Orders
WHERE CustomerID = 14000
```

However, the same code can be a hazardous weapon in the hands of a malicious user. Now, imagine that person Y comes along and enters the following data in the CustomerID field: “14; DROP TABLE Orders”. This would cause the following query to execute:

```
SELECT *
FROM Orders
WHERE CustomerNumber = 14; DROP TABLE Orders
```

The “DROP TABLE Orders” query will delete the table name called “Orders” from the database, which will result in loss of all the data from the table “Orders.”

3.5.2 SQL Injections Results

The three most common results from SQL injections are described below (PHP Security Consortium, 2005).

New data can be added to database

With the use of SQL injection, malicious users can perform an INSERT operation for adding new unauthentic data to the existing database that may result in inconsistency of the real data.

Existing data can be modified

The existing data can be updated by the use of SQL injections that can be very costly to any organization. For instance, the price of a product can be lowered in the database with the use of the UPDATE command via form.

Gain access to other user’s system capability

Last but not least, the hacker can also gain access to other system capabilities with the use of SQL injections, and can delete entire tables in the database by executing the DELETE SQL statement.

3.5.3 Cross Site Scripting Vulnerability (XSS)

Cross-site scripting (XSS) is very common web-based security vulnerability that happens when malicious data are gathered by the end user. This kind of vulnerability has accounted for 80% of all security risks to web applications (Symantec Internet Security Threat Report, 2007). Most of the time, this type of security vulnerability occurs when user data are collected by the web application in the form of a hyperlink that is compromised by the malicious code in it (Huseby, 2005). In order to collect user data, the malicious user employs client side script (JavaScript, VBScript, ActiveX, and HTML) to inject virus code into the high risk web application. By injecting the malicious code into the web pages, an attacker can gain access to the user’s session cookies, and a variety of other sensitive information that resides on the user browser. Some of the web applications that are most affected by the XSS are social networking sites, such as Facebook, Twitter, MySpace etc. The XSS scripting vulnerability has been classified into two categories:

a) Persistent: This type of vulnerability occurs when the server permanently displays the saved data from malicious users to the other users without properly escaping HTML. This kind of attack has more impact, as the malicious code is executed automatically without the need of the end user to execute it.

b) Non-Persistent: The non-persistent type of vulnerability is the most common type of attack that occurs when the server side script outputs the result page from user input without validating and escaping the malicious sql query in the user inputs (sanitizing the user request) (Web Application Security Consortium, 2008).

3.5.4 Cross Site Request Forgery (CSRF)

This type of security vulnerability results from the actions of web attackers that compel end users to execute malicious script or load a page that contain a malicious request when the person is currently logged into the system or web application. This type of security vulnerability can lead to stealing of the end user’s sensitive data, such as account information, updating of account information, and/or gain access to the entire system. Cross site request forgery works in just the opposite manner to cross site scripting (XSS). In XSS, user trust is exploited by the web application, whereas in the CSRF web application, trust is exploited by the user’s browser (PHP Security Consortium, 2005). The below example illustrates how CSRF can be unsafe to end users:

Let say **User A** is browsing a forum where another **User B** has posted a malicious HTML image element that references **User A’s** bank website. Now, if **User B** attempts to load that image, it will process the withdrawal request, if the withdrawal authenticated information is stored in a cookie and that cookie is still active in **User B’s** browser.

To protect the web application from the cross-site request forgeries, the use of the “POST” method is the best practice to use whenever the end user is required to submit the data in the database via web forms instead of “GET” method in the web forms (PHP Security Consortium, 2005).

3.5.5 Global Registers

In web applications, global registers possess another kind of security risk that every developer must disable while developing the web application. By default, the global register is disabled in the php.ini file of PHP versions 4.2.0 and greater (PHP Security Consortium, 2005). The code below illustrates the example of how an enabled global register can be harmful to the web application.

```
<? php
if (User_authenticated ( ))
{
$authorized = true;
}
if ($authorized)
{
Include '/ classified/Data.php';
}
```

```
?>
```

Now, if the _global register is enabled, the malicious user can request this page with "?authorized=1" in the query string to bypass the access control, and by disabling the global registers, the global variables will not be effected by the user submitting the data.

3.6 Database Security and Concerns

Database security is the mechanism of protecting and securing a database from its use, access, disclosure, or destruction by unauthorized intruders. Database security is becoming more critical, as anyone can access databases via networks. The failure to protect and secure the database can cause a serious threat to organizations or individuals. Usually, databases are protected from external network connections by use of system firewalls or routers on the network perimeter existing on the internal network. The database provides many layers of security that includes access control, auditing, authentication, encryption, and integrity control to protect the data, and information from the unauthorized user. Access control allows the authority to control access to areas and resources in a given physical facility. Access control includes authentication, authorization, and audit, which determines who is allowed to enter or exit, as well as where, and when. Access control systems are categorized into three most widely recognized models (Olzak, 2006).

- **Discretionary Access Control (DAC):** In DAC, the owner of the system decides who is allowed to access the object and what privileges to assign. DAC allows users to control access to their resources.

- **Mandatory Access Control (MAC):** In MAC, the system decides who is allowed to access the object and what privileges to assign. MAC is used in multilevel systems that process highly sensitive data, such as classified government and military information.
- **Role Based Access Control (RBAC):** In RBAC, the system decides who is allowed to access the object and what privileges to assign. RBAC is used in commercial applications and military systems, where multi-level security requirements may also exist.

Database security also allows the facility to encrypt the data and information stored in the database. The encryption is a mechanism of transforming data and information into unreadable form with the use of an algorithm called a cipher. These data and information can only be accessed into readable form with the decryption key. This is the most effective way of protecting and securing the database from the unauthorized user, as the data becomes useless without the decryption key. Finally, integrity control is the way to ensure the data consistency. Data consistency means that only valid data are stored in the database. The integrity control can be achieved by the use of the primary key (every table must have a primary key and columns chosen to be the primary key should be unique and not null), foreign key (foreign key refers to a primary key of some table in the database) (Ramakrishnan and Gehrke, 2009).

To further strengthen database security, different network intrusion detection systems can be used that can detect and alert the database administrator to malicious database protocol traffic.

3.7 Security Programs

Security programs are the security measures that any organization that deals with the processing and storage of vital information must implement. Healthcare organizations, such as hospitals, nursing homes, and private practices, must have effective security measures in place, as they deal with senstive patient information in day-to-day activities. Security measures includes access control management, audits trail programs, polices and procedures, guidelines and standards. In addititon to this, an effective security program includes risk assessment activities for testing controls' effectiveness (Olzak, 2006).

3.7.1 Access Controls

Access controls are a systematic way of managing the electronic IT systems and other infrastructure within the organization, so that the right users have the privileges to access the data and information that is necessary to conduct the job function, and restricting the action of unauthorized personnel from access to the information (Christiansen, 2000). Access control is classified into three groups, technical access control, physical access control, and administrative access control (Olzak, 2006). Technical access control deals with controlling access to information among the authorized users within the organization. For the healthcare organization, it is very important to have different levels of access to restrict the different levels of user within the organization for accessing the patient information. Creating and managing different levels of access will minimize the exposure to a patient's information among different users, and will help in protecting patient information from being misused or mishandled by users. User rights or privileges should be granted based on a set of access rules that are defined by the roles of individual users in the organization. Implementation of physical access control is necessary to bar the intrusion of unauthorized personnel into the sensitive area of the organization and to minimize the risk of physical damage by man-made or natural disasters. Physical access control includes: backups, fences, man trap schema, security guard, alternative power sources, proper and effective use of fire detection, and fire suppression systems. Administrative access control is required to prevent the threat from the users that are involved with processing the electronic information. Administrative controls consist of the policies, procedures, standards, and baselines that make up an organization’s security program (Olzak, 2006).

The administrative access control includes: separation of duties, business continuity and data recovery planning, proper hiring process, and proper termination process of the user. Separation of duties means dividing the task among several personnel rather than allocating the entire task to any single person. Separating of duties into discrete tasks and allocating duties among different personnel will alleviate the likelihood of information being misused by the user, either intentionally or unintentionally. Business continuity planning is another very important administrative control, which needs to be a continuous process rather than a onetime die, as it helps to protect the availability of the information whenever required and to serve as a future reference. This process includes the detail report of various incidents that occurred over time, action taken to prevent the security incidents, and their outcomes. Hiring of the proper employees is very important for the organization, since most security incidents result from the actions of employees. Whenever any new employee is to be hired, it’s very important to have the proper background and reference checks to ensure that the employee doesn’t carry any harmful effect that can be potentially dangerous for the organization. Proper termination process is equally important, since the employee will have access to various information resources when he/she is working within the organization. Whenever an employee leaves the organization, it’s very important for the person who is responsible for processing his/her termination to follow well-documented policy, guidelines, and procedures to ensure the proper exclusion from technical and physical access/devices to all business assets. Assessing the technical risks at various stages and applying risk management approaches (policies, procedures, guidelines) will always be necessary to recognize the key aspects (Coleman, 2004).

3.7.2 Audit Trails

Security reviews and audit trails form important components of the security program, as they help the organization in evaluating and analyzing its current IT systems (hardware and software), infrastructure, and compliance procedure on a regular basis. Audit trails are a very effective method, as they help the organization to improve and enhance its current system by assessing the overall organization performance and, hence, ensuring integrity, confidentiality, and availability of the information. The assessments from the audits trails must include four areas of compliance:

a) Program policies and processes,

b) System policies and processes,

c) Vulnerability tests, and

d) Penetration tests.

3.7.3 Standards, Guidelines, Policies and Procedures

Implementation of proper standards, guidelines, policies, and procedures are very important for healthcare organizations to protect their information assets flowing in and out of the organization. The deployment and use of right policies and procedures helps in controlling and managing the IT infrastructure and employees, and the use of standards and guidelines helps in controlling facility areas where sensitive information resides. The standards, guidelines, policies, and procedures define a framework for developing three types of security controls (prevent, detect, and recover). “Prevent” security control means preventing IT systems and infrastructure vulnerabilities before the intruder penetrates the system. “Detect” security control means identifying the IT systems and infrastructure breaches whenever protocols are compromised by the intruder. Finally “recovery” security control means recuperating the IT systems and infrastructure when the damage has been done by the intruder.

CHAPTER 4

EMR CHALLENGES

The success of this web-based EMR application is accomplished by overcoming various challenges involved with the development process. Some of the key challenges in the development of the web-based TigerPlace EMR systems are outlined below:

1. Understanding how each module should work, and developing the functionality of that module per healthcare team recommendations, was the first challenge involved in this project.
2. After developing and implementing the Web-based EMR System in TigerPlace, the main challenge was to incorporate enough security measures to protect the web application from being misused by malicious or unauthorized users, and to make it compliant with HIPAA rules and regulations.
3. Another challenge involved ensuring data and information recorded by the clinical staff were saved appropriately in the database tables to avoid any data inconsistencies in the web form that may lead to incorrect assessment of the residents.
4. Regularly maintaining the backup copies of TigerPlace database and files that could be used in case of emergency or disaster.
5. Last but not least, integrating the web-based EMR application with other clinical IT systems at TigerPlace remains an ongoing challenge, but it will be less challenging because a foundation has already been laid.

CHAPTER 5

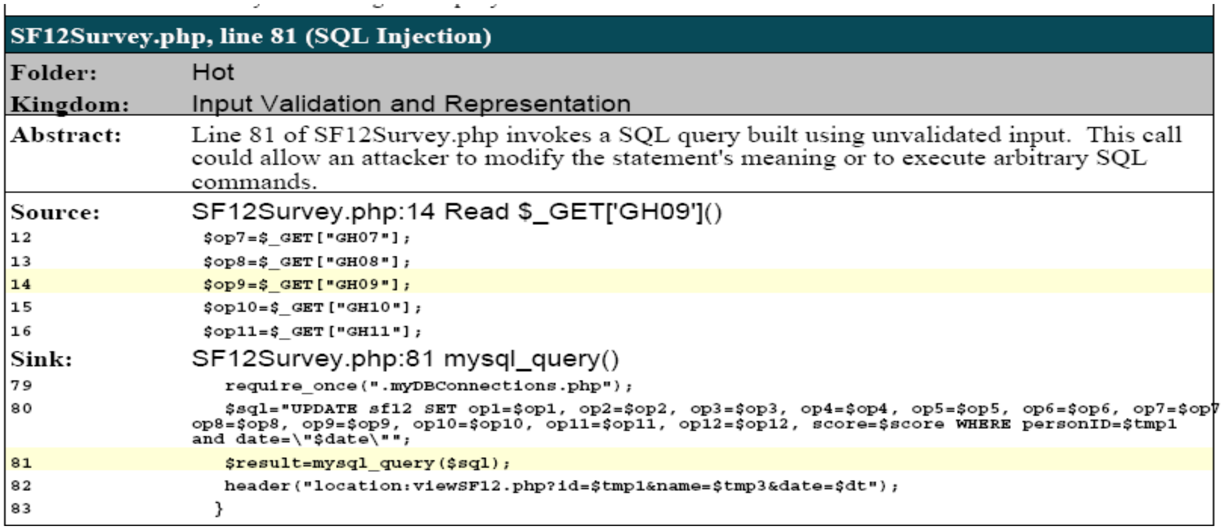
METHODOLOGY

To overcome the previously mentioned challenges, security measures for EMR application at TigerPlace included the following protections.

5.1 Web Application Methodology

5.1.1 Fortify Scan

The Fortify Scan is the security software which identifies and reports the bugs and security vulnerabilities, along with a list of problems in the source code. It generates the report of SQL injections and weak queries from the source code and assists the security analyst by providing remedies in improving the weak SQL queries. This tool also assists security analysts in providing relative assessment of the potential severity of each problem. Figure 26 illustrates how Fortify Scan software helped to indentify and fix the security risks and vulnerabilities associated with the SQL injections and cross site scripting vulnerabilities in the TigerPlace web EMR system.



SF12Survey.php, line 81 (SQL Injection)

Folder:	Hot
Kingdom:	Input Validation and Representation
Abstract:	Line 81 of SF12Survey.php invokes a SQL query built using unvalidated input. This call could allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.

Source: SF12Survey.php:14 Read $_GET['GH09']()

```
12    $op7=$_GET["GH07"];
13    $op8=$_GET["GH08"];
14    $op9=$_GET["GH09"];
15    $op10=$_GET["GH10"];
16    $op11=$_GET["GH11"];
```

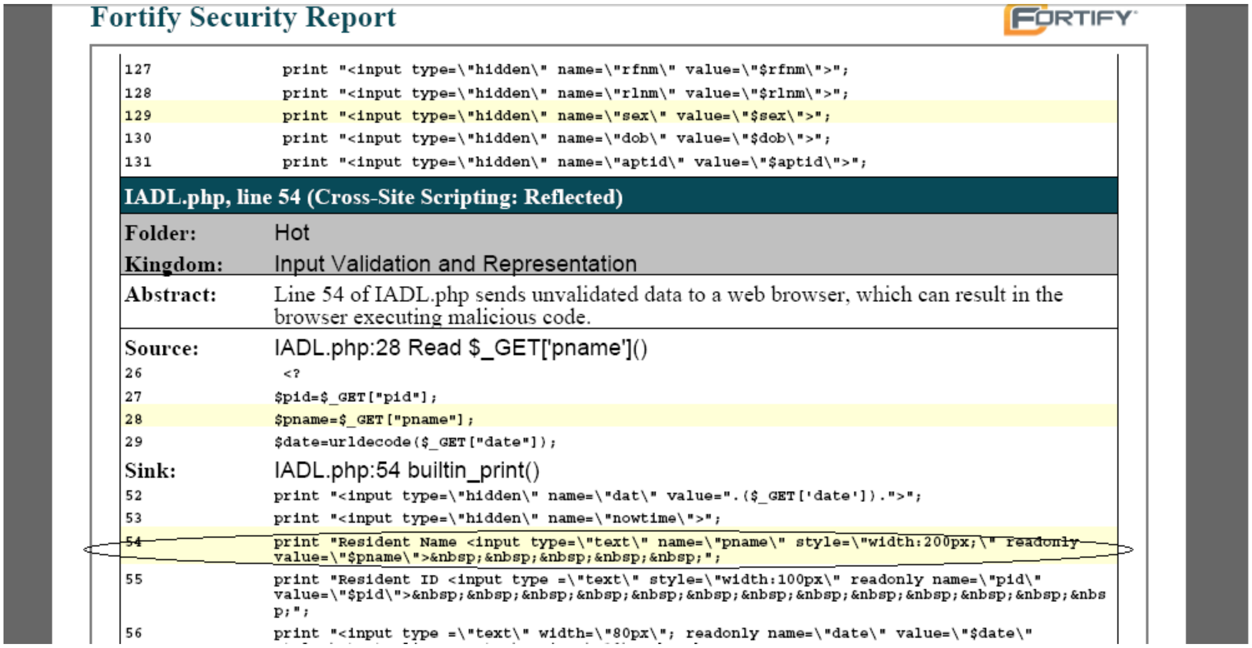
Sink: SF12Survey.php:81 mysql_query()

```
79      require_once(".myDBConnections.php");
80      $sql="UPDATE sf12 SET op1=$op1, op2=$op2, op3=$op3, op4=$op4, op5=$op5, op6=$op6, op7=$op7,
op8=$op8, op9=$op9, op10=$op10, op11=$op11, op12=$op12, score=$score WHERE personID=$tmp1
and date=\"$date\"";
81      $result=mysql_query($sql);
82      header("location:viewSF12.php?id=$tmp1&name=$tmp3&date=$dt");
83     }
```

Fig 26 – SQL Injection Identified by Fortify Scan Software

In this PHP file (SF12survey.php), the Fortify Scan software indentified and reported line number 81 ($result=mysql_query($sql);) to be vulnerable to SQL injection.

Figure 27 illustrates how Fortify Scan software helped to identify and fix the security risks and vulnerabilities associated with the Cross Site Scripting in the TigerPlace web EMR system.



Fortify Security Report

```
127        print "<input type=\"hidden\" name=\"rfnm\" value=\"$rfnm\">";
128        print "<input type=\"hidden\" name=\"rlnm\" value=\"$rlnm\">";
129        print "<input type=\"hidden\" name=\"sex\" value=\"$sex\">";
130        print "<input type=\"hidden\" name=\"dob\" value=\"$dob\">";
131        print "<input type=\"hidden\" name=\"aptid\" value=\"$aptid\">";
```

IADL.php, line 54 (Cross-Site Scripting: Reflected)

Folder:	Hot
Kingdom:	Input Validation and Representation
Abstract:	Line 54 of IADL.php sends unvalidated data to a web browser, which can result in the browser executing malicious code.

Source: IADL.php:28 Read $_GET['pname']()

```
26     <?
27    $pid=$_GET["pid"];
28    $pname=$_GET["pname"];
29    $date=urldecode($_GET["date"]);
```

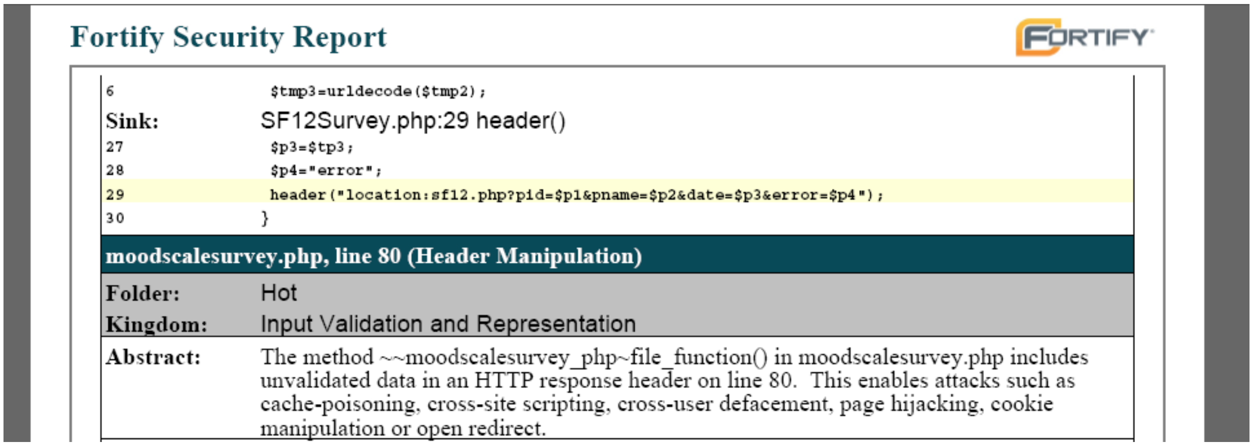
Sink: IADL.php:54 builtin_print()

```
52    print "<input type=\"hidden\" name=\"dat\" value=".($_GET['date']).">";
53    print "<input type=\"hidden\" name=\"nowtime\">";
54    print "Resident Name <input type=\"text\" name=\"pname\" style=\"width:200px;\" readonly
value=\"$pname\">&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;";
55    print "Resident ID <input type =\"text\" style=\"width:100px\" readonly name=\"pid\"
value=\"$pid\">&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbs
p;";
56    print "<input type =\"text\" width=\"80px\"; readonly name=\"date\" value=\"$date\"
```

Fig 27 – Cross Site Scripting Issue identified by Fortify Scan Software

In this PHP files (IADL.php), the Fortify Scan software indentified and reported line number 54 (print "Resident Name <input type=\"text\" name=\"pname\" style=\"width:200px;\" readonly value=\"$pname\">";) to be vulnerable to Cross Site Scripting.

Figures 28 and29 illustrate how Fortify Scan software helped to identify and fix the security risks and vulnerabilities associated with the cache-poisoning, cross-site scripting, cross-user defacement, page hijacking, cookie manipulation, or open redirect in the TigerPlace web EMR system.



Fortify Security Report

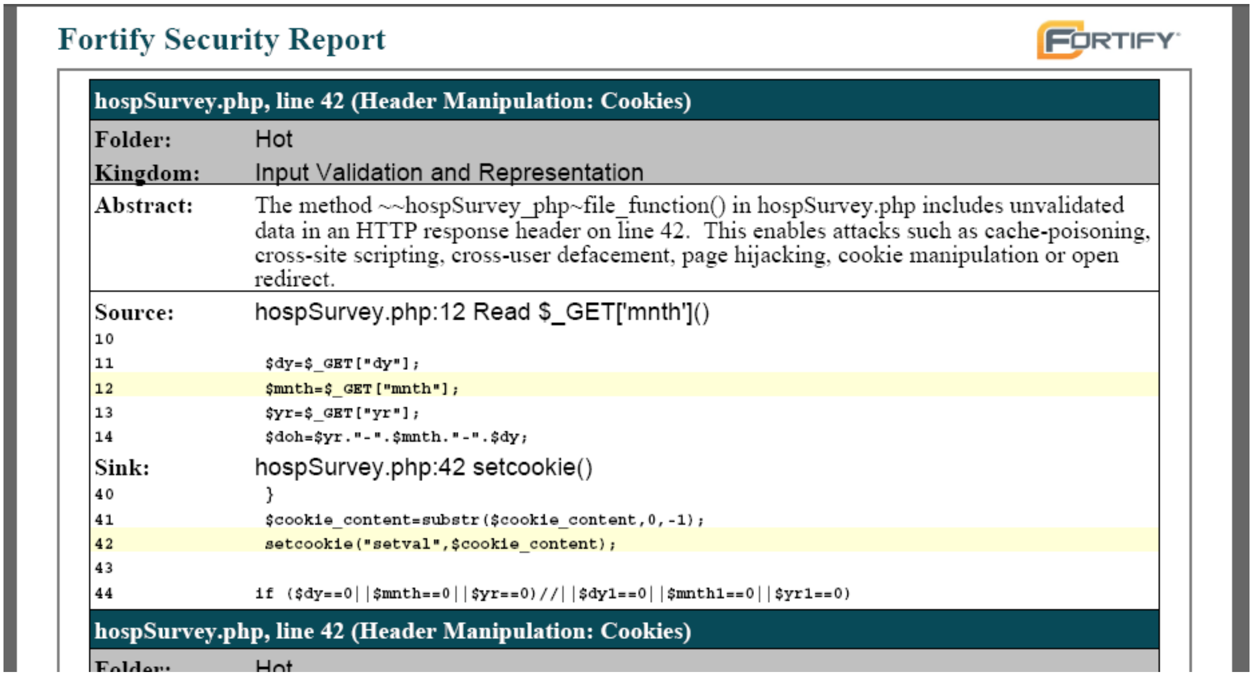
```
6                $tmp3=urldecode($tmp2);
Sink:           SF12Survey.php:29 header()
27               $p3=$tp3;
28               $p4="error";
29               header("location:sf12.php?pid=$p1&pname=$p2&date=$p3&error=$p4");
30              }
```

moodscalesurvey.php, line 80 (Header Manipulation)

Folder: Hot
Kingdom: Input Validation and Representation

Abstract: The method ~~moodscalesurvey_php~file_function() in moodscalesurvey.php includes unvalidated data in an HTTP response header on line 80. This enables attacks such as cache-poisoning, cross-site scripting, cross-user defacement, page hijacking, cookie manipulation or open redirect.

Fig 28 – Header Manipulation issue identified by Fortify Scan Software



Fortify Security Report

hospSurvey.php, line 42 (Header Manipulation: Cookies)

Folder: Hot
Kingdom: Input Validation and Representation

Abstract: The method ~~hospSurvey_php~file_function() in hospSurvey.php includes unvalidated data in an HTTP response header on line 42. This enables attacks such as cache-poisoning, cross-site scripting, cross-user defacement, page hijacking, cookie manipulation or open redirect.

Source: hospSurvey.php:12 Read $_GET['mnth']()

```
10
11           $dy=$_GET["dy"];
12           $mnth=$_GET["mnth"];
13           $yr=$_GET["yr"];
14           $doh=$yr."-".$mnth."-".$dy;
```

Sink: hospSurvey.php:42 setcookie()

```
40           }
41           $cookie_content=substr($cookie_content,0,-1);
42           setcookie("setval",$cookie_content);
43
44          if ($dy==0||$mnth==0||$yr==0)//||$dy1==0||$mnth1==0||$yr1==0)
```

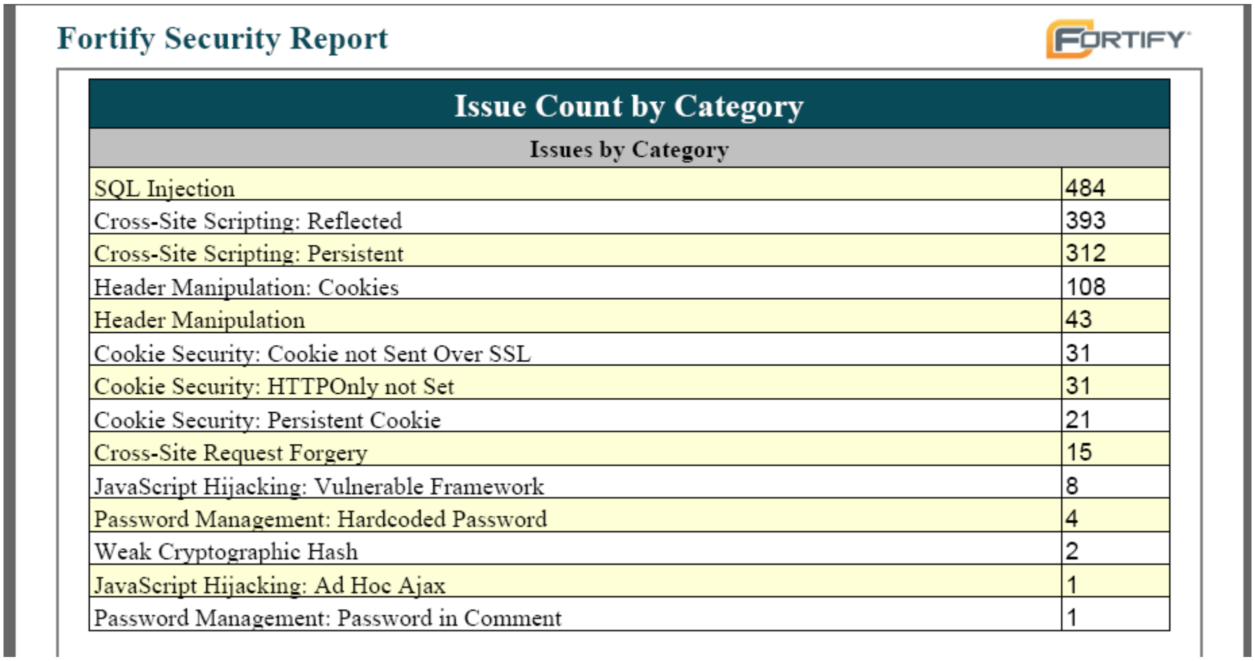
hospSurvey.php, line 42 (Header Manipulation: Cookies)

Folder: Hot

Fig 29 – Header Manipulation Cookies issue identified by Fortify Scan Software

In these PHP files (SF12Survey.php, hospSurvey.php), the Fortify Scan software identified and reported the line number 80 and line number 42, respectively (print "Resident Name <input type=\"text\" name=\"pname\" style=\"width:200px;\" readonly value=\"$pname\">";) to be vulnerable to cache-poisoning, cross-site scripting, cross-user defacement, page hijacking, cookie manipulation, or open redirect.

Figure 30 below lists all the security risks and vulnerabilities that were identified while scanning the TigerPlace EMR system with Fortify Scan software.



Fortify Security Report

Issue Count by Category

Issues by Category	
SQL Injection	484
Cross-Site Scripting: Reflected	393
Cross-Site Scripting: Persistent	312
Header Manipulation: Cookies	108
Header Manipulation	43
Cookie Security: Cookie not Sent Over SSL	31
Cookie Security: HTTPOnly not Set	31
Cookie Security: Persistent Cookie	21
Cross-Site Request Forgery	15
JavaScript Hijacking: Vulnerable Framework	8
Password Management: Hardcoded Password	4
Weak Cryptographic Hash	2
JavaScript Hijacking: Ad Hoc Ajax	1
Password Management: Password in Comment	1

Fig 30 – Displays all security related issues identified by the Fortify Scan Software

5.1.2 Escaping of Input (Data Filtering)

Escaping of user input, also called data filtering, is an effective method for securing and protecting the web application from being destroyed or modified by malicious users with the use of SQL injections. This mechanism tends to resolve most of the web security vulnerabilities without doing much effort. By escaping the special characters, such as semicolon, and single quotes, the risk of SQL injection attacks can be minimized (Andonov, 2007). So, in order to secure and protect the TigerPlace web-based EMR system, mysql_real_escape_string( ), gpc_magic_quotes are the functions that have been used for filtering and escaping the special characters in a string that are used in SQL statements. The below code illustrates how this mysql_real_escape_string() escape detects the user input special characters that can be hazardous to the database.

```
// Query to database by malicious user

 < ?

      $malicious_user = "SELECT * FROM person WHERE username = 'OR 1’";

       echo $malicious_user;

? >
```

Problem #1: By using a single quote (‘) to the username, the malicious user has ended the string part of the MySQL query.

Problem #2: The WHERE statement is added with an OR clause of 1 which mean always true.

Result: The “OR clause of 1” will select every single row in the "person" table, and, hence, it will display all the data in the person table to the malicious user, which he/she is not authorized to view.

Solution: Use of mysql_real_escape_string( ) function that will filter and escape the special characters (such as single quote) with the safe substitute backslash (\’) in a string.

```
\\ Use of mysql_real_escape_string( ) function
< ?
      $malicious_user = "SELECT * FROM person WHERE username = 'OR 1’";

      $malicious_user = mysql_real_escape_string($malicious_user);

     echo $malicious_user;

?>
```

Result: Escaped bad SQL queries**:**

```
SELECT * FROM Person WHERE username = \' OR 1\'
```

5.1.3 Use of MD5 Methodology for Encrypting Passwords

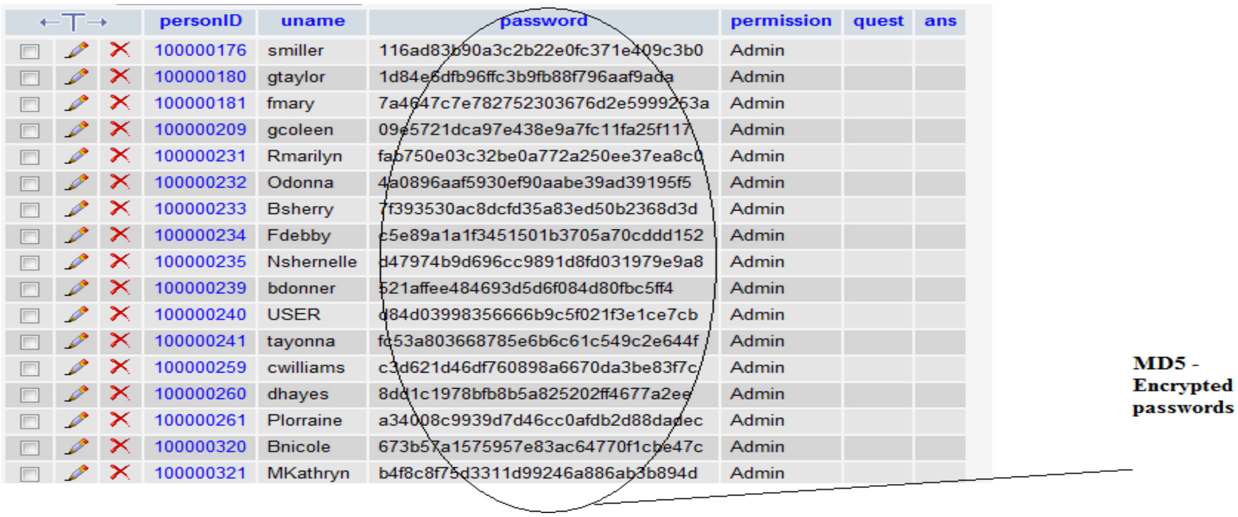
The database security has been enhanced by the use of the MD5 hash generator. The MD5 hash generator is a program/algorithm based on a complex mathematical function that takes input (string) and converts (encrypts) the string into a large random alphanumeric character. The alpha-numeric string generated by the MD5 hash generator is hard or impossible to decrypt by the intruder, and, thus, this improves the security of passwords in the database. So, I have used the MD5 hash generator to decrypt the passwords of all of the users rather than using plain-text passwords, which are vulnerable if the plain-text passwords are compromised by the intruder/malicious users. The encrypted passwords have no value to the intruder, as this will never allow them to access the system without properly decrypting them, and decrypting the MD5 generated password may be beyond the scope of any hacker at this stage.

Example: `MD5 ("SauravG") = "6282ede2cd977a65ab206840fb1bce6d"`

`MD5("6282ede2cd977a65ab206840fb1bce6d")=`

`"a2d23d87256d15ea7488eb6ddab2ee7f"`

The figure 31 below illustrates the encryption of password using MD5 methodology for all the end users who access the TigerPlace EMR web application.



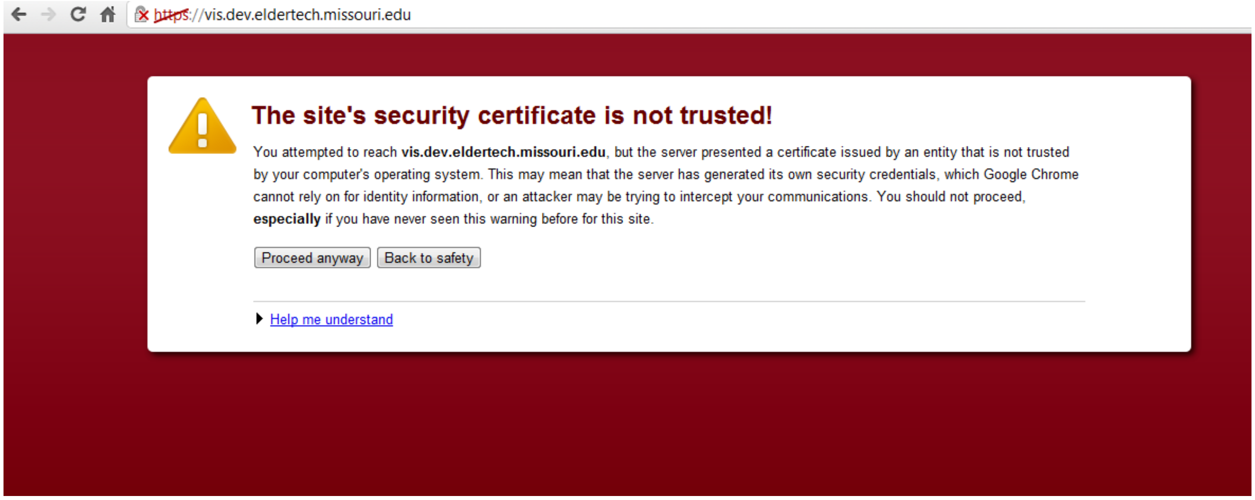
←T→			personID	uname	password	permission	quest	ans
☐	✎	✗	100000176	smiller	116ad83b90a3c2b22e0fc371e409c3b0	Admin		
☐	✎	✗	100000180	gtaylor	1d84e6dfb96ffc3b9fb88f796aaf9ada	Admin		
☐	✎	✗	100000181	fmary	7a4647c7e782752303676d2e5999253a	Admin		
☐	✎	✗	100000209	gcoleen	09e5721dca97e438e9a7fc11fa25f117	Admin		
☐	✎	✗	100000231	Rmarilyn	fab750e03c32be0a772a250ee37ea8c0	Admin		
☐	✎	✗	100000232	Odonna	4a0896aaf5930ef90aabe39ad39195f5	Admin		
☐	✎	✗	100000233	Bsherry	7f393530ac8dcfd35a83ed50b2368d3d	Admin		
☐	✎	✗	100000234	Fdebby	c5e89a1a1f3451501b3705a70cddd152	Admin		
☐	✎	✗	100000235	Nshernelle	d47974b9d696cc9891d8fd031979e9a8	Admin		
☐	✎	✗	100000239	bdonner	521affee484693d5d6f084d80fbc5ff4	Admin		
☐	✎	✗	100000240	USER	d84d03998356666b9c5f021f3e1ce7cb	Admin		
☐	✎	✗	100000241	tayonna	fc53a803668785e6b6c61c549c2e644f	Admin		
☐	✎	✗	100000259	cwilliams	c3d621d46df760898a6670da3be83f7c	Admin		
☐	✎	✗	100000260	dhayes	8dd1c1978bfb8b5a825202ff4677a2ee	Admin		
☐	✎	✗	100000261	Plorraine	a34008c9939d7d46cc0afdb2d88dadec	Admin		
☐	✎	✗	100000320	Bnicole	673b57a1575957e83ac64770f1cbe47c	Admin		
☐	✎	✗	100000321	MKathryn	b4f8c8f75d3311d99246a886ab3b894d	Admin		

MD5 -
Encrypted
passwords

Fig 31 – Demonstrate use of MD5 method for encrypting passwords

5.1.4 Use of HTTPS URL Instead of HTTP URL

Whenever any sensitive information needs to be sent over URL, the first line of defense would be to pass it using Secure HTTP. The Web page security has been enhanced by the use of **Hypertext Transfer Protocol Secure (**HTTPS) instead of **Hypertext Transfer Protocol (**HTTP). HTTPS creates a secure channel over an insecure network by incorporating the Secured socket layer (SSL) to move data. The SSL takes the data, going or coming, and encrypts it. This means that SSL uses a mathematical algorithm to hide the true meaning of the data; the hope is that this algorithm is so complex it is either impossible or prohibitively difficult to crack. With the use of HTTPS, we can block the web attackers from gaining access to the website accounts and sensitive information that is processed over the network. Figure 32 below illustrates how the HTTPS works.



The site's security certificate is not trusted!

You attempted to reach **vis.dev.eldertech.missouri.edu**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

Fig 32 – USE of HTTPS URL

5.1.5 Form Validation

Form validation is the process of validating the end user input data in the web form with the JavaScript functions. Whenever any user submits the data in the form, the JavaScript validation function is invoked to check the user input data; if there is any error in the submitted data, the warning message is send back to the end user machine. The form validation has been very beneficial in various aspects of web application for improving and enhancing the integrity of the web application (Auger, 2007). The form validation methodologies not only safeguard the integrity of data, but also help in improving the security risk to the database. The implementation of parameter checking (such as numeric data in numeric field, proper length, etc.) on various fields in the form minimizes the risk of SQL injections. Using form validation methodology for data integrity and security ensures compliance with HIPAA rule and regulations. The following diagram explains how the JavaScript validation function validates the end user input response.

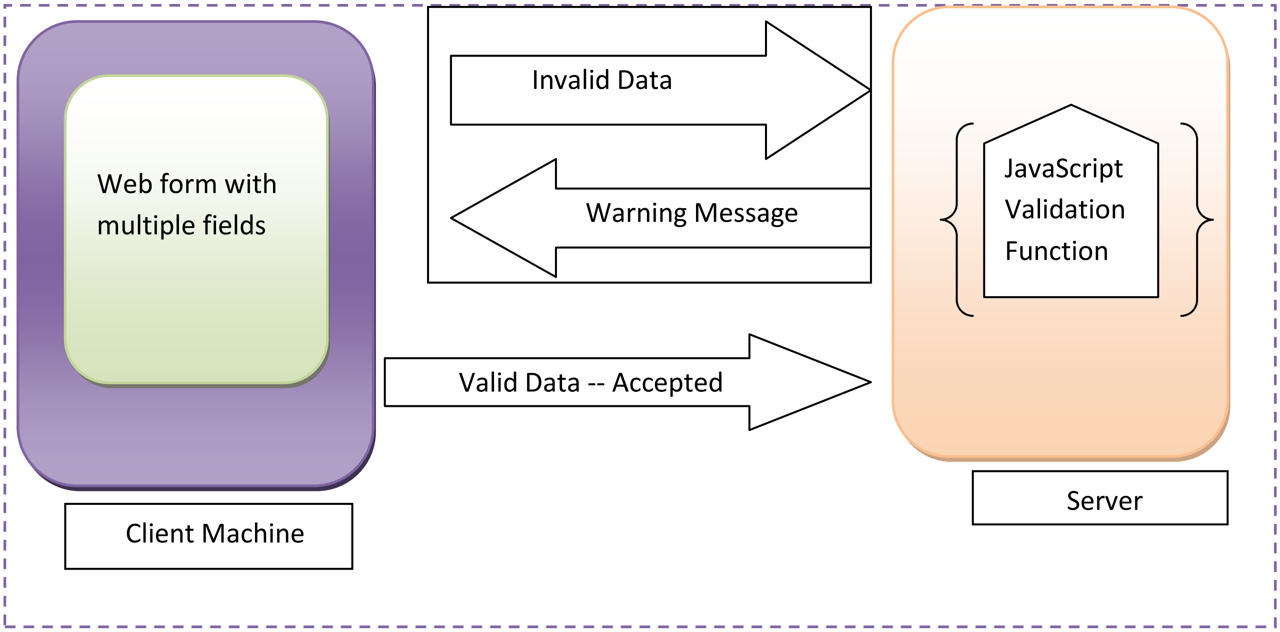
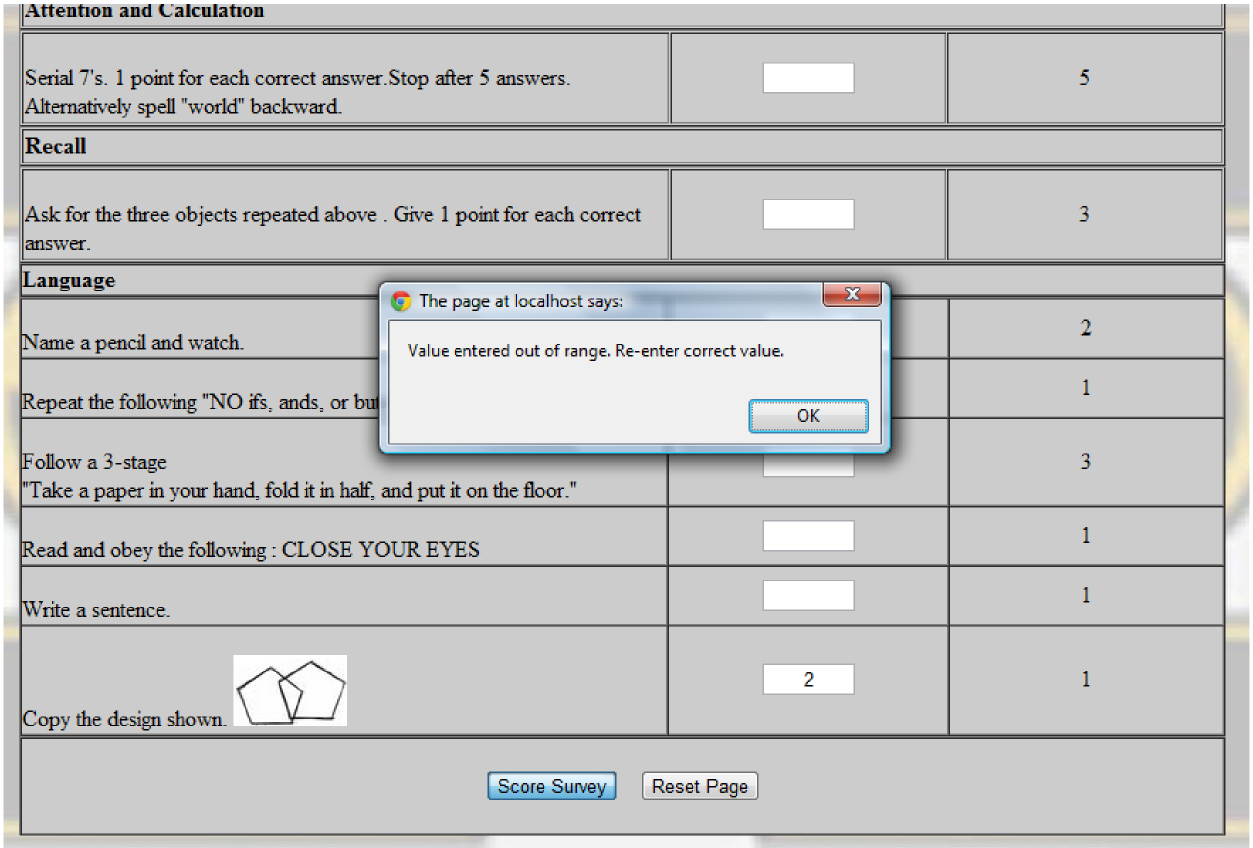


Fig 33 – Form Validation Process

Some of the form validation methodologies implemented in the TigerPlace EMR system to improve the integrity and security of the web application are illustrated below:

a) **Avoiding incorrect, out of range values, and empty field:** Figure 34 below illustrates how form validation methodology assist the end users to avoid incorrect or out of range values in the text field, and helps to enter appropriate data or information in the respective fields. Whenever a user accidently enters a value that is out of range or is invalid data, the popup window will appear with the suggestion that will guide the end user to enter correct data in the respective fields. In the figure below, the popup window with the suggestion was displayed ("Value entered out of range. Re-enter correct value") when the user accidently entered the value "2" in the last field and the maximum value he/she is allowed to enter ranges from 0-1.



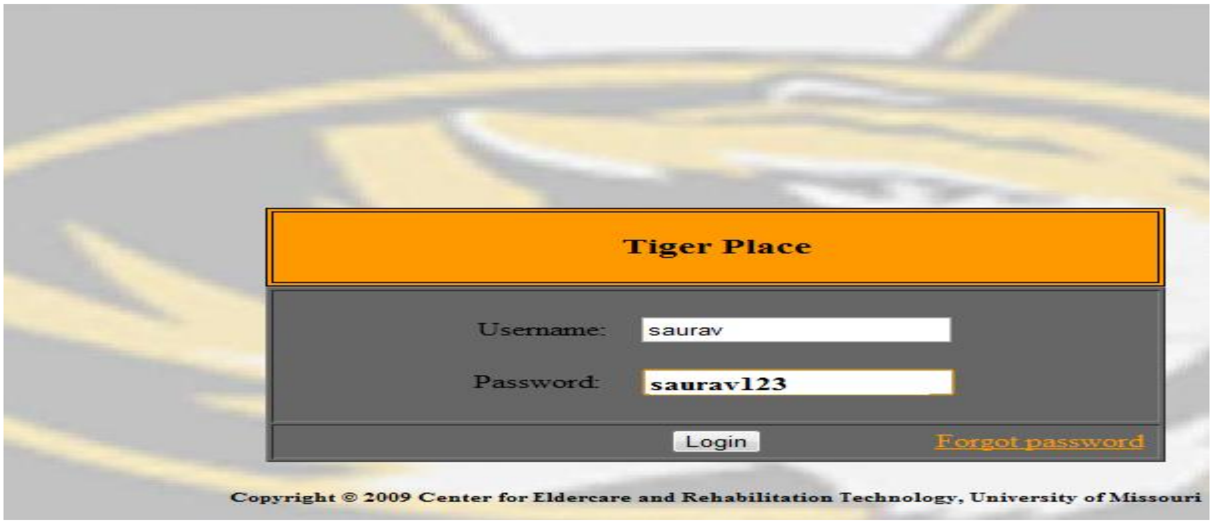
Attention and Calculation		
Serial 7's. 1 point for each correct answer.Stop after 5 answers. Alternatively spell "world" backward.		5
Recall		
Ask for the three objects repeated above . Give 1 point for each correct answer.		3
Language		
Name a pencil and watch.		2
Repeat the following "NO ifs, ands, or bu		1
Follow a 3-stage "Take a paper in your hand, fold it in half, and put it on the floor."		3
Read and obey the following : CLOSE YOUR EYES		1
Write a sentence.		1
Copy the design shown.	2	1

The page at localhost says:

Value entered out of range. Re-enter correct value.

Fig 34 – User Data Validation

b) Validating Password field: To improve the security of the web application, it is very important to validate the password field which will allow end users to use robust passwords instead of simple guessable passwords. With the use of the JavaScript validation function, we can restrict the length of the password (8-10) and can enforce the end user to use the combination of alphanumeric (For instance “abc123rs”) and special characters (For instance “!@$”). In the TigerPlace EMR application, the combination of alphanumeric characters has been enforced in the password field, which makes the web hacker’s decrypting job tougher. Figure 35 below shows the use of alphanumeric characters used for password field.



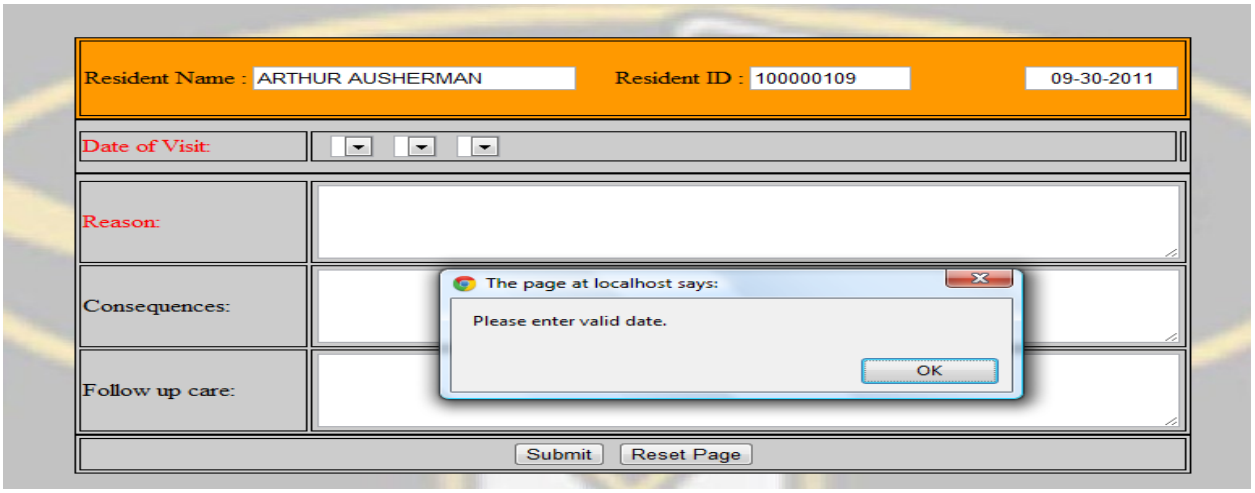
Username: saurav

Password: saurav123

Copyright © 2009 Center for Eldercare and Rehabilitation Technology, University of Missouri

Fig 35 - Use of alphanumeric characters in "Password" field

c) **Validating Date/time field:** It is very important to validate the "Date /time" fields in the electronic medical application system. If the date/time field is missing or incorrect date is entered, it may result in fatal medical error leading to disastrous results (Incorrect medication dose, etc.). Importance of validating the date/time field in the TigerPlace EMR web application arises from the need to determine the date and time when the resident was admitted to emergency room (ER)/Hospital and discharged from ER/Hospital. Figure-36 below illustrates the pop-up window with the warning message, when the user tries to submit the form without entering the "Date" field.



Resident Name : ARTHUR AUSHERMAN Resident ID : 100000109 09-30-2011

Date of Visit:

Reason:

Consequences:

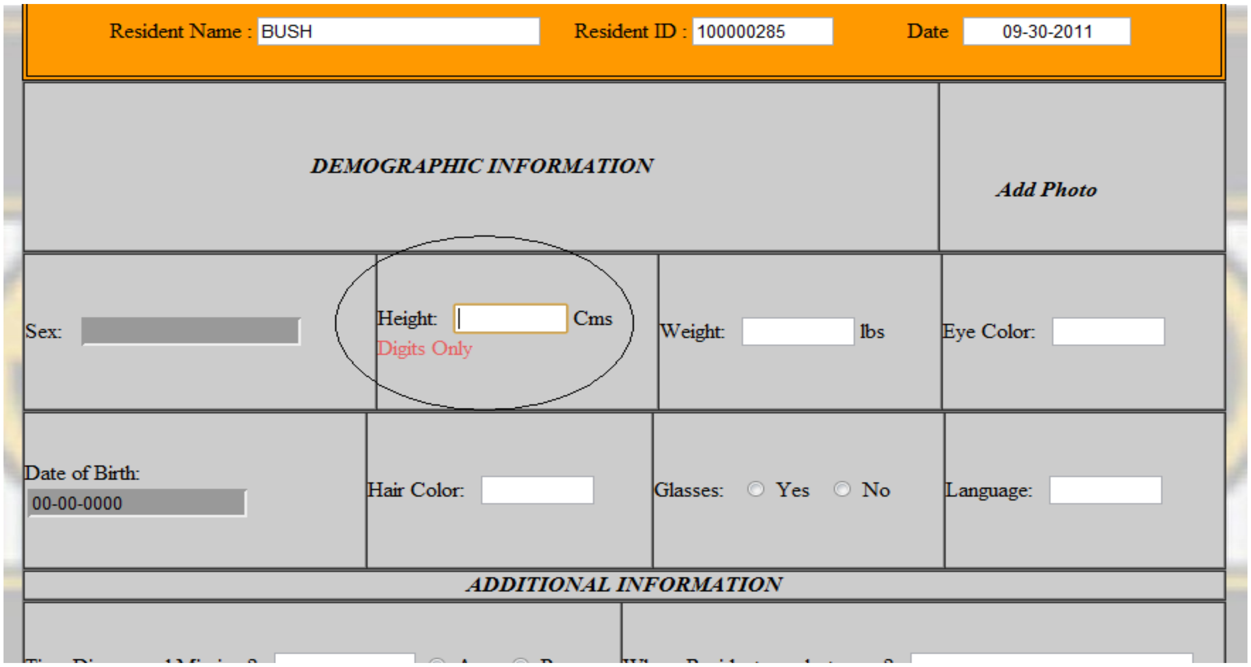
Follow up care:

The page at localhost says:

Please enter valid date.

Fig 36 - Validating Date/Time field

d) **Avoiding wrong data entry (Data Integrity)**: Figure 37 below illustrates how form validation methodology assists end users to avoid wrong data entry in the text field, and aids in entry of appropriate data or information in the respective fields. Whenever the user tries to enter some alphabet in the “Height” field, or she he will be prompted with a warning message to enter a numeric value only (displayed in red below the “Height” field). Avoiding wrong data entry in the web form improves the integrity of the web application.



Resident Name : BUSH Resident ID : 100000285 Date 09-30-2011

DEMOGRAPHIC INFORMATION

Add Photo

Sex:

Height: Cms
Digits Only

Weight: lbs

Eye Color:

Date of Birth:
00-00-0000

Hair Color:

Glasses: ○ Yes ○ No

Language:

ADDITIONAL INFORMATION

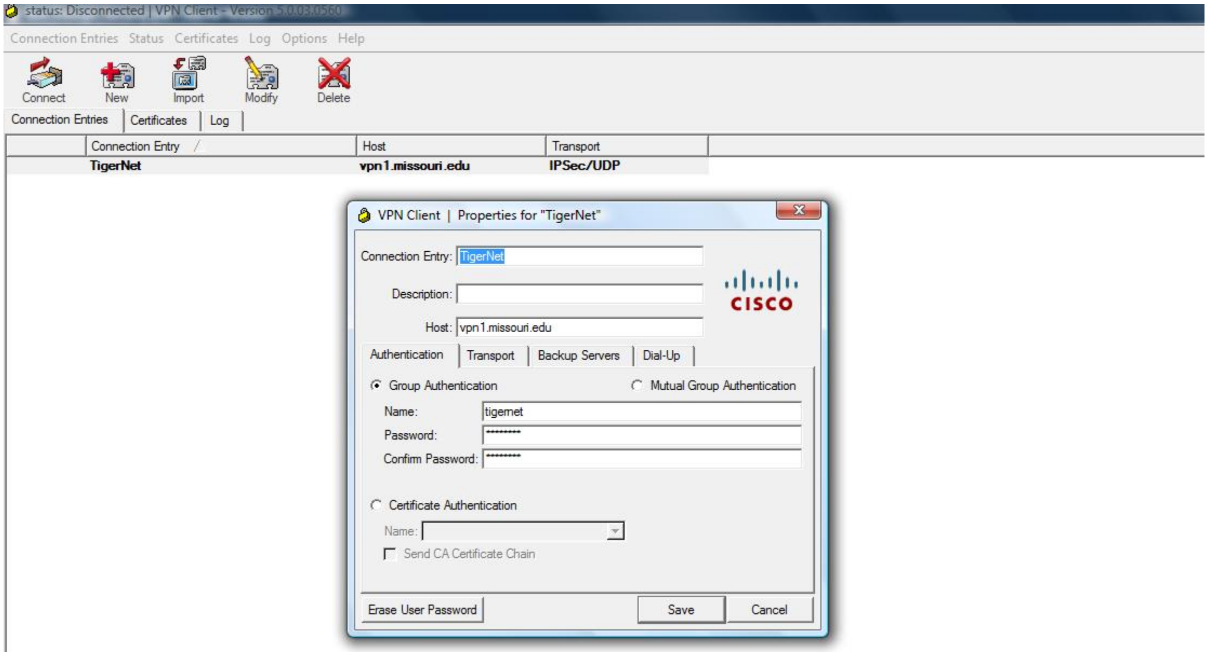
Fig 37 – Data integrity using Form Validation process

5.1.6 Use of POST method instead of GET

Another security method used to protect the web-based EMR application against Cross-Site Request Forgeries was the use of “POST” method instead of “GET” method in the web forms. POST method is a powerful method for eliminating the security vulnerabilities in web applications whenever the user submits the data in the database via web forms. Whenever form data are submitted using the POST method, the data are encoded, which mean the data are not exposed over the URL when the request is submitted. So, the sensitive data and information (such as password, credit card detail etc.) sent in the form via the POST method will not be visible later on the URL bar. However, using the GET method, it will be visible in the browser history and the URL bar, which makes it unsafe.

5.1.7 Firewalls

A firewall is the way of protecting the internal network from being accessed and attacked by malwares and other web security threats. It acts as a barrier and restricts the external networks from getting access to the vital information that resides on the mainframe server. The firewall can be a program that can reside in the system, or can be a device that can be attached to the system to detect and prevent the unauthorized connections to the internal network. In order to protect the TigerPlace web server from being accessed by malicious users, the Virtual Private Network (VPN) technology has been in place, acting as a secure connection between two systems over the Internet. Figure 38 below illustrates the VPN tunnel connection that is required to access the web server of the TigerPlace EMR system.



Connection Entry	Host	Transport
TigerNet	vpn1.missouri.edu	IPSec/UDP

Connection Entry: TigerNet

Description:

Host: vpn1.missouri.edu

● Group Authentication ○ Mutual Group Authentication

Name: tigemet

Password: *********

Confirm Password: *********

○ Certificate Authentication

Name:

□ Send CA Certificate Chain

Fig 38 – VPN Firewall

However, with the emergence of new technology, VPN can be combined with the SSL, which uses certificates and public and private key encryption technology to further strengthen the network firewall against malwares and other threat agents, since SSL VPN ensures setup of personal firewalls and antivirus applications before allowing a device access to the internal network.

5.1.8 Backups

Backups are a very important security measure that organizations must perform each day to ensure proper, complete, and accurate backup of critical data and information. As we know, healthcare organizations are constantly involved in processing patient data and information. Maintaining the proper backups at regular interval is very important for the safety of the healthcare consumers. The main purpose of regular backups lies with the need to recover the IT systems or data centers in case of failure caused by human or natural disasters. In the case of the TigerPlace EMR system, regular backup is done every night, which will certainly help TigerPlace to recover the IT system in-case of emergency.

5.1.9 Authentication Mechanism

The TigerPlace EMR system is protected with two layers of authentication that are required to access the TigerPlace EMR system. The first layer of authentication requires users to have MU login credentials, created by the Lightweight Directory Access protocol (LDAP) and the second layer of authentication requires users to have web application login credentials. So, to access the TigerPlace EMR system, users must have MU login credentials at first level that ensures the user is authenticated to access the MU system, and then web application login credentials created for particular active users by the administrator of the web application. In addition to this, different level of access is also defined in the database table that restricts the access to the comprehensive EMR based on the role or level of users.

The diagram below explains the featured security layers used for nursing EMR system in order to comply with HIPAA rule and regulations.

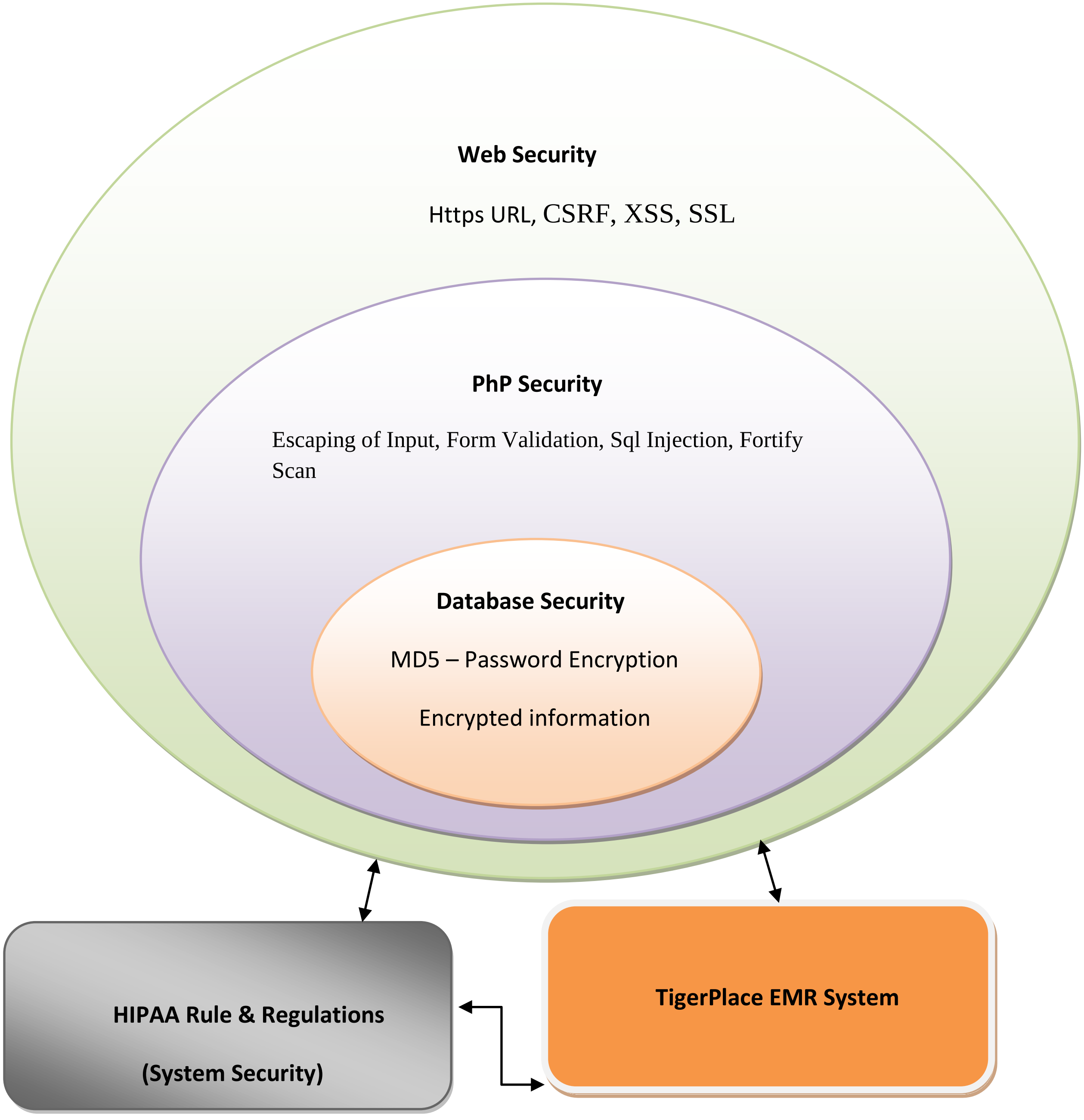


Fig 39 - Model Representing Featured Security Layers for Nursing EMR System

CHAPTER 6

RESULTS

The development of the web-based EMR system was started in August 2008; within two year, the CareFacts™ program was replaced with the web-based EMR system in TigerPlace. To secure the web-based EMR system from misuse by malicious users, various security measures are now successfully implemented within the web application. Implementation of various security measures will not only protect the information system from unauthorized users, but will also ensure compliance of this web-based EMR system with HIPAA rule and regulations. This HIPAA-compliant web-based EMR system ensures integrity, confidentiality, and availability of patient information, and protects the covered entity or organization as a whole from being penalized.

Last but not least, working with the interdisciplinary team of researchers, healthcare team members, and IT engineers for the development of such a comprehensive web-based HIPAA compliant EMR system was a great challenge and a wonderful experience in life.

CHAPTER 7

RECOMMENDATIONS

Although various forms of administrative, technical, and physical security features are in place to protect the EMR and patient-related information from theft, there is still a need for administrative, technical, and physical security safeguards to be followed to ensure confidentiality, integrity, and availability of electronic health records. I have monitored and noticed various security loopholes from administrative, technical, and physical point of view that are summarized below.

7.1 Security awareness and training program to end users

Implementation of a strong user awareness program is a very crucial step for any organization to make users aware of security risks associated with information infrastructure. Health care organizations are recommended to follow the National Institute of Standards and Technology (NIST) model to meet user awareness and human resources obligations to ensure privacy of patient data and information (Craig, 2009). User awareness is an essential requisite for effectiveness of data and information security in the organization. It involves providing regular training sessions to existing employees and newly hired employees about security measures. Employees who deal with processing of sensitive information must be reminded on a daily basis via posters, table tent cards in lunch rooms, voice mail announcements, and login messages, of their roles and responsibilities in the protection of information assets through a strong user awareness program. Security training programs, coupled with organizational reminders, help to overcome human vulnerabilities and risk (Christiansen, 2000). A user awareness program must be a continuous process, as it plays a key role in securing and protecting vital information from theft and misuse by unauthorized persons, and forms the foundation of a secure information processing environment.

a) End users at TigerPlace often forget to close the application when they leave the room to check the patient, allowing free passage to unauthorized users. To avoid any misuse of patient related data, it's very important to provide proper security awareness and training to the end user at regular intervals. The security awareness and training program should include avoiding any use of malicious software, properly closing the application after use, and avoiding sharing of passwords among staff.

b) Another security issue is staff members using notepads to keep track of their system logins. To avoid misuse, they must save the login credentials they find difficult to remember at a secure location, such as locked drawers rather than using stick pads on the desk.

7.2 Contingency plan

It is very important to have proper contingency planning to assure that critical (health related) data survive a natural or human-made disaster. With the need to have access to patient information 24 hours a day and 7 days a week for the provision of care, this aspect of the system is extremely important. At present, there are no policies and procedures in place to protect electronic health records from natural or human-made disasters. In order to deal with emergency situations that can be a threat to vital patient information, there must be a data backup plan, risk analysis, disaster recovery plan, emergency mode operation plan, and testing and revision procedures.

An ongoing audit trail must be implemented for all transactions and accesses to the system. Random and directed review of the audit trail should be accomplished regularly to test compliance with confidentiality policies and procedures.

7.3 Automatic Logoff Mechanism

Users should be responsible for turning their IT system off when their workstation is not in use. However, I have noticed that many users often forget to turn off their workstation. To deal with this issue, implementing an automatic logoff mechanism after a predetermined time of inactivity can be a very effective methodology for protecting IT systems from unauthorized users. The automatic logoff mechanism will force any authorized or unauthorized user or intruder to re-login to again access the IT system whenever the workstation is left unattended by the authorized user.

7.4 IP tracking Mechanism

The IP tracking mechanism tracks who attempts, as well as when and where attempts are made to access the web application. If we can track this information (IP address of M/C, time, and location) in the system, we can easily restrict access to the TigerPlace EMR web application using a firewall or other mechanism. For instance, we know the location (Columbia, Missouri) of the authorized individuals, and if someone from another location (let say: Heathrow, London) tries to access this web application, that access can be considered as unauthorized access by a malicious user and their IP address can be blocked to avoid any future attempts to access the web application.

7.5 Use of stored procedures

Stored procedures are another effective methodology that can be implemented in the TigerPlace web EMR application for dealing with SQL injections, as stored procedures restrict the user from directly interacting with the SQL code, ensuring the integrity and security of the data.

7.6 Database Privileges

Minimizing the database privilege that executes SQL queries will enhance database integrity and security. For instance, if the database does not have the drop or alter permission set on a specific table, the SQL injections that will try to delete or modify the record will not succeed.

7.7 Use of MD5 + Salt methodology instead of MD5 methodology

From the technical point of view, web-based EMR security can be further enhanced and improved by the use of MD5+ salt technology, which is an upgraded or modified methodology in regard to MD5 methodology to harden the process of decoding the password by the intruders. The need to implement MD5+ salt methodology is due to the fact that there are many methods that can decode the MD5 passwords with length of 5-6. However, with the use of MD5+ salt method, a new random alphanumeric string is added which increases the size of password string. The below illustrated how MD5+ salt mechanism is more effective then MD5 mechanism:

MD5 hash converts `("SauravG") = 6282ede2cd977a65ab206840fb1bce6d"`

MD5+ salt converts (“SauravG + Salt string") =
"(6282ede2cd977a65ab206840fb1bce6d + o6Mi122187Yre)" =
6282ede2cd977a65ab206840fb1bce6do6Mi122187Yre

7.8 SSL Certification

SSL, also called Secure Socket Layer, provides secure communication between the two different systems over the internet. The SSL mechanism is mainly used for web applications whenever there is a need to exchange information between client and server machine. The SSL serves a dual purpose (encryption and identification). The SSL layer hides or encrypts the sensitive information that is transmitted from one computer to another with the use of some encryption methodology. Secondly, it assists the client machine to identify the trusted server and prevents any unauthorized system from getting access to the information.

a) **Encryption Mechanism**: Using SSL certification, the client and server first exchange a few messages to decide the encryption algorithm and encryption key and to establish the secure connection. Once the secure connection is established, the web server sends the public key to the client machine to decrypt the information and uses an associated private key to decrypt the information when it is received from the client machine. All the information that is exchanged between client machines to the web server is sent in the encrypted format. This encrypted information that is exchanged between the different systems is garbage for the other unauthorized systems or programs. So, this SSL encryption mechanism eliminates the risk of sensitive information being stolen by malicious users. Figure 40 below illustrates how SSL encrypts the information over the internet and the garbage information is received when the unauthorized system try to intrude between the web server and client machine.

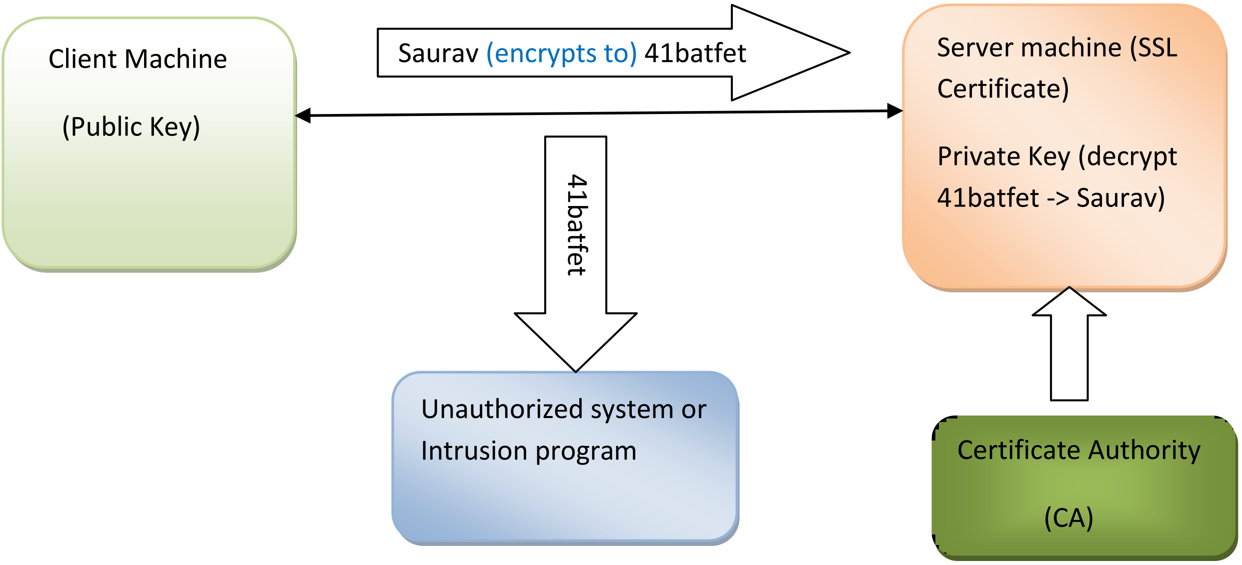
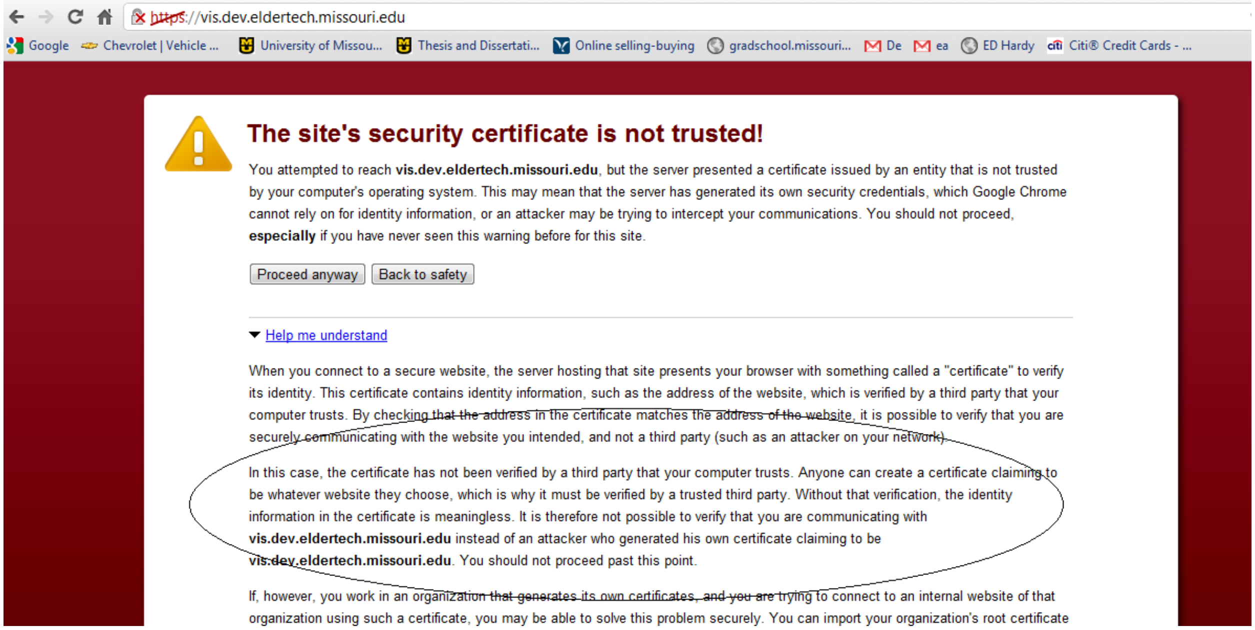

Client Machine
(Public Key)
Saurav (encrypts to) 41batfet
Server machine (SSL Certificate)
Private Key (decrypt 41batfet -> Saurav)
41batfet
Unauthorized system or Intrusion program
Certificate Authority
(CA)

Fig 40 – SSL Certificate Mechanism

b) **Identification Mechanism:** The SSL technology also ensures the client machine that the web server to whom it's connected is the trusted one. Whenever the client machine sends the connection request to the web server, the web browser will verify the information with the third party called certification authority (CA), who keeps track of the web server owner to ensure the validity and reliability of the web server. The SSL certificate is only provided by the certificate authority to the owner of web server, after carefully verifying the owner details.



The site's security certificate is not trusted!

You attempted to reach **vis.dev.eldertech.missouri.edu**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

When you connect to a secure website, the server hosting that site presents your browser with something called a "certificate" to verify its identity. This certificate contains identity information, such as the address of the website, which is verified by a third party that your computer trusts. By checking that the address in the certificate matches the address of the website, it is possible to verify that you are securely communicating with the website you intended, and not a third party (such as an attacker on your network).

In this case, the certificate has not been verified by a third party that your computer trusts. Anyone can create a certificate claiming to be whatever website they choose, which is why it must be verified by a trusted third party. Without that verification, the identity information in the certificate is meaningless. It is therefore not possible to verify that you are communicating with **vis.dev.eldertech.missouri.edu** instead of an attacker who generated his own certificate claiming to be **vis.dev.eldertech.missouri.edu**. You should not proceed past this point.

If, however, you work in an organization that generates its own certificates, and you are trying to connect to an internal website of that organization using such a certificate, you may be able to solve this problem securely. You can import your organization's root certificate

Fig 41 – TigerPlace Web application lacking SSL Certification

So, the use of Secure Socket Layer will certainly help the TigerPlace web EMR system to improve and enhance the three important areas of web security concerns; authentication: verifying the valid web server during connection, confidentiality: ensuring the data are transmitted in encrypted form, and integrity: ensuring that data will not be modified during transmission.

7.9 Physical Access Control

Physical security control is another method that organizations must implement effectively to mitigate the intensity of damage to the facilities and IT systems that deal with the protecting of vital information from the intruder. Effective physical security control will act as a roadblock or barrier against the intruder who will try to move toward sensitive areas within the facility, and will assist in protecting the misuse and theft of information. The physical access control within the organization can be achieved with the use of secure locked doors, cable locks, and security personnel. This security measure will allow physical access to the data center only to the right personnel who possess the key. Physical access controls are not only limited to prevent damage from humans, but also intended to prevent damage from natural events, such as earthquake, hurricane, floods, etc. The physical prevention controls include: regular backups of data and information, proper use of fences, secured location of data centers, limited access to buildings through the use of badge systems, locks, etc., security personnel at various entrances, alternative use of power sources, such as uninterruptible power supplies or generators in-case of electricity loss, fire detection and suppressions systems in case of fire in the organization.

7.9.1 Use of Locks

Locks are another effective method that helps in protecting valuable data from being stolen. The three common types of lock that can be effective in protecting valuable data and information include: card reader, combination locks, and push-button/cipher locks. Card readers are the electronic deceives that aid the efficient management of authorized access and the monitor the entry points. The locks, like the card reader, allow access to the entry points by releasing the lock controlled by the reader. The few disadvantages of this kind of lock include cost of installation, maintenance, and most importantly, lost or mishandling of badges by authorized personnel can result in the compromise of physical security. Combination locks are another type of inexpensive lock alternative to the badge reader, which facilitate the management of authorized access to the private areas. Combination locks are easy to handle locks, as it is an easy system for the administrator/controller to change the code whenever there is the possibility of the code being compromised by unauthorized personnel. Push-buttons are another type of commonly used locks, which allow authorized personnel to enter a code using the numbered buttons attached to the mechanical device and the locking mechanism is released if code is accepted; otherwise, the door remains closed and warning messages popup in-case of the wrong code being entered. Push-buttons locks are easy to handle locks, as it’s easy for system administrator/controller to change the code whenever there is an uncertainty of whether the code is being compromised by unauthorized personnel.

7.9.2 Locations

The geographic location of the data center plays a major role in the level of risk for business operations. Any organization that deals with processing of vital information must select a location that is free from physical threats caused by humans or natural disasters for uninterruptable business operations. Human and natural disasters, such as high crime rate, hurricanes, earthquake, violent storms, and power outages, may cause significant damage to the organization in term of dollars and organization reputation. Security events related to quick reaction times will radically reduce business impact.

7.9.3 Fire Suppressions

Fire suppression plays an important role in preventing the IT infrastructure from damage or demolition by the fire in the organization. Fire extinguishers are one of the common types of fire suppression that can be used to protect IT infrastructure, and to assist personnel evacuating from affected or risky areas and minimizing the risk to one’s life. Fire extinguishers may not be effective enough to suppress a large fire, but can be used to control small fires in contained areas.

7.9.4 Intrusion Detection and Prevention Tool

TigerPlace EMR system security can be further enhanced by the use of intrusion detection and protection (IDS and IPS) systems that monitor intruder activities and prevent the internal network from being accessed by an unauthenticated systems/users. The IDS continuously monitors and detects system vulnerabilities associated with user activities, and IPS prevents the action that can cause damage to the internal system or the entire network based on the algorithm defined by the user or system (Conorich, 2004). The IDS/IPS can be placed either on the port of entry of the internal network to protect the network segment or a single standalone machine to protect the individual systems. The figure-42 and figure-43 below illustrates the use of IDS/IPS on entire internal network and individual systems.

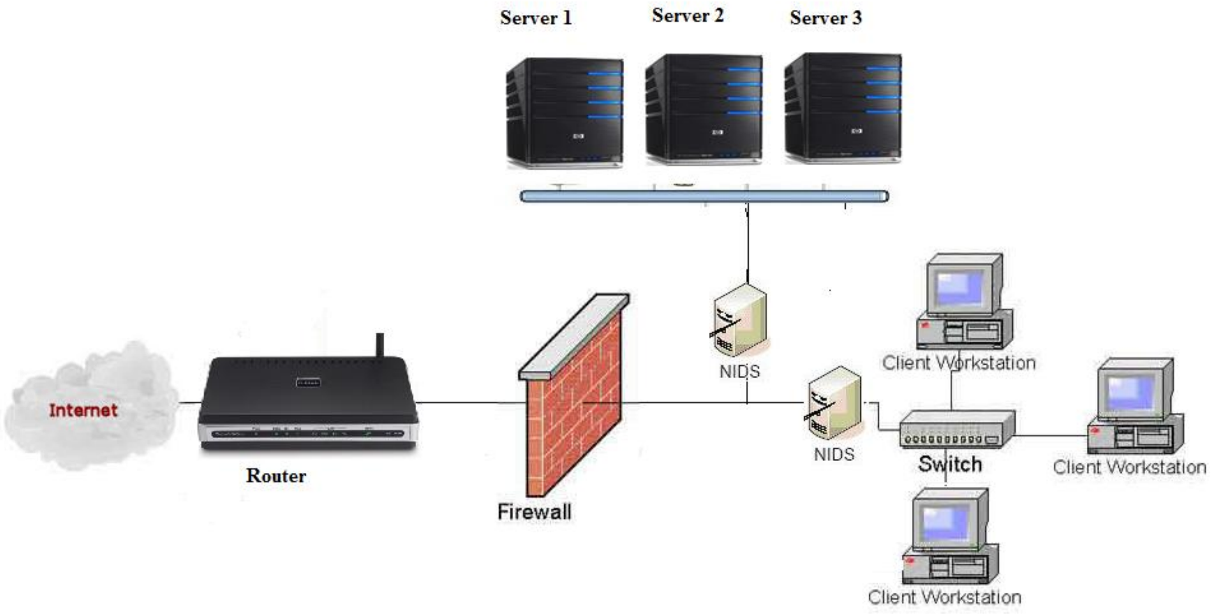


Fig 42 - Intrusion Detection/Prevention System Network Based Security

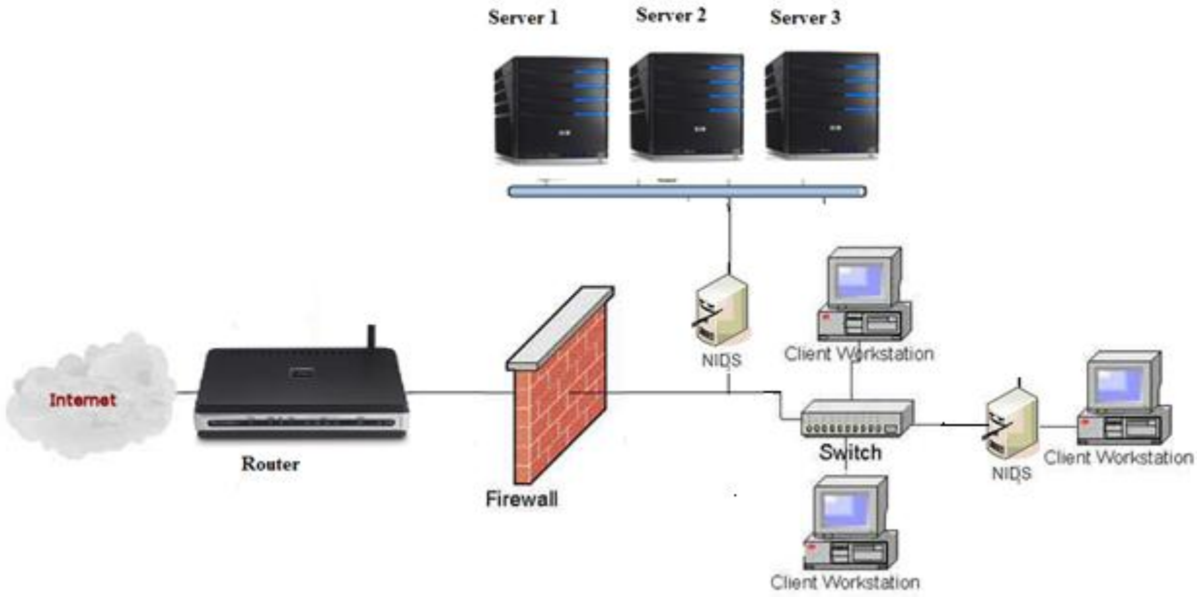


Fig 43 - Intrusion Detection/Prevention System Host Based Security

CHAPTER 8

CONCLUSION

This thesis will inform healthcare organizations that are involved directly and indirectly with EMR systems. This thesis describes various security measures that are essential for keeping the web-based EMR system secure from unauthorized users. With the increased number of web attacks in the last decade, the TigerPlace EMR system demands more robust security features to be implemented in the near future to ensure the integrity, availability, and confidentiality of patients' records.

It is important to note that developing and implementing the web-based EMR system in any healthcare setting that is 100% foolproof is practically impossible. However, the appropriate use and implementation of various security safeguards (administrative, physical, and technical) will ensure integrity, confidentiality, and availability of patient information, and protect the covered entity or an organization as a whole from being penalized by HIPAA. Finally, this thesis can serve as a meaningful document for appropriate use of EMR systems to nurses or other technical staff.

REFERENCES

Alexander, G. L. & Wakefield, D. S. (2009). Information Technology Sophistication in Nursing Homes. *J Am Med Dir Assoc*; 10(6):398-407.

Andonov, A. (2007). The Unexpected SQL Injection: When Escaping Is Not Enough. http://www.webappsec.org/ projects/articles/ 091007.shtml

Aud, M., Alexander, G. L., Rantz, M., and Skubic, M. (2007). "Use of sensor system data for early detection of health status changes in older adult residents of a retirement community," Midwest Nursing Research Society Conference, Omaha, Nebraska.

Auger, R. (2007). The Business case for security frameworks. http://www.webappsec.org/ projects/articles/042307.shtml

Bashshur, R.L. (2002). Telemedicine and Health Care. *Telemedicine Journal And e-Health , 8* (2): 5-12.

Centers for Medicare & Medicaid Services, Health Insurance Portability and Accountability Act of 1996, available at http://www.hhs.gov/hipaa (last modified Oct.16, 2002); accessed Nov. 15, 2003.

Christiansen, J. (2000). Electronic health information*: Privacy and security compliance under HIPAA*. American Health Lawyers Association, Washington, D.C.

Cimino, J. J., Sengupta, S., Patel, V. L., Kushniruk, A. & Huang, X. (1998). Architecture for a Web-Based Clinical Information System that Keeps the Design Open and the Access Closed. *AMIA*, 121-125.

Coleman, J. (2004). Assessing Information Security Risk in Healthcare Organizations of Different Scales. *CARS*, 1-4.

Conorich, D, G. (2004). Monitoring Intrusion Detection Systems: From Data to Knowledge; 13(2): 19-30.

Craig, J.S. (2009). The human element: Training, awareness, and human resources implications of health information security policy under the Health Insurance Portability and Accountability Act (HIPAA). 95-99.

Dennis, J. C. (2000). Privacy & confidentiality of health information. San Francisco: Jossey-Bass.

Department of Health and Human Services (2003). 45 CFR Parts 160, 162 and 164. Health Insurance Reform: Security Standards; Final Rule. http://aspe.hhs.gov/admnsimp/final/FR03-8334.pdf

Fitzgerald, T. (2003). HIPAA security rule 101: The time to act is now. *Information Systems Security*; 12(1): 43.

Frank, S. M. (2002). How HIPAA Will Change Your Practice. *Nursing 2002*; 32(9):54-57.

Huseby, S. H. (2005). Common Security problems in the code of Dynamic Web Applications. http://www.webappsec.org/articles/

Jones, T.S., Ghosh, T. S., Horn, K., Smith, J., Vogt, R. L. (Sep 2011). Primary care physician's perceptions and practices regarding fall prevention in adult's 65 years and over. 43(5):1605-1609.

Kohane, I.S. (1996). Exploring the functions of World Wide Web-based electronic medical record systems. *MD Comput*; 13(4):339-46.

Kohane, I.S., Wingerde, F.J., Fackler, J.C. (1996). Sharing electronic medical records across multiple heterogeneous and competing institutions, 608-12.

Kurtz, G. (2003). EMR confidentiality and information security. Journal of *Healthcare Informatics Management*; 17(3):41-8.

Lorence, D. P. & Churchill, R. (2005). Incremental Adoption of Information Security in Health-Care Organizations: Implications for Document Management. *IEEE Transaction on Information Technology in Biomedicine*; 9(2):169-173.

Lourde, K. (2009). Long Term Care Health Information Technology Inevitable. *Provider;* 35(3): 21-32.

Mack, D., Alwan, M., Turner, B., Suratt, R., and Felder, R. (2006). A passive and portable system for monitoring heart rate and detecting sleep apnea and arousals: Preliminary validation, Proceedings Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2), Arlington VA, 51-54.

Olzak, T. (2006). Just Enough Security: Information Security for Business Managers. *Erudio Security, LLC.*

Ramakrishnan, R. & Gehrke, J. (2009). Database Management Systems. *The McGraw-HillCompanies, Inc., Avenue of Americas, New York, NY*.

Rantz, M. J., Dorman-Marek K., Aud, M. A., Tyrer, H. W., Skubic, M., Demiris, G., and Hussam, A. (2005). A technology and nursing collaboration to help older adults age in place, Nursing Outlook, 53(2), 40-45.

Rantz, M. J., Skubic, M., Alexander, G., Popescu, M., Aud, M. A., Wakefield, B. J. (2010). Developing a Comprehensive Electronic Health Record to Enhance Nursing Care Coordination, Use of Technology, and Research. *Journal of GerontoloGical nursing;* 36(1), 13-17.

Rind, D.M., Kohane, I.S., Szolovits, P., Safran, C., Chueh, H.C., Barnett, G.O. (1997). Maintaining the confidentiality of medical records shared over the Internet and the World Wide Web. *Ann Intern Med*; 127(2):138-41.

Scharlach, A. (2008). Supporting Family Care Givers. *American Journal of Nursing;108(9),* 16-22.

Schiller,J.S., Kramarow, E.A., Dey A.N.(2007).Fall injury episodes among non-institutionalized older adults. 21(392):1-16.

Starren, J., Tsai, C., Bakken, S., Aidala, A.(2005). The role of nurses in installing telehealth technology in the home. *Computer Information Nursing*; 23(4): 181-9

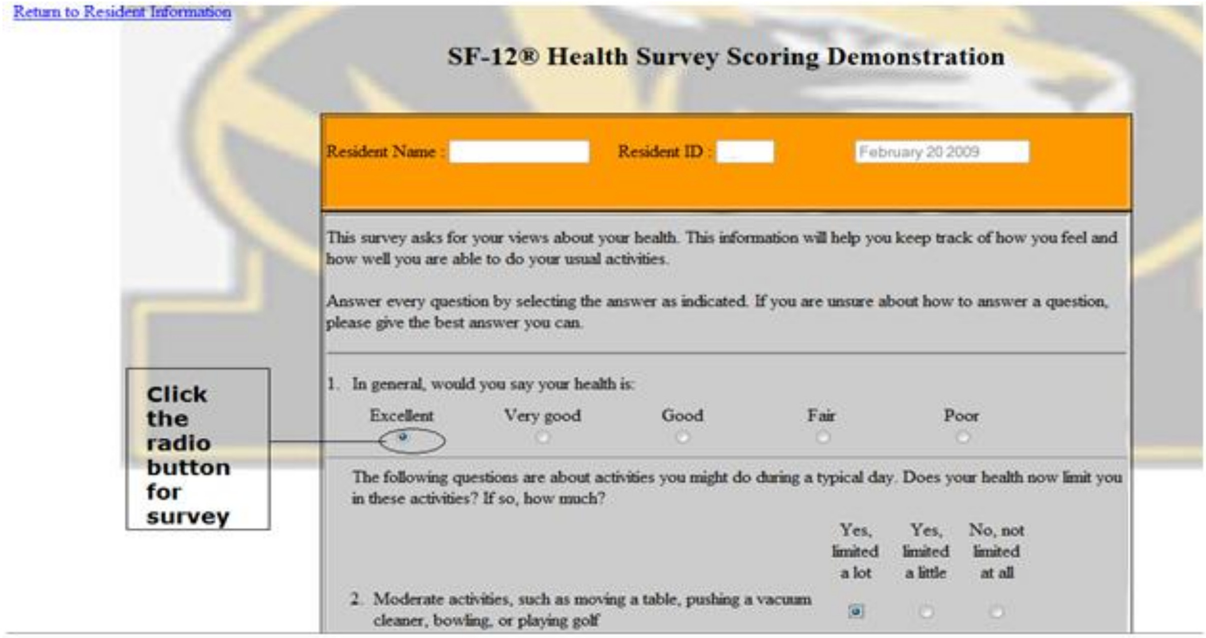
Symantec Internet Security Threat Report: Trends for July–December 2007 (Executive Summary). XIII. April 2008. pp. 1–3. Retrieved May 11, 2008. http://eval.symantec.com.

Szydlowski, M., Kruegel, C., Kirda, C. (2006). Secure Input for Web Applications. ACSAC; 2007: 375-384

Web Application Security Consortium. (2005). Retrieved May 28, 2008. http://www.webappsec.org/

World Wide Web Consortium (2008). Retrieved December 2010. http://www.w3.org/.

APPENDIX – I (Assessment Forms)



Return to Resident Information

SF-12® Health Survey Scoring Demonstration

Resident Name : ______ Resident ID : ______ February 20 2009

This survey asks for your views about your health. This information will help you keep track of how you feel and how well you are able to do your usual activities.

Answer every question by selecting the answer as indicated. If you are unsure about how to answer a question, please give the best answer you can.

1. In general, would you say your health is:

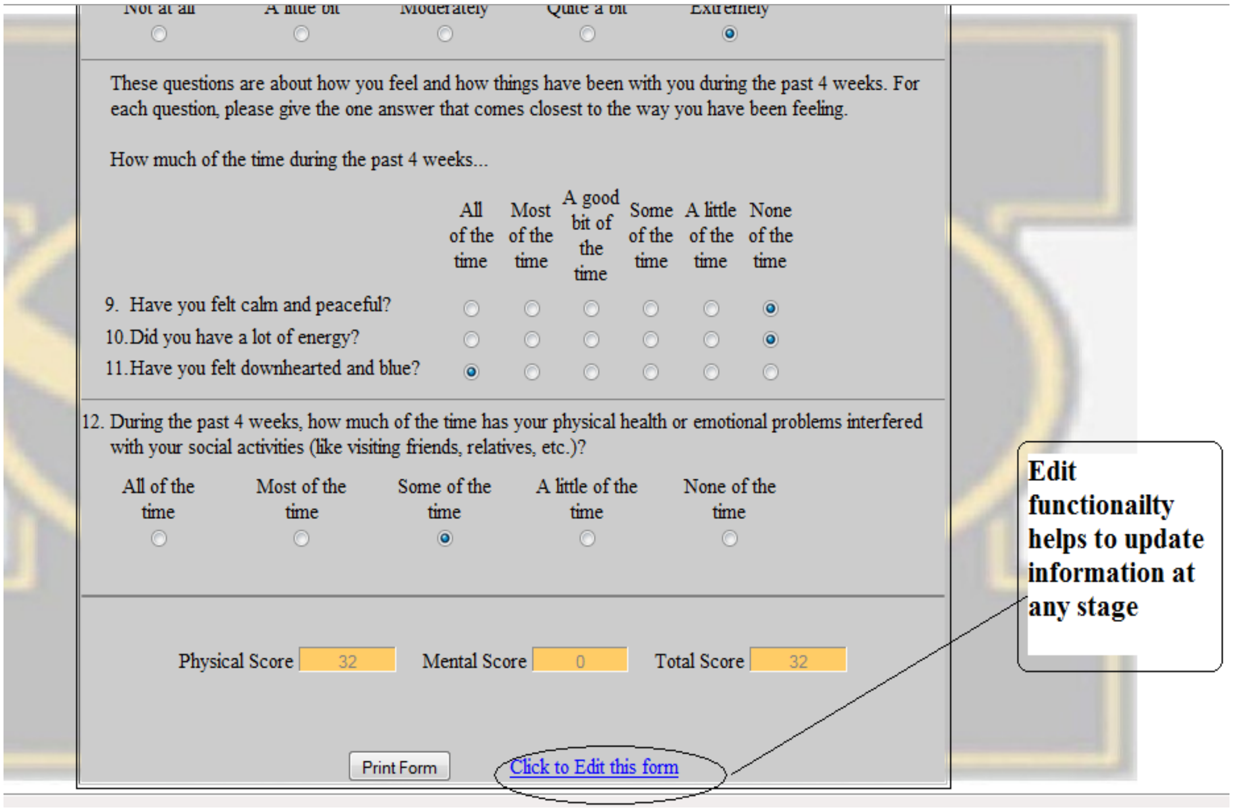
Excellent	Very good	Good	Fair	Poor
●	○	○	○	○

Click the radio button for survey

The following questions are about activities you might do during a typical day. Does your health now limit you in these activities? If so, how much?

	Yes, limited a lot	Yes, limited a little	No, not limited at all
2. Moderate activities, such as moving a table, pushing a vacuum cleaner, bowling, or playing golf	●	○	○

SF-12 Form (Before Survey)



Not at all	A little bit	Moderately	Quite a bit	Extremely
○	○	○	○	●

These questions are about how you feel and how things have been with you during the past 4 weeks. For each question, please give the one answer that comes closest to the way you have been feeling.

How much of the time during the past 4 weeks...

	All of the time	Most of the time	A good bit of the time	Some of the time	A little of the time	None of the time
9. Have you felt calm and peaceful?	○	○	○	○	○	●
10. Did you have a lot of energy?	○	○	○	○	○	●
11. Have you felt downhearted and blue?	●	○	○	○	○	○

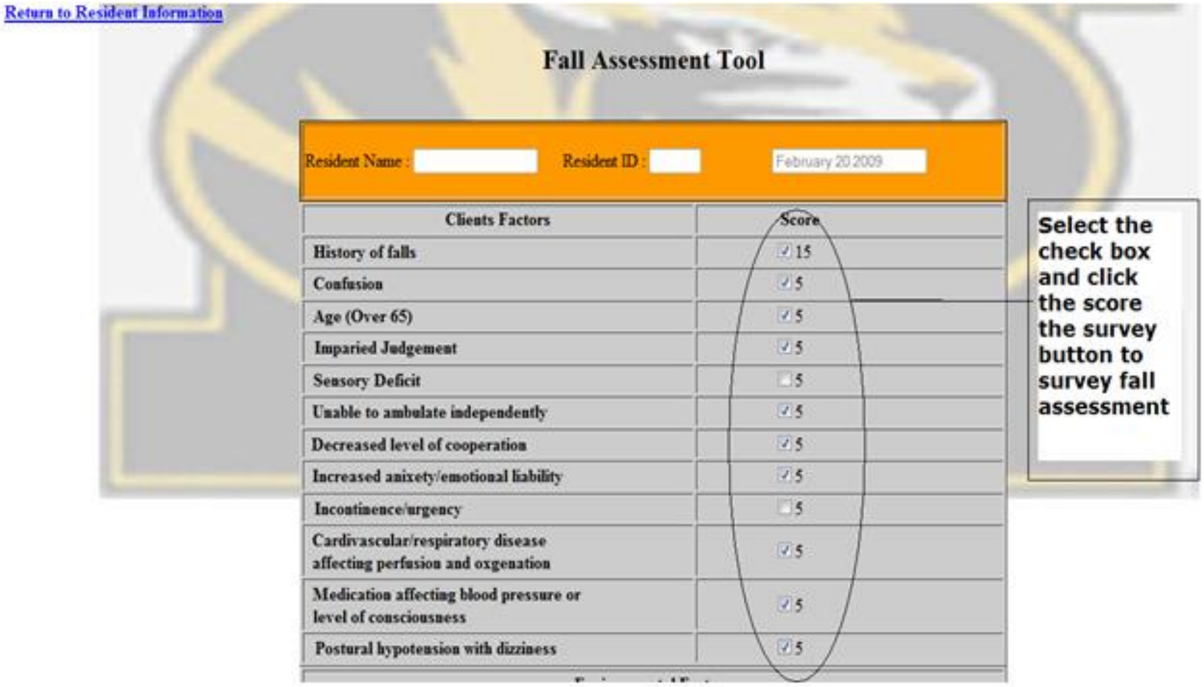
12. During the past 4 weeks, how much of the time has your physical health or emotional problems interfered with your social activities (like visiting friends, relatives, etc.)?

All of the time	Most of the time	Some of the time	A little of the time	None of the time
○	○	●	○	○

Physical Score 32 Mental Score 0 Total Score 32

Edit functionailty helps to update information at any stage

SF-12 Form (After Survey)



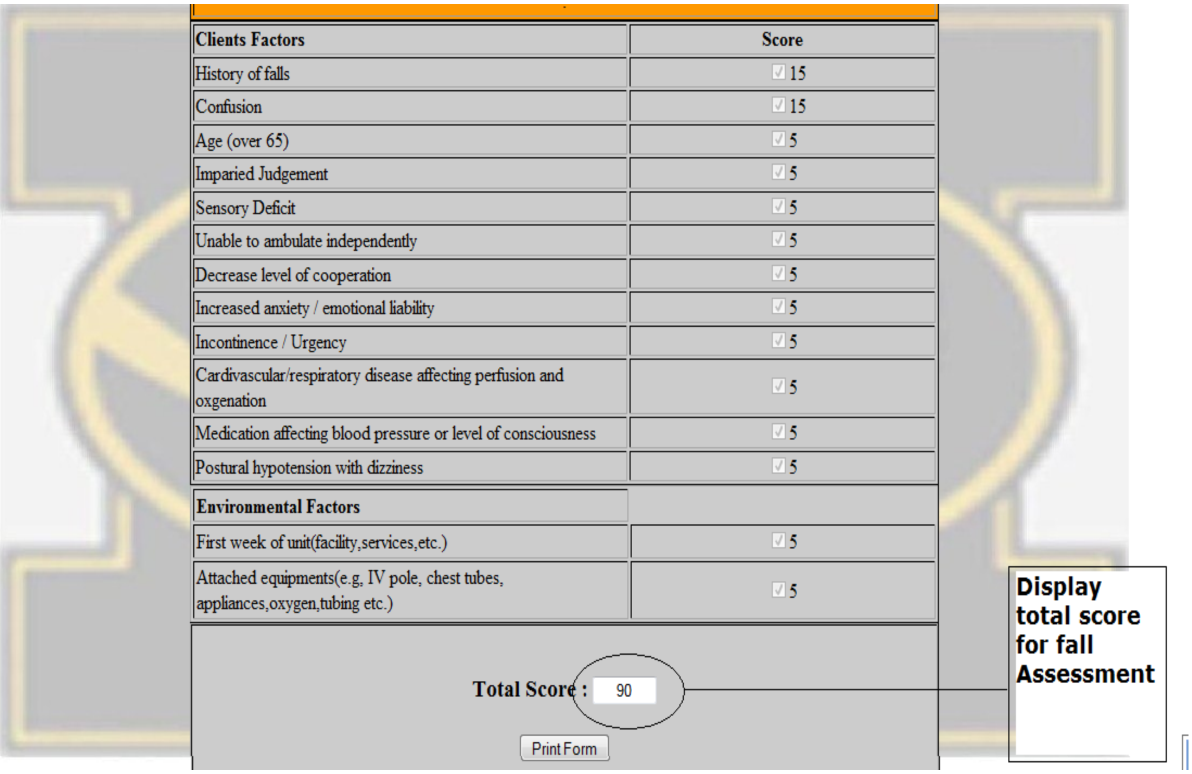
Fall Assessment Tool

Resident Name : Resident ID : February 20 2009

Clients Factors	Score
History of falls	☑ 15
Confusion	☑ 5
Age (Over 65)	☑ 5
Imparied Judgement	☑ 5
Sensory Deficit	□ 5
Unable to ambulate independently	☑ 5
Decreased level of cooperation	☑ 5
Increased anixety/emotional liability	☑ 5
Incontinence/urgency	□ 5
Cardivascular/respiratory disease affecting perfusion and oxgenation	☑ 5
Medication affecting blood pressure or level of consciousness	☑ 5
Postural hypotension with dizziness	☑ 5

Select the check box and click the score the survey button to survey fall assessment

Fall Assessment Form (Before Survey)

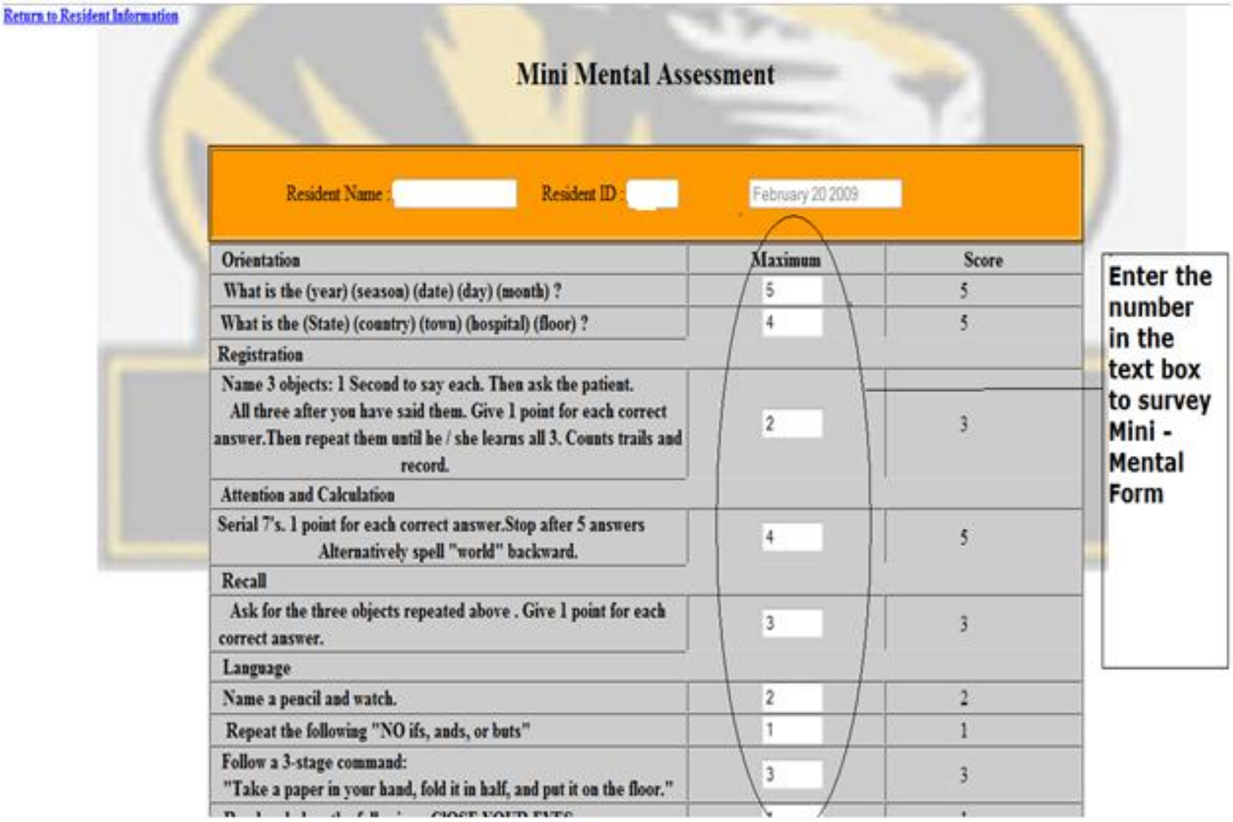


Clients Factors	Score
History of falls	☑ 15
Confusion	☑ 15
Age (over 65)	☑ 5
Imparied Judgement	☑ 5
Sensory Deficit	☑ 5
Unable to ambulate independently	☑ 5
Decrease level of cooperation	☑ 5
Increased anxiety / emotional liability	☑ 5
Incontinence / Urgency	☑ 5
Cardivascular/respiratory disease affecting perfusion and oxgenation	☑ 5
Medication affecting blood pressure or level of consciousness	☑ 5
Postural hypotension with dizziness	☑ 5
Environmental Factors	
First week of unit(facility,services,etc.)	☑ 5
Attached equipments(e.g, IV pole, chest tubes, appliances,oxygen,tubing etc.)	☑ 5

Total Score : 90

Display total score for fall Assessment

Fall Assessment Form (After Survey)



Return to Resident Information

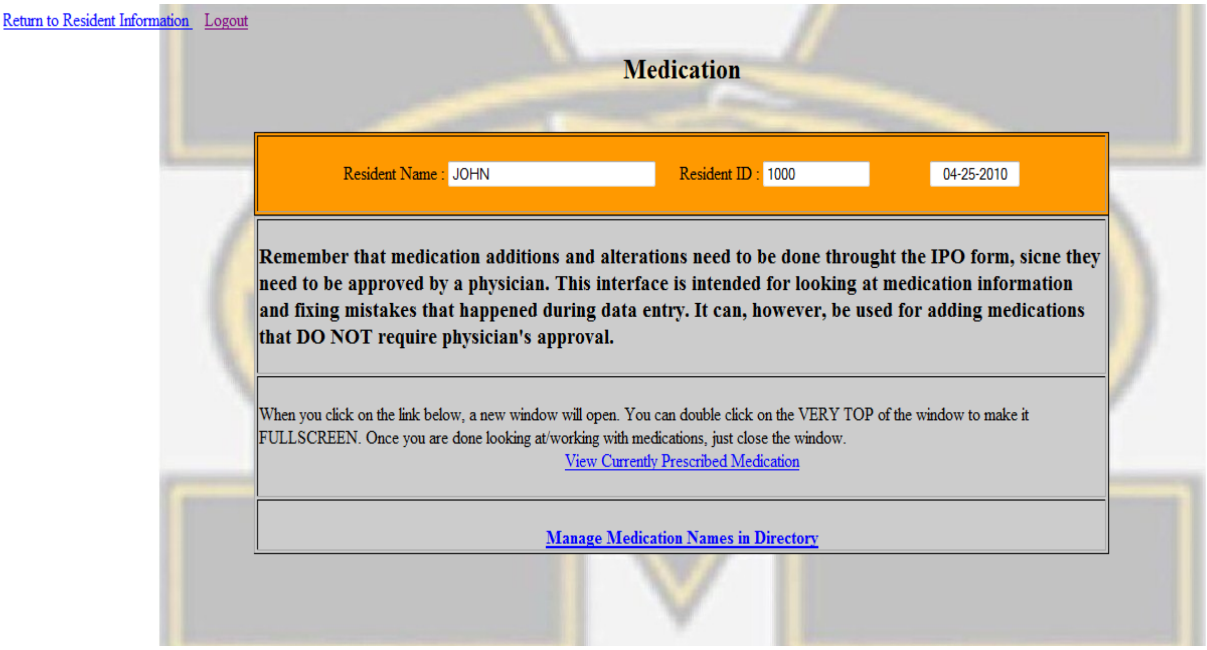
Mini Mental Assessment

Resident Name : Resident ID : February 20 2009

Orientation	Maximum	Score
What is the (year) (season) (date) (day) (month) ?	5	5
What is the (State) (country) (town) (hospital) (floor) ?	4	5
Registration		
Name 3 objects: 1 Second to say each. Then ask the patient. All three after you have said them. Give 1 point for each correct answer.Then repeat them until he / she learns all 3. Counts trails and record.	2	3
Attention and Calculation		
Serial 7's. 1 point for each correct answer.Stop after 5 answers Alternatively spell "world" backward.	4	5
Recall		
Ask for the three objects repeated above . Give 1 point for each correct answer.	3	3
Language		
Name a pencil and watch.	2	2
Repeat the following "NO ifs, ands, or buts"	1	1
Follow a 3-stage command: "Take a paper in your hand, fold it in half, and put it on the floor."	3	3

Enter the number in the text box to survey Mini - Mental Form

Mini Mental Assessment



Return to Resident Information Logout

Medication

Resident Name : JOHN Resident ID : 1000 04-25-2010

Remember that medication additions and alterations need to be done throught the IPO form, sicne they need to be approved by a physician. This interface is intended for looking at medication information and fixing mistakes that happened during data entry. It can, however, be used for adding medications that DO NOT require physician's approval.

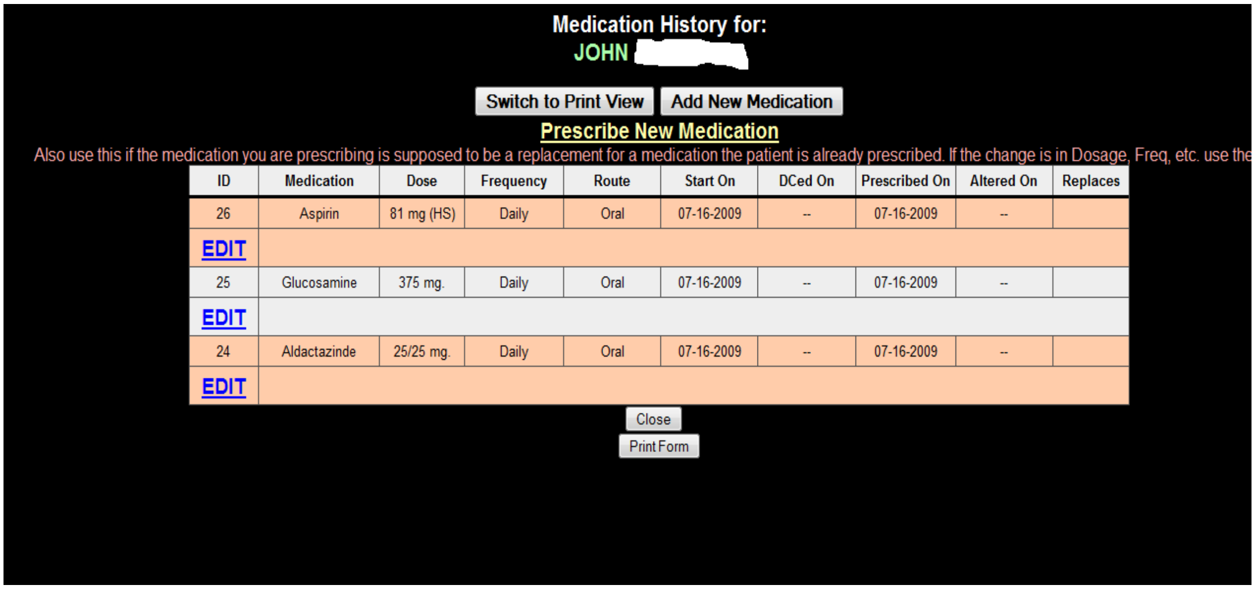
When you click on the link below, a new window will open. You can double click on the VERY TOP of the window to make it FULLSCREEN. Once you are done looking at/working with medications, just close the window.

View Currently Prescribed Medication

Manage Medication Names in Directory

APPENDIX – II (Medication Form)

Medication Form (1)



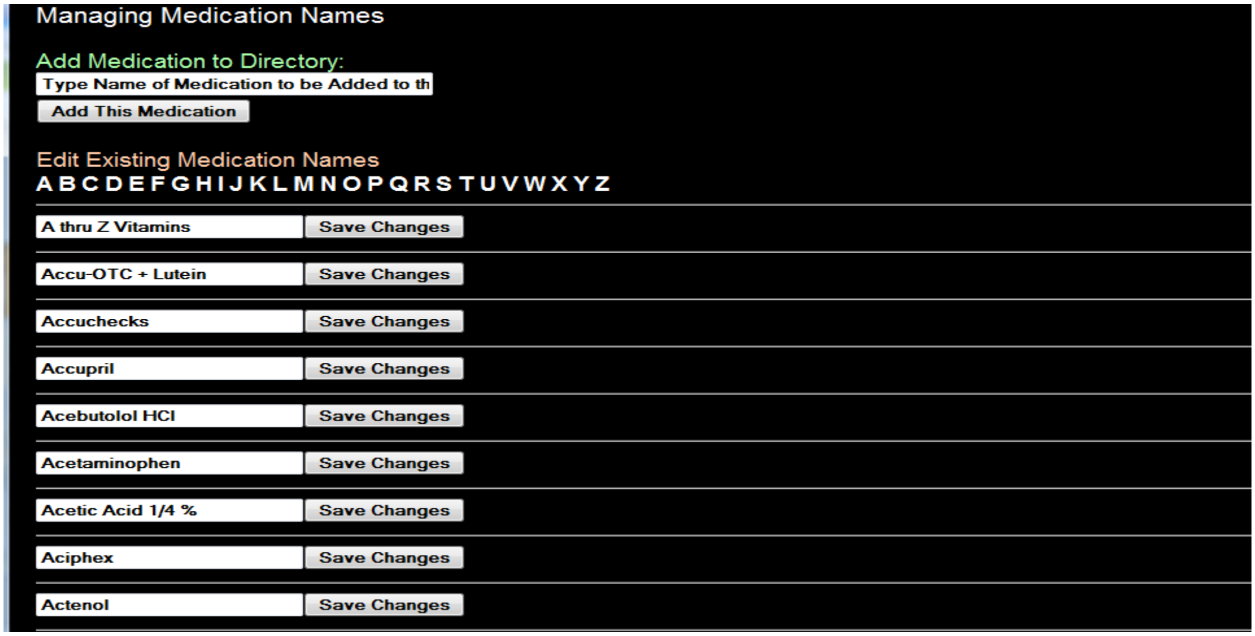
Medication History for:
JOHN [redacted]

Prescribe New Medication

Also use this if the medication you are prescribing is supposed to be a replacement for a medication the patient is already prescribed. If the change is in Dosage, Freq, etc. use the

ID	Medication	Dose	Frequency	Route	Start On	DCed On	Prescribed On	Altered On	Replaces
26	Aspirin	81 mg (HS)	Daily	Oral	07-16-2009	--	07-16-2009	--	
EDIT									
25	Glucosamine	375 mg.	Daily	Oral	07-16-2009	--	07-16-2009	--	
EDIT									
24	Aldactazinde	25/25 mg.	Daily	Oral	07-16-2009	--	07-16-2009	--	
EDIT									

Medication Form (2)



Managing Medication Names

Add Medication to Directory:

Type Name of Medication to be Added to th

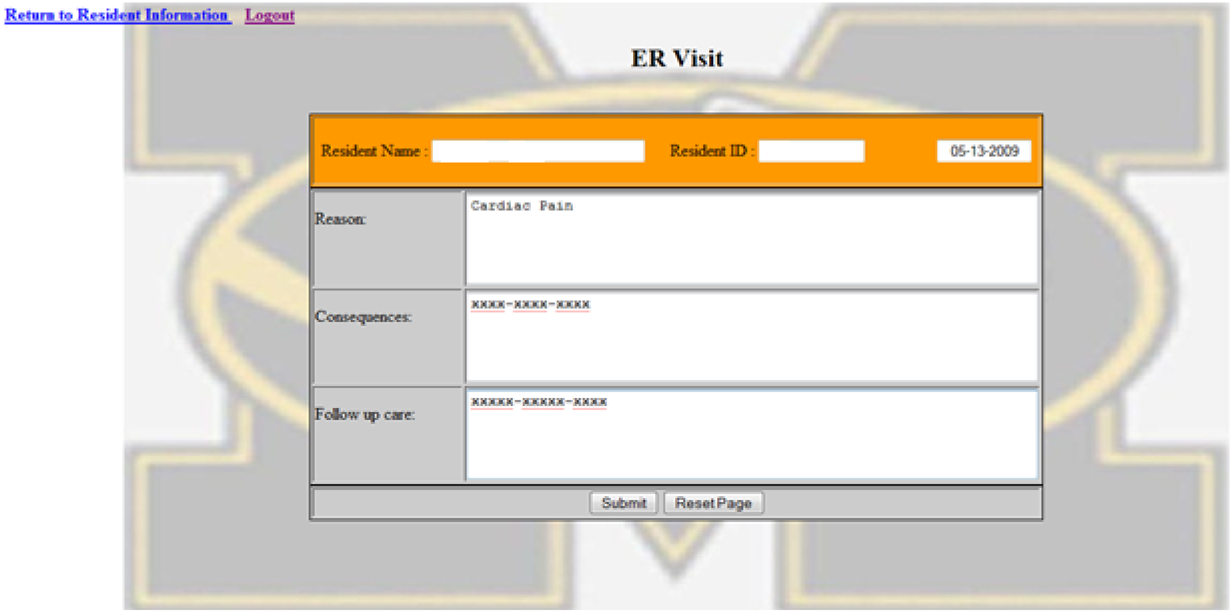
Edit Existing Medication Names

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A thru Z Vitamins	Save Changes
Accu-OTC + Lutein	Save Changes
Accuchecks	Save Changes
Accupril	Save Changes
Acebutolol HCl	Save Changes
Acetaminophen	Save Changes
Acetic Acid 1/4 %	Save Changes
Aciphex	Save Changes
Actenol	Save Changes

Medication Form (3)

APPENDIX-III (ER Visit Form)



ER Visit

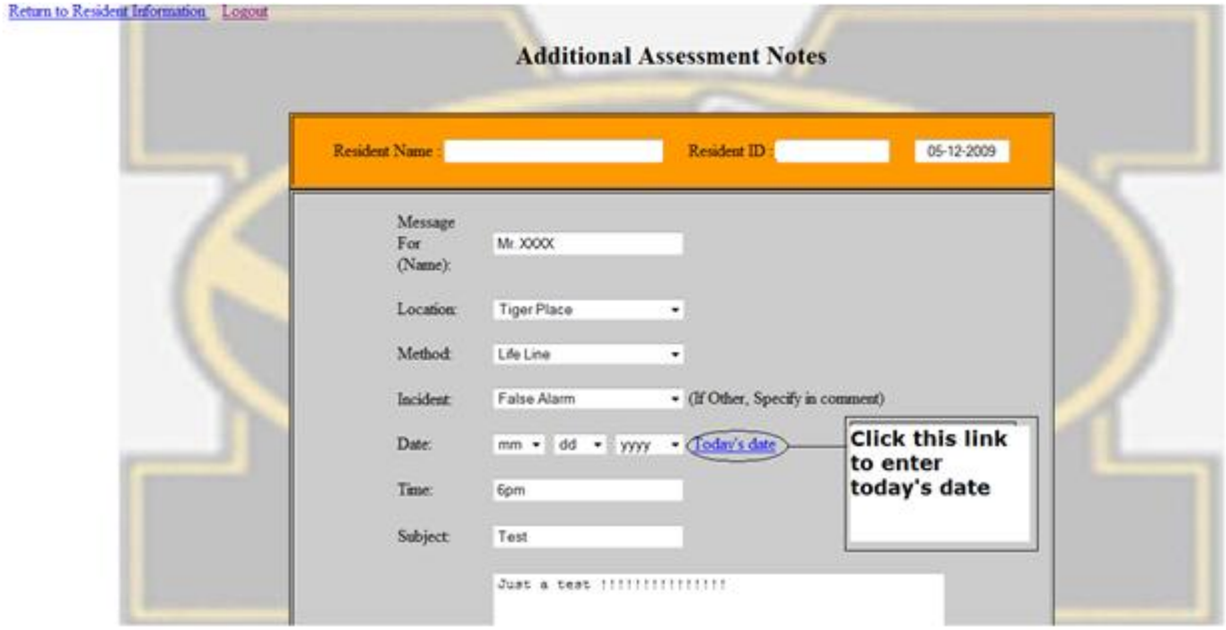
Resident Name : Resident ID : 05-13-2009

Reason: Cardiac Pain

Consequences: xxxx-xxxx-xxxx

Follow up care: xxxxx-xxxxx-xxxx

ER Visit Form



Additional Assessment Notes

Resident Name : Resident ID : 05-12-2009

Message For (Name): Mr. XXXX

Location: Tiger Place

Method: Life Line

Incident: False Alarm (If Other, Specify in comment)

Date: mm dd yyyy Today's date

Click this link to enter today's date

Time: 6pm

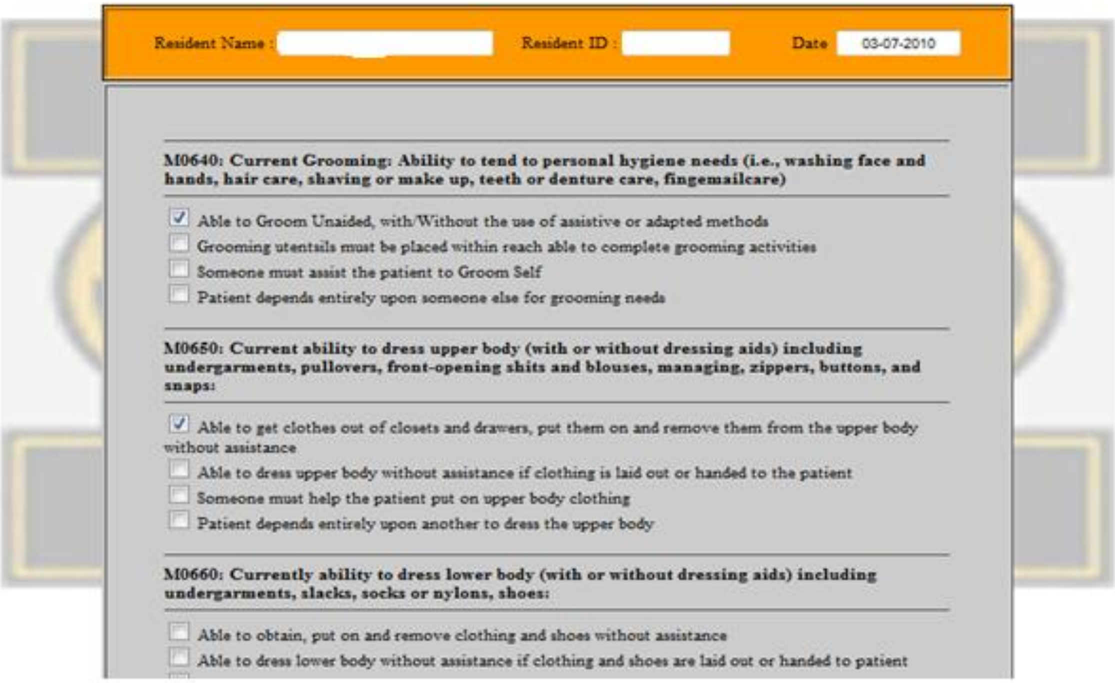
Subject: Test

Just a test !!!!!!!!!!!!!!!

Progress Note Form

APPENDIX – IV (ADL form)

ADL



Resident Name : Resident ID : Date 03-07-2010

M0640: Current Grooming: Ability to tend to personal hygiene needs (i.e., washing face and hands, hair care, shaving or make up, teeth or denture care, fingemailcare)

☑ Able to Groom Unaided, with/Without the use of assistive or adapted methods
□ Grooming utentsils must be placed within reach able to complete grooming activities
□ Someone must assist the patient to Groom Self
□ Patient depends entirely upon someone else for grooming needs

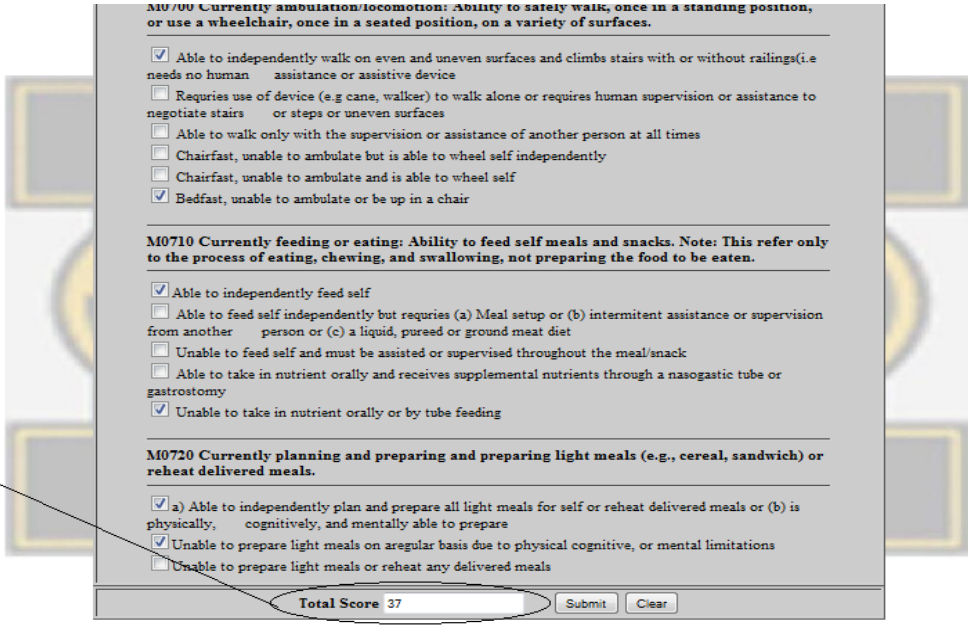
M0650: Current ability to dress upper body (with or without dressing aids) including undergarments, pullovers, front-opening shits and blouses, managing, zippers, buttons, and snaps:

☑ Able to get clothes out of closets and drawers, put them on and remove them from the upper body without assistance
□ Able to dress upper body without assistance if clothing is laid out or handed to the patient
□ Someone must help the patient put on upper body clothing
□ Patient depends entirely upon another to dress the upper body

M0660: Currently ability to dress lower body (with or without dressing aids) including undergarments, slacks, socks or nylons, shoes:

□ Able to obtain, put on and remove clothing and shoes without assistance
□ Able to dress lower body without assistance if clothing and shoes are laid out or handed to patient

ADL Form (1)



M0700 Currently ambulation/locomotion: Ability to safely walk, once in a standing position, or use a wheelchair, once in a seated position, on a variety of surfaces.

☑ Able to independently walk on even and uneven surfaces and climbs stairs with or without railings(i.e needs no human assistance or assistive device
□ Requries use of device (e.g cane, walker) to walk alone or requires human supervision or assistance to negotiate stairs or steps or uneven surfaces
□ Able to walk only with the supervision or assistance of another person at all times
□ Chairfast, unable to ambulate but is able to wheel self independently
□ Chairfast, unable to ambulate and is able to wheel self
☑ Bedfast, unable to ambulate or be up in a chair

M0710 Currently feeding or eating: Ability to feed self meals and snacks. Note: This refer only to the process of eating, chewing, and swallowing, not preparing the food to be eaten.

☑ Able to independently feed self
□ Able to feed self independently but requries (a) Meal setup or (b) intermitent assistance or supervision from another person or (c) a liquid, pureed or ground meat diet
□ Unable to feed self and must be assisted or supervised throughout the meal/snack
□ Able to take in nutrient orally and receives supplemental nutrients through a nasogastic tube or gastrostomy
☑ Unable to take in nutrient orally or by tube feeding

M0720 Currently planning and preparing and preparing light meals (e.g., cereal, sandwich) or reheat delivered meals.

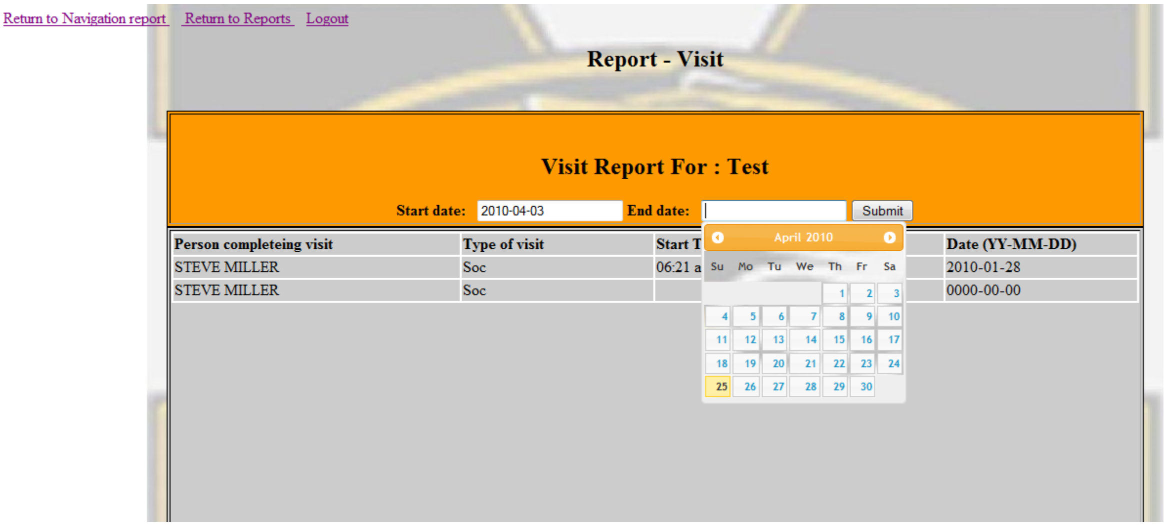
☑ a) Able to independently plan and prepare all light meals for self or reheat delivered meals or (b) is physically, cognitively, and mentally able to prepare
☑ Unable to prepare light meals on aregular basis due to physical cognitive, or mental limitations
□ Unable to prepare light meals or reheat any delivered meals

Total Score 37

Score is calculated based on the checkbox option selected by the user

ADL Form (2)

APPENDIX – V (Report Form)



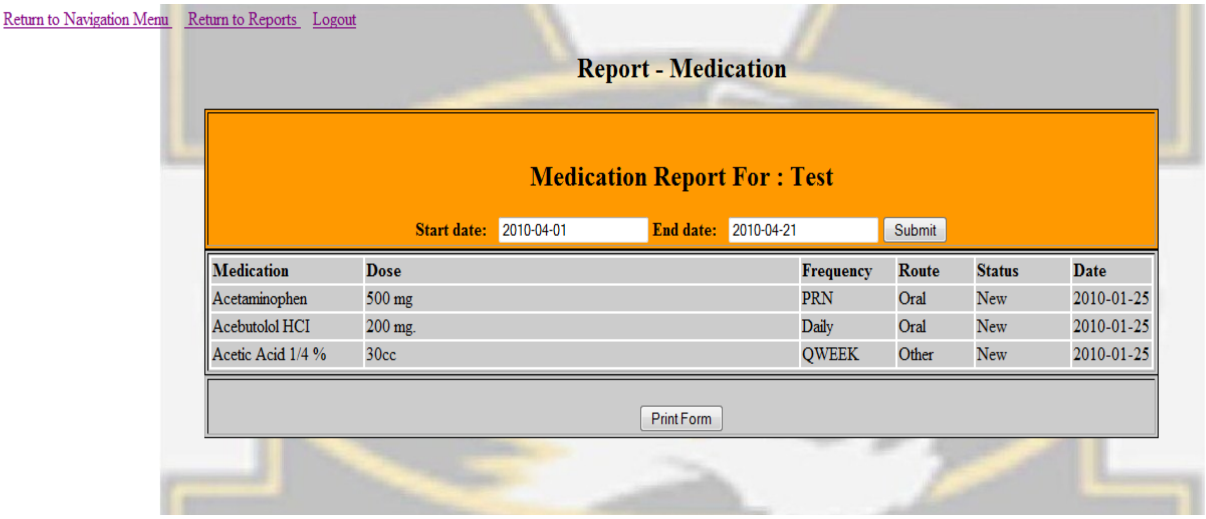
Report - Visit

Visit Report For : Test

Start date: 2010-04-03 End date:

Person completeing visit	Type of visit	Start T	Date (YY-MM-DD)
STEVE MILLER	Soc	06:21 a	2010-01-28
STEVE MILLER	Soc		0000-00-00

Visit Report



Report - Medication

Medication Report For : Test

Start date: 2010-04-01 End date: 2010-04-21

Medication	Dose	Frequency	Route	Status	Date
Acetaminophen	500 mg	PRN	Oral	New	2010-01-25
Acebutolol HCI	200 mg.	Daily	Oral	New	2010-01-25
Acetic Acid 1/4 %	30cc	QWEEK	Other	New	2010-01-25

Medication Report