SEMRS: Secure Electronic Medical Records System

Ryan Kane and Ricky Orndorff

Department of Computer Science

Spring 2012

Project Background

- Mitchell's Plain Community Health Center

- No general health insurance standard

- Average annual income (2005) = 75,000 ZAR or 10,000 USD

- Majority of population has 7th grade education

- 20% of the population diagnosed with HIV/AIDS

Problem Statement

- Loss/Damage to patient files

- Delay or hinder treatment progress

- Confidentiality of patient files

- Data integrity

Motivation

- Improved electronic medical records management system

  - Secure

  - Easy to use

- Proposed Solution

  - Enforce patient confidentiality

  - Ensure data integrity

  - HIPAA

Background on HIPAA Security Rules

- Access Control

- Audit Controls

- Integrity Controls

- Transmission Security

|	ZEPRS	OpenEMR	THIRRA
Year Introduced	2001	2001	2007
Pros	• Offline mode • Role based access control	• Most mature • Insurance and Billing support	• Mobile EHR • Bio-surveillance mode • Modularity
Cons	• Lacks security	• Complexity • Lacks encryption	• Lacks security

Proposed Implementation

- Simpler than OpenEMR

  - Removed features

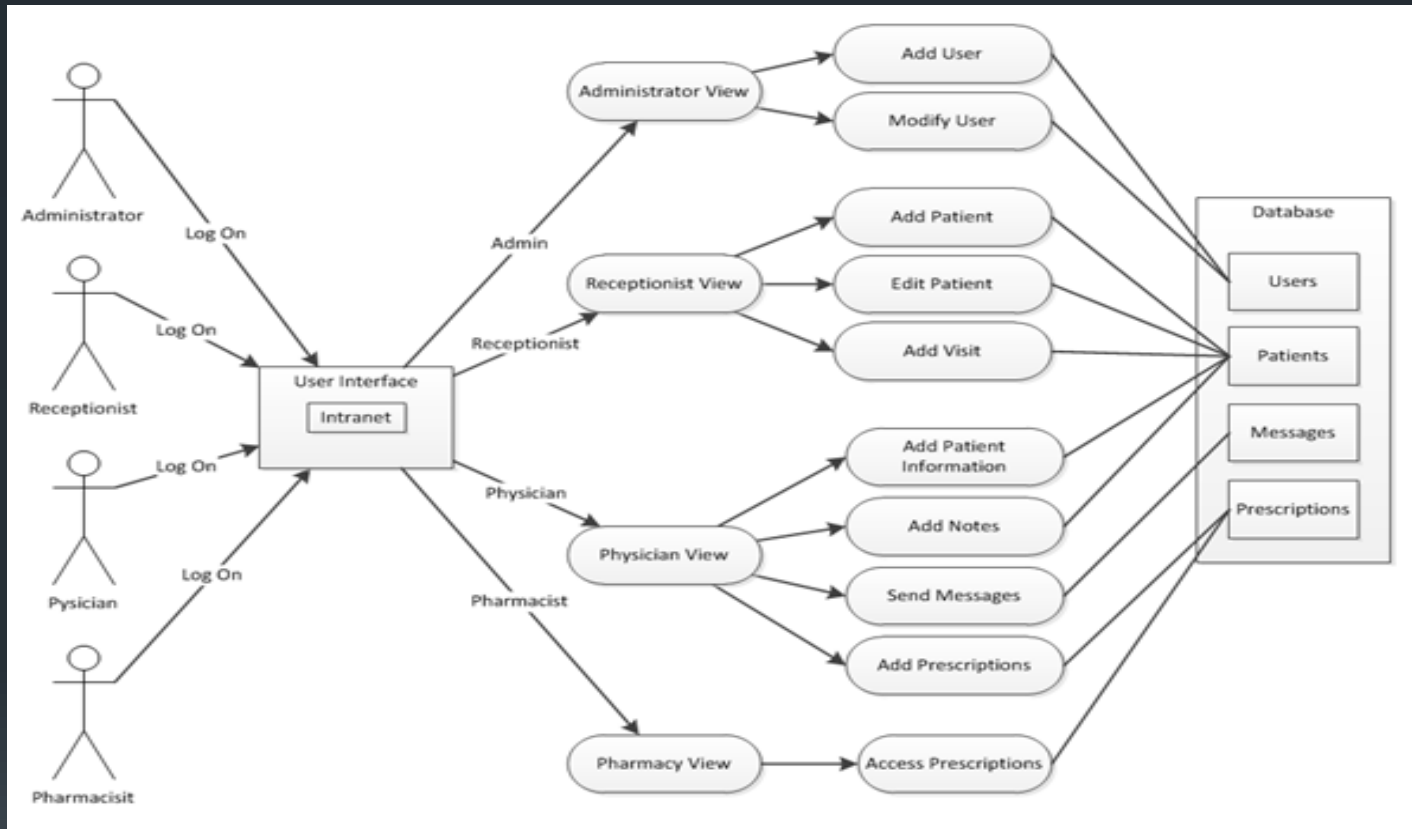- Onsite Access through intranet (LAN)

- SSL Encryption

System Architecture Diagram
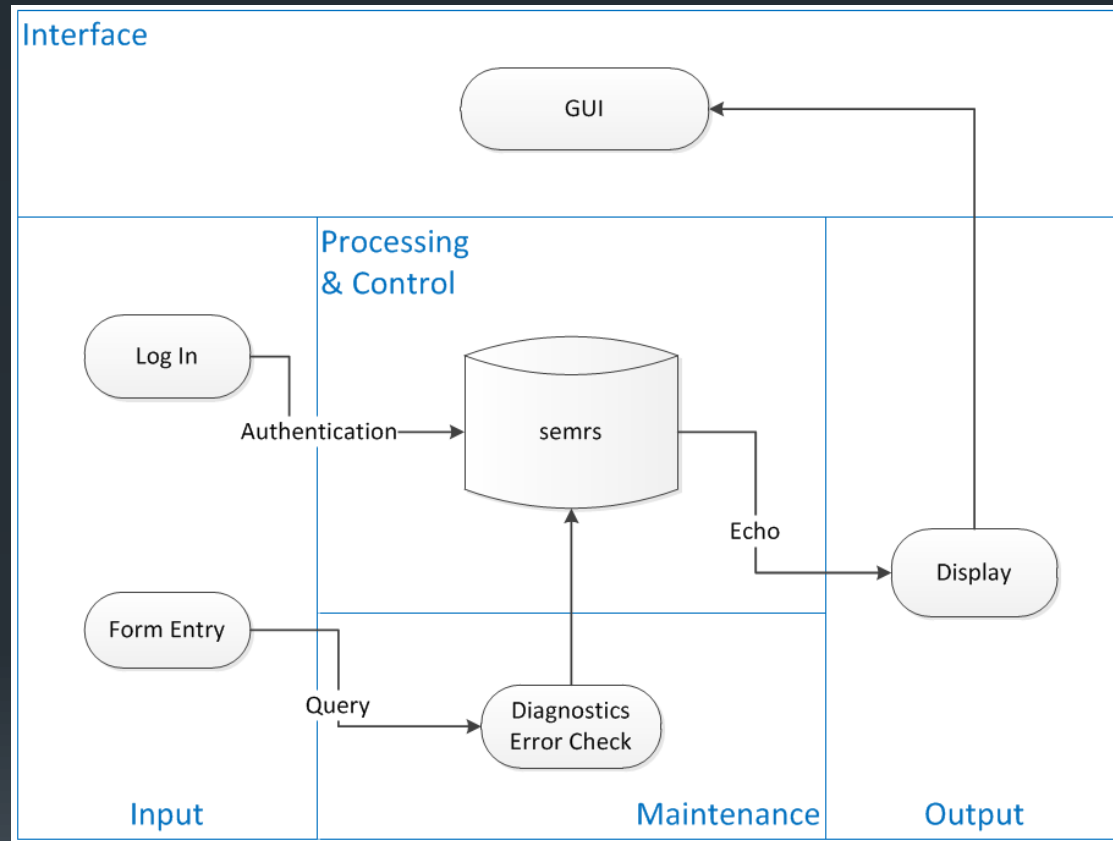
This system context diagram depicts the basic input, output, and processing of the SEMRS system.

Use Case Diagram

This use case diagram depicts the different user types and what they have access to within the SEMRS system.

Summary

- Portability of a streamlined secure system

  - SSL Encryption

  - Patients treatment will no longer be restarted

  - Uphold Confidentiality and data integrity

  - Automatic log off

- Access controls

  - user groups

  - audit trail

Possible Future Work

- Ability to upload existing multimodal hardcopy files

- Prescriptions:

  - Add

  - Update

  - Control dispensing

- Greater domain portability