SecureMed User Guide

How to Use the Healthcare Cybersecurity & HIPAA Compliance Platform

Version: 1.0

Release Date: Fall 2025

Project: SecureMed Healthcare Security & HIPAA Compliance Platform

Institution: Florida International University, Knight Foundation School of Computing and Information Sciences

Course: CIS 4914 - Cybersecurity Capstone Project II

Table of Contents

1.0 Introduction

Welcome to SecureMed, a comprehensive healthcare security and HIPAA compliance management system. This guide provides step-by-step instructions for using the SecureMed platform, including:

- **Navigation**: How to move through the system interface
- **User Roles**: Admin vs. Nurse permissions and responsibilities
- **Patient Management**: Adding, editing, and viewing patient records
- **Task Management**: Completing PHI transmission assignments
- **Training Modules**: Interactive HIPAA compliance training
- **Threat Detection**: Monitoring security vulnerabilities via the EDR panel
- **Audit Review**: Accessing complete activity logs for compliance

What is SecureMed?

SecureMed unifies five critical healthcare security capabilities:

1. **Encrypted PHI Management** - All sensitive patient data protected with Fernet AES-128 encryption
2. **Real-Time Threat Detection (EDR)** - Continuous monitoring of security vulnerabilities

3. **Interactive HIPAA Training** - 3 modules with 9 scenarios and compliance scoring
4. **Audit Trail Automation** - Complete logging of all system activities (100% completeness)
5. **Breach Simulation Workflows** - 5 comprehensive incident response playbooks

This system is designed for healthcare organizations (clinics, small hospitals) that need enterprise-grade security without enterprise-level costs.

2.0 Logging In

2.1 Access the Login Page

1. **Ensure Flask is Running**
    - See Installation Guide if you haven't started the application
    - Terminal should show: `Running on http://127.0.0.1:5000`
2. **Open Your Web Browser**
    - Chrome, Firefox, Safari, or Edge (recommended: Chrome)
    - Any modern browser from 2020 onwards
3. **Navigate to the Login Page**

```
http://127.0.0.1:5000/login
```

4. **Expected Screen**
    - SecureMed logo and branding (top)
    - "Login to SecureMed" heading
    - Username field
    - Password field
    - "Login" button

2.2 Default Credentials

Use one of the following accounts to log in:

Admin Account (Full System Access)

Field	Value
Role	Administrator
Username	`admin`
Password	`Admin123!`
Access	Dashboard, User Management, EDR Panel, Audit Logs, Compliance Reports

Use this account to:

- Generate demo data with Quick Setup
- Simulate breach incidents
- View system-wide violations
- Generate compliance reports
- Reset the entire system
- Review audit logs of all users

Demo Nurse Accounts (Limited Access)

Username	Password	Purpose	Access Level
`stefan`	`Stefan123!`	Patient management, training	Nurse
`ana`	`Ana123!`	Patient access, assignments	Nurse
`jordan`	`Jordan123!`	Dashboard, training completion	Nurse
`jeremiah`	`Jeremiah123!`	Testing account	Nurse
`mumin`	`Mumin123!`	Testing account	Nurse

Use these accounts to:

- View assigned patients
- Complete HIPAA training modules
- Submit task assignments
- View personal compliance scores
- View audit trail (own actions only)

2.3 Login Steps

1. **Enter Username**
    - Click the "Username" field
    - Type your username (e.g., `admin`)
2. **Enter Password**
    - Click the "Password" field
    - Type your password (e.g., `Admin123!`)
    - Characters will show as dots for security
3. **Click Login**
    - Click the blue "Login" button
    - System authenticates your credentials
4. **Expected Outcomes**

    Success:

- You're redirected to your dashboard
- Your role name appears in the top-right corner
- Navigation menu is visible

Failure:

- Red error message: "Invalid username or password"
- Try again with correct credentials

2.4 Troubleshooting Login Issues

Issue: "Invalid username or password" repeatedly

- Solution: Double-check username spelling and capitalization (case-sensitive)
- Solution: Verify password is correct (check Caps Lock)

Issue: Page doesn't load or shows "Connection refused"

- Solution: Verify Flask is running in terminal (`python webapp.py`)
- Solution: Check URL is correct: `http://127.0.0.1:5000/login` (not `https`)

Issue: "Page not found" (404 error)

- Solution: Ensure Flask is running
- Solution: Clear browser cache (Ctrl+Shift+Delete / Cmd+Shift+Delete)

3.0 User Roles & Dashboard Overview

SecureMed has two primary user roles with different permissions and dashboards.

3.1 Nurse Dashboard (Standard User Role)

Who uses this: Nurses, medical assistants, front desk staff

Permissions:

- □ View assigned patients
- □ Edit patient contact info (email, phone, address only)
- □ Complete HIPAA training modules
- □ Submit task assignments
- □ View personal compliance score
- □ Cannot view other users' data
- □ Cannot create violations
- □ Cannot reset system

Dashboard Components (visible after login as nurse):

1. Dashboard Header

- Your username (top right)
- "Welcome, [Your Name]" greeting
- Logout link
- Session timer (2 minutes before automatic logout)

2. Navigation Menu

- **Patients** - View and edit patient records
- **Assignments** - Complete task assignments
- **Training** - Access HIPAA training modules
- **Compliance Score** - View your personal score (0-100%)
- **Audit Trail** - View your own activity log

3. Quick Stats Widget

- Total patients you have access to
- Pending assignments
- Your current compliance score
- Training modules completed

4. Main Content Area

Displays the section you've selected (Patients, Training, etc.)

5. Session Timer

- **Description**: Countdown to automatic logout
- **Visual**: Warning at 90 seconds remaining
- **Duration**: 2 minutes total (configurable, 15-30 minutes in production)
- **Purpose**: HIPAA §164.312(a)(2)(iii) - Automatic logoff

Example Workflow (Nurse):

```
Login as "stefan"
  ↓
View Patients (see 5 assigned patients)
  ↓
Click "Edit" on patient "John Doe"
  ↓
Update phone number and address
  ↓
Click "Save" (audit log created)
  ↓
Go to Assignments
  ↓
Complete task: "Send secure message to Dr. Sarah Chen for patient John Doe"
  ↓
Go to Training
  ↓
Complete Module 1: PHI Protection (3 questions, score 67%)
  ↓
View Compliance Score (33% overall)
  ↓
Logout
```

3.2 Admin Dashboard

Who uses this: System administrators, compliance officers, security teams

Permissions:

- □ View all patients
- □ View all users and their activity
- □ Review all violations (system-wide)
- □ Access EDR security panel
- □ Generate compliance reports
- □ Simulate breach incidents
- □ View complete audit logs
- □ Reset system/demo data
- □ User management (create, disable accounts)

Dashboard Components (visible after login as admin):

1. Admin Header

- "SecureMed Admin Dashboard" heading
- Current timestamp

- Your username + "Admin" badge
- Logout link

2. Key Metrics Widget

Shows critical system information:

- **Total Patients**: Number of patient records in system
- **Pending Tasks**: Unsubmitted task assignments
- **Active Violations**: Open HIPAA/security violations
- **System Status**: Green (healthy) or Red (issues)

3. Quick Action Buttons

- ⚡ **Quick Setup** - Auto-generate demo patients, tasks, violations
- □ **Simulate Breach** - Run one of 5 breach scenarios
- □ **Generate Report** - Create HIPAA compliance PDF
- □ **Demo Reset** - Clear all data (keeps user accounts)

4. Navigation Menu (Admin-specific)

- **Dashboard** - Overview and metrics
- **Patients** - View/manage all patients
- **Users** - Manage staff accounts
- **Violations** - Review all violations
- **EDR Panel** - Threat detection and monitoring
- **Audit Trail** - Complete system activity log
- **Reports** - Generate compliance documents

5. Main Content Area

Displays detailed information for selected section

6. EDR Panel (Real-Time Threat Monitoring)

Located on admin dashboard or separate tab:

- **System Hardening Status** (5 controls):
    1. HTTPS/TLS 1.3 security
    2. AES-128 encryption deployment
    3. API authentication strength
    4. SQL injection protection
    5. Dependency security updates
- **Vulnerabilities List**:
    - Type (HTTPS missing, weak auth, etc.)

    - Severity (Critical, High, Medium, Low)
    - Status (Open, Resolved)
    - Remediation button

- **Violations Summary**:

    - Organizational violations (system-level)
    - Individual nurse violations (training errors, wrong task submissions)
    - Filter by user, type, or date

Example Workflow (Admin):

```
Login as "admin"
  ↓
Click "⚡ Quick Setup"
  ↓
System generates: 15 patients, 10 tasks, 3 violations, 5 vulnerabilities
  ↓
Go to EDR Panel
  ↓
Review "Missing HTTPS/TLS" vulnerability (Critical)
  ↓
Click "Mark Resolved" (logs remediation action)
  ↓
Go to Violations
  ↓
See "stefan" submitted wrong task assignment (violation)
  ↓
Review "Audit Trail"
  ↓
See all logins, patient edits, training completions
  ↓
Click "Generate Report"
  ↓
PDF downloads with violations, audit summary, compliance score
  ↓
Logout
```

4.0 Performing Common Actions

4.1 Using the "Quick Setup" Tool (Admin Only)

Quick Setup auto-generates realistic demo data to test system functionality without manual entry.

Prerequisites:

- Must be logged in as **admin**
- Optional: Run "Demo Reset" first if you want a clean slate

Steps:

1. **Log in as Admin**

```
Username: admin
Password: Admin123!
```

2. **Navigate to Dashboard**
    - You should be on the admin dashboard by default
3. **Locate Quick Setup Button**
    - Look for the blue button with ⚡ icon
    - Text reads "⚡ Quick Setup"
    - Located in the top section of dashboard
4. **Click Quick Setup**
    - Button triggers data generation
    - Wait 3-5 seconds for completion
5. **Verify Data Generated**
    - Check dashboard metrics update
    - Go to **Patients** - should see 10-15 records
    - Go to **Violations** - should see 2-3 violations
    - Go to **EDR Panel** - should see 5+ vulnerabilities

What Gets Generated:

Item	Count	Examples
Patients	10-15	John Doe, Jane Smith, etc.
Tasks	5-10	"Send secure message to Dr. Chen"
Violations	2-3	Training failures, wrong task submissions
Vulnerabilities	5+	HTTPS missing, weak authentication
Training Results	Varies	Some users complete modules, others don't

Use Cases:

- **First-time testing**: Populate system with data
- **Demo preparation**: Get realistic scenario for presentation
- **Training staff**: Show how system works with actual data

- **Benchmark testing**: Performance test with sample workload

---

4.2 Managing Patients (Admin + Nurse)

4.2.1 Viewing Patients

Step 1: Navigate to Patients

- Click "Patients" in the left navigation menu
- Table appears with all accessible patients

Step 2: Understand the Patient Table

Column	Description	Editable	Encrypted
MRN	Medical Record Number (unique ID)	□ No	□ No
First Name	Patient's first name	□ No	□ No
Last Name	Patient's last name	□ No	□ No
DOB	Date of birth (MM/DD/YYYY)	□ No	□ No
Email	Email address	□ **Yes**	□ No
Phone	Phone number	□ **Yes**	□ No
Address	Street address	□ **Yes**	□ No
SSN	Social Security Number	□ No	□ **Yes**
Actions	Edit/Delete buttons	-	-

Permissions:

- **Admins**: See all patients in the system
- **Nurses**: See only patients assigned to them

Step 3: Search/Filter Patients (if available)

- Enter patient name or MRN in search field
- Results filter in real-time
- Click column header to sort

4.2.2 Editing Patients (Contact Information Only)

IMPORTANT: For HIPAA compliance, only contact information can be edited. Critical identifiers are protected.

Editable Fields □:

- Email address
- Phone number
- Street address

Protected Fields □ (Cannot Edit):

- Medical Record Number (MRN)
- First Name
- Last Name
- Date of Birth
- SSN (encrypted, hidden for security)

Why These Protections?

- **HIPAA §164.312(a)(2)(iv)**: Encryption and access controls for critical identifiers
- **Data Integrity**: Prevents accidental modification of key identifiers
- **Audit Trail**: All edits logged with before/after values

How to Edit Patient Contact Information:

Step 1: Locate Patient

- Find patient in the patient list
- Admins: See all patients
- Nurses: See only assigned patients

Step 2: Click Edit Button

- Look for pencil icon (✏) or "Edit" button
- Click to open edit form

Step 3: Edit Modal Opens Modal displays:

- Patient name (read-only for context)
- MRN (read-only for reference)
- Email field (editable) - shows current value
- Phone field (editable) - shows current value
- Address field (editable) - shows current value
- Note: "Protected fields marked read-only per HIPAA §164.312(a)(2)(iv)"

Step 4: Make Changes

- Click each field you want to update
- Type new value
- Old value stays visible in placeholder

Example:

```
Patient: John Doe (MRN: MRN2871)

Before:
  Email: john.doe@old.com
  Phone: (555) 123-4567
  Address: 123 Main St, Miami, FL

After (edited):
  Email: john.doe@new.com
  Phone: (555) 987-6543
  Address: 456 Oak Ave, Miami, FL
```

Step 5: Click Save

- Button text: "Save Changes" or "Update Patient"
- Green success message appears: "Patient updated successfully"
- Modal closes, table refreshes

Step 6: Verify in Audit Trail

- Go to **Audit Trail** section
- Search for your username
- Find entry: `PATIENT_INFO_UPDATED`
- Details show: `phone: '555-123-4567' → '555-987-6543'`
- Timestamp and your username logged

Audit Trail Entry Example:

```
User: stefan
Action: PATIENT_INFO_UPDATED
Timestamp: 2025-12-03 14:25:33
Patient: John Doe (MRN2871)
Changes:
  - phone: '555-0101' → '555-0199'
  - address: '123 Main St' → '456 Oak Ave'
```

4.2.3 Adding New Patients (Admin Only)

Permissions: Admins can add patients; nurses can only edit contact info.

Steps:

1. **Go to Patients Section**

- Click "Patients" in navigation

2. **Click "+ Add Patient" Button**

   - Located at top of patient list
   - Opens patient creation form

3. **Fill in Required Fields** (marked with *)

Field	Format	Example	Notes
First Name *	Text	John	Required
Last Name *	Text	Doe	Required
Date of Birth *	MM/DD/YYYY	01/15/1980	Required
SSN *	XXX-XX-XXXX	123-45-6789	Encrypted after save
Email	email@domain.com	john@example.com	Optional
Phone	(XXX) XXX-XXXX	(555) 123-4567	Optional
Address	Street, City, ST ZIP	123 Main St, Miami, FL 33139	Optional

4. **Click Save**

   - System generates unique MRN automatically
   - SSN encrypted with Fernet AES-128
   - Confirmation message appears

5. **Verify Creation**

   - Patient appears in patient list
   - Audit log created: `PATIENT_CREATED`

4.3 Completing Assigned Tasks (Nurse)

Tasks are HIPAA compliance exercises where nurses must correctly identify recipients before transmitting PHI.

4.3.1 Understanding Task Types

SecureMed includes 5 types of PHI transmission tasks:

Task Type	Description	Real-World Example	Validation
Fax	Send patient records via fax to approved locations	Fax to radiology department	Must select correct fax number from directory
Email	Email PHI via internal secure email only	Email lab results to doctor	Must choose internal secure email, not personal
Hospital Transfer	Transfer patient to approved facility	Admit patient to hospital	Must verify facility is approved
Courier Service	Send records via approved courier	Overnight courier to specialist	Must select approved courier company

Task Type	Description	Real-World Example	Validation
Secure Messaging	Send via healthcare secure messaging	Secure message to patient portal	Must select approved messaging platform

4.3.2 The Directory System

What is the Directory?

- Pre-approved list of recipients for PHI transmission
- Contains names and contact information
- Prevents accidental transmission to unauthorized recipients
- Enforces HIPAA §164.502(b) "Minimum Necessary" principle

Directory Contents (Sample):

```
Approved Fax Destinations:
  - Radiology Dept: (305) 555-0120
  - Lab Services: (305) 555-0121
  - Cardiology: (305) 555-0122

Approved Email:
  - Dr. Sarah Chen: sarah.chen@hospital.internal
  - Dr. James Wilson: james.wilson@hospital.internal

Approved Facilities:
  - Jackson Memorial Hospital
  - South Shore Hospital
  - Primary Care Clinic

Approved Couriers:
  - FedEx Healthcare
  - UPS Medical Express

Approved Messaging:
  - Patient Portal SecureMessaging
  - Epic MyChart
```

4.3.3 How to Complete a Task

Step 1: Navigate to Assignments

- Click "Assignments" in left menu
- List of pending tasks appears

Step 2: Read the Task Description Task description format:

```
"Send secure message to 'Dr. Sarah Chen' for patient MRN2871"
```

Important:

- Task shows recipient name and patient MRN
- Task does NOT show contact details (you must look them up)
- This forces verification in the Directory

Step 3: Open the Directory

- Click "View Directory" link (usually bottom of task)
- Directory opens in new section or modal
- Shows all approved recipients

Step 4: Find the Correct Recipient

- Search directory for "Dr. Sarah Chen"
- Verify it matches the task requirement
- Find the correct code/contact (e.g., "SM-1847")

Step 5: Enter the Code

- Task form has input field for answer
- Enter the code exactly as shown in directory
- Example: "SM-1847" (case-insensitive)

Step 6: Submit Task

- Click "Submit" or "Complete Task" button
- System validates your answer

Step 7: Verify Outcome

If Correct □:

- Green success message: "Task completed successfully"
- Audit log created: `TASK_COMPLETED`
- Task removed from pending list

If Incorrect □:

- Red error message: "Incorrect recipient selected"
- **HIPAA Violation Created**: Logged to system
- **Compliance Score Reduced**: Training score penalty
- Task stays pending to retry

Example Task Workflow:

```
Task: "Send secure message to 'Dr. Sarah Chen' for patient MRN2871"

You see:
  - Recipient: Dr. Sarah Chen
  - Patient: MRN2871
  - Input field: "Enter approved contact code"

You click "View Directory"

Directory shows:
  Approved Secure Messaging:
    1. Dr. Sarah Chen: SM-1847 ✓ APPROVED
    2. Dr. James Wilson: SM-1848
    3. Patient Portal: SM-1849

You enter: "SM-1847"
You click: "Submit"

System checks: ✓ Correct (matches Dr. Sarah Chen)

Result:  Task completed, compliance maintained
```

Another Example (Wrong Answer):

```
Task: "Fax patient records to 'Cardiology Department'"

You see:
  - Recipient: Cardiology Department
  - Input field for fax number

You click "View Directory"

Directory shows:
  Approved Fax:
    - Radiology: (305) 555-0120
    - Cardiology: (305) 555-0122  ← Correct
    - Lab Services: (305) 555-0121

You mistakenly enter: "(305) 555-0120"  ← Wrong (Radiology)
You click: "Submit"

System checks: ✗ Incorrect (that's Radiology, not Cardiology)

Result:  HIPAA violation created, score reduced
        Task remains pending for you to retry
```

4.4 Training Modules (Nurse)

SecureMed includes 3 interactive HIPAA training modules covering the most critical areas of healthcare compliance. Training is mandatory for new hires and annually for all staff.

4.4.1 Training Module Overview

Module	Focus Area	HIPAA Section	Scenarios	Time
Module 1	PHI Protection & Privacy	§164.502 (Privacy Rule)	3 scenarios	5-8 min
Module 2	Secure Communication	§164.312(e) (Transmission Security)	3 scenarios	5-8 min
Module 3	Breach Prevention & Response	§164.400-414 (Breach Notification)	3 scenarios	5-8 min
Total	-	-	9 scenarios	15-24 min

4.4.2 Module 1: PHI Protection & Privacy

Learning Objectives:

- Understand what constitutes Protected Health Information (PHI)

- Know the minimum necessary standard
- Understand patient rights

Scenarios (3 questions):

Scenario 1: "A patient calls and asks for another patient's test results. What do you do?"

- A. Give them the results (patient is asking) □
- B. Verify the caller's identity first □
- C. Tell them to call back later □

Scenario 2: "You notice a coworker left a chart on a public desk. What do you do?"

- A. Leave it there, not your problem □
- B. Move it to secure location immediately □
- C. Tell the coworker later □

Scenario 3: "A patient requests a copy of their medical record. What's the requirement?"

- A. You can deny the request □
- B. Provide it within 30 days □
- C. They must pay full staff time to retrieve it □

Scoring:

- Correct answer: +20 points
- Incorrect answer: 0 points
- Module score: (correct / 3) × 100
- Example: 2 correct = 66.67%

4.4.3 Module 2: Secure Communication

Learning Objectives:

- Know approved channels for PHI transmission
- Understand encryption and secure email
- Identify risks of unsecured communication

Key Concept: "STOP Framework"

- **S**ecure method (encrypted email, secure portal)
- **T**rust the recipient (verify identity)
- **O**nly necessary information (minimum standard)
- **P**rotect the message (use approved systems)

Scenarios (3 questions):

Scenario 1: "A doctor requests lab results via personal Gmail. What do you do?"

- A. Send via Gmail (convenient) □
- B. Refuse and direct them to secure system □
- C. Send in plain text with password □

Scenario 2: "You're at a clinic and a visitor asks about a patient in the waiting room. What happens?"

- A. Tell them the patient is here □
- B. Verify visitor has legitimate business need first □
- C. That's public information, it's okay □

Scenario 3: "What is the safest way to transmit patient SSN?"

- A. Call the number verbally □
- B. Email in plain text □
- C. Encrypted secure messaging only □

4.4.4 Module 3: Breach Prevention & Response

Learning Objectives:

- Recognize breach scenarios
- Know incident response procedures
- Understand notification requirements

Key Concept: "60-Day Rule"

- Breaches must be reported to HHS within **60 days**
- Patients must be notified within 60 days
- Media notification required if 500+ people affected

Scenarios (3 questions):

Scenario 1: "You discover an unencrypted laptop with patient data was stolen. Is this a reportable breach?"

- A. No, it's just one laptop □
- B. Yes, unencrypted = reportable (no safe harbor) □
- C. Only if more than 100 patients affected □

Scenario 2: "An administrator notices a database is publicly accessible. First action?"

- A. Take the database offline immediately □
- B. Notify the database company first □
- C. Continue investigating before action □

Scenario 3: "How quickly must you notify affected patients after discovering a breach?"

- A. As soon as possible, within 60 days □
- B. Within 1 year (time for investigation) □
- C. Within 30 days □

4.4.5 How to Complete Training

Step 1: Navigate to Training

- Click "Training" or "Training Simulator" in left menu
- Module selection page appears

Step 2: Select a Module

- Click on Module 1, 2, or 3
- Module content loads
- Read educational material (2-3 minutes)

Step 3: Review Scenario

- Scenario displays on screen
- Situation described clearly
- 3-4 multiple choice options

Step 4: Select Your Answer

- Click the radio button for your choice
- Selected option highlights

Step 5: Submit Answer

- Click "Next" or "Submit Answer" button
- System validates answer immediately

Step 6: See Feedback

- Correct answer: Green checkmark + positive feedback
- Incorrect answer: Red X + explanation of correct response
- Point value displayed (+20 or 0)

Step 7: Continue to Next Scenario

- Same module shows next scenario (if available)
- Or move to next module

Step 8: View Final Score After completing all 9 scenarios across 3 modules:

Score Calculation:

```
Total correct answers: ? / 9
Compliance Score = (correct / 9) × 100%

Examples:
- 9 correct = 100% (Excellent - green badge)
- 6 correct = 67% (Passing - yellow badge)
- 3 correct = 33% (Needs improvement - red badge)
- 0 correct = 0% (Training required - red badge)
```

Step 9: View Compliance Scorecard

- Click "Compliance Score" or "My Score"
- Personal dashboard shows:
    - Overall score (0-100%)
    - Modules completed ✓ or pending ◯
    - Correct/incorrect breakdown
    - Status badge (Excellent, Needs Improvement, Training Required)

Step 10: Performance Review

- **80-100%**: Excellent (Green badge) - Compliant with HIPAA
- **50-79%**: Needs Improvement (Yellow badge) - Requires retraining
- **0-49%**: Training Required (Red badge) - Mandatory retraining

---

4.5 EDR — Threat Detection Panel (Admin Only)

The EDR (Endpoint Detection & Response) panel provides real-time monitoring of security vulnerabilities, HIPAA violations, and system health.

4.5.1 Accessing the EDR Panel

Who can access: Admins only

Steps:

1. Log in as **admin**
2. Click "EDR Panel" or "Threat Detection" in navigation
3. Panel loads with real-time threat data

4.5.2 EDR Panel Layout

The EDR panel displays **4 main sections**:

Section 1: System Hardening Status

Shows the 5 core security controls:

Control	Status	Icon	Action
HTTPS/TLS 1.3	□ Configured	✓	Enabled
AES-128 Encryption	□ Configured	✓	100% coverage
API Authentication	□ Configured	✓	JWT enforced
SQL Injection Protection	□ Configured	✓	Parameterized queries
Dependency Updates	□ Review Needed	⚠	Update available

Meaning:

- □ Green = Control is properly implemented
- □ Yellow = Review needed or minor issue
- □ Red = Critical issue requiring immediate action

Section 2: Active Vulnerabilities

Lists detected security weaknesses:

Example Vulnerabilities:

```
Vulnerability 1:
  Type: HTTPS Not Enabled
  Severity: CRITICAL 
  Description: Unencrypted connections allow man-in-the-middle attacks
  Affected Systems: Web server
  Status: Open
  [Mark Resolved] button

Vulnerability 2:
  Type: Weak Password Hashing
  Severity: HIGH 
  Description: Consider migrating to bcrypt
  Affected Systems: User authentication
  Status: Open
  [Mark Resolved] button

Vulnerability 3:
  Type: Missing Rate Limiting
  Severity: MEDIUM 
  Description: Brute force attacks not prevented
  Affected Systems: Login endpoint
  Status: Resolved ✓
  [Reopen] button
```

How to Remediate:

1. Read vulnerability description
2. Click "Mark Resolved" if you've fixed it
3. System logs remediation action to audit trail
4. Vulnerability status changes to "Resolved"

Section 3: System Violations

Organizational Violations (System-level, admins see):

- "Missing Risk Assessment" - HIPAA §164.308(a)(1)
- "No Contingency Plan" - HIPAA §164.308(a)(7)
- "Weak Authentication Controls" - HIPAA §164.312(a)(2)(i)

Individual Nurse Violations (Personal, filtered by user):

- "Training Module Failed" - Scored <80%
- "Wrong Task Submission" - Selected incorrect recipient
- "Unauthorized Access Attempt" - Tried to view unassigned patient

4.5.3 Threat Monitoring Example

Scenario: Admin logs in and sees EDR panel

```
System Status:  WARNING (1 critical vulnerability)

System Hardening Status:
  ✓ HTTPS/TLS 1.3: Configured
  ✓ AES-128 Encryption: Configured
  ✓ API Authentication: Configured
  ✓ SQL Injection Protection: Configured
  ⚠ Dependency Updates: Review needed

Active Vulnerabilities: 3
  CRITICAL: HTTPS Not Enabled (Web server)
  HIGH: Weak Password Hashing (Authentication)
  MEDIUM: Missing Rate Limiting (Login endpoint)

Violations: 5
  Organizational:
    - "No Contingency Plan" (Open)
  Individual:
    - stefan: "Wrong task selection" (3 instances)
    - ana: "Training score 45%" (Needs retraining)

Recommended Actions:
  1. Enable HTTPS/TLS immediately (CRITICAL)
  2. Review password hashing algorithm
  3. Implement Flask-Limiter for rate limiting
  4. Retrain ana on Module 1
```

Admin Response:

1. Click "Mark Resolved" on HTTPS vulnerability (after fixing)
2. System logs: "CRITICAL_ISSUE_RESOLVED - HTTPS/TLS enabled"
3. Go to Training section and flag ana for retraining
4. Generate compliance report showing remediation

4.6 Viewing Audit Logs (Admin)

The Audit Trail is the complete activity log of all system actions. HIPAA §164.312(b) requires maintaining a complete audit trail.

4.6.1 What Gets Logged

SecureMed automatically logs **every significant action**:

Action	User	Timestamp	Details
LOGIN	stefan	2025-12-03 14:20:00	From IP 127.0.0.1
LOGOUT	stefan	2025-12-03 14:25:00	Session ended normally
PATIENT_ACCESSED	ana	2025-12-03 14:25:30	Viewed MRN2871 record
PATIENT_INFO_UPDATED	stefan	2025-12-03 14:26:00	Changed phone for MRN2871
PATIENT_CREATED	admin	2025-12-03 14:27:00	New patient: John Doe
TASK_COMPLETED	ana	2025-12-03 14:28:00	Correct submission
TASK_FAILED	jordan	2025-12-03 14:29:00	Wrong recipient selected
TRAINING_ANSWER_SUBMITTED	stefan	2025-12-03 14:30:00	Module 1, Scenario 2, Correct
VIOLATION_CREATED	system	2025-12-03 14:31:00	jordan scored 45% on Module 1
REPORT_GENERATED	admin	2025-12-03 14:32:00	HIPAA compliance report
BREACH_SIMULATED	admin	2025-12-03 14:33:00	Ransomware scenario

4.6.2 How to Access Audit Trail

Step 1: Navigate to Audit Trail

- Click "Audit Trail" in left navigation menu
- Audit log table appears

Step 2: Understand the Columns

Column	Content	Example
Timestamp	Date and time of action	2025-12-03 14:25:33
Username	User who performed action	stefan
Action	Type of action	PATIENT_INFO_UPDATED
Description	Human-readable summary	Updated patient contact info
Details	Technical details (JSON)	`{"phone": "555-0101 → 555-0199"}`
IP Address	Network location	127.0.0.1

Step 3: Filter/Search Audit Logs

By Date:

- Click date picker
- Select date range (e.g., "Last 7 days")

- Table refreshes to show matching entries

By User:

- Click "Filter by User" dropdown
- Select username (e.g., "stefan")
- Shows only actions by that user

By Action Type:

- Click "Filter by Action" dropdown
- Select action (e.g., "PATIENT_ACCESSED")
- Shows only that type of action

By Patient:

- Enter patient name or MRN
- Shows all actions related to that patient

Step 4: View Detailed Logs

Click on any row to expand and see:

- Complete action details
- Before/after values (for edits)
- Full timestamp
- User information
- IP address and session info

Example: Patient Edit Log

```
User: stefan
Action: PATIENT_INFO_UPDATED
Timestamp: 2025-12-03 14:26:15
Patient: John Doe (MRN2871)
Details:
  - phone: '555-0101' → '555-0199'
  - address: '123 Main St' → '456 Oak Ave'
IP Address: 127.0.0.1
```

Example: Training Log

```
User: ana
Action: TRAINING_ANSWER_SUBMITTED
Timestamp: 2025-12-03 14:28:42
Module: 1 - PHI Protection & Privacy
Scenario: 2 - Coworker leaves chart on public desk
Answer: B (Move to secure location immediately)
Result: Correct ✓
Points: +20
IP Address: 127.0.0.1
```

4.6.3 Compliance Use Cases

Use Case 1: Investigating Unauthorized Access

```
Admin receives HIPAA audit request: "Who accessed patient MRN2871?"

Steps:
1. Filter by Patient: "MRN2871"
2. Filter by Action: "PATIENT_ACCESSED"
3. See entries:
   - stefan: 2025-12-01 14:20:00 ✓ (Assigned nurse)
   - ana: 2025-12-01 14:22:00 ✓ (Assigned nurse)
   - jeremiah: 2025-12-01 16:45:00 □ (Not assigned! Violation)
4. Click on jeremiah's entry to see full details
5. Document violation and report to compliance officer
```

Use Case 2: Proving Staff Training Completion

```
Admin needs to prove "stefan" completed HIPAA training for auditor.

Steps:
1. Filter by User: "stefan"
2. Filter by Action: "TRAINING_ANSWER_SUBMITTED"
3. See all training submissions with timestamps and scores
4. Print audit trail as evidence
5. Attach to audit response: "Staff training completed and logged"
```

Use Case 3: Tracking Patient Data Edits

```
Patient questions: "When was my phone number changed?"

Steps:
1. Filter by Patient: "John Doe" or "MRN2871"
2. Filter by Action: "PATIENT_INFO_UPDATED"
3. Find entry: "2025-12-03 14:26:15 by stefan"
4. Shows: "phone: '555-0101' → '555-0199'"
5. Respond to patient: "Updated by staff on 12/03 at 2:26 PM"
```

5.0 Security Features Users Must Understand

5.1 Automatic Session Timeout

What it is: User automatically logged out after period of inactivity (demo: 2 minutes, production: 15-30 min)

Why it exists: HIPAA §164.312(a)(2)(iii) - "Automatic Logoff"

How it works:

1. **Timer Starts**: When you log in
2. **Activity Resets**: Every mouse movement, keystroke, or page navigation resets timer
3. **90-Second Warning**: When 90 seconds remaining, warning popup appears:

```
⚠ Your session expires in 90 seconds
[Stay Logged In] [Logout Now]
```

4. **Logout at 2 Minutes**: If no action, auto-logout occurs
5. **User Sees**: Redirected to login page with message "Session expired"

Best Practices:

- □ Log out when leaving your desk
- □ Click "Stay Logged In" if you need more time
- □ Don't leave unattended computer with active session
- □ Don't share login credentials to bypass timeout

5.2 Encrypted Data Handling

What's encrypted: PHI (Protected Health Information)

Encryption method: Fernet (AES-128 CBC mode)

What gets encrypted:

- □ SSN (Social Security Number) - shown as "**-**-***" in table
- □ Medical diagnoses and notes
- □ Lab results and sensitive findings
- □ Patient name (needs to be searchable)
- □ Email and phone (needs contact capability)

Why encryption matters:

- HIPAA §164.312(a)(2)(iv) requires encryption
- If database is stolen, encrypted data is useless to attacker
- Protects against insider threats

User Impact:

- No visible impact - encryption happens automatically
- Can edit patient email/phone normally
- SSN appears masked: "123-45-****"

5.3 Role-Based Access Control (RBAC)

What it is: Different users can access different features based on their role

Two roles in SecureMed:

Admin Role □ Can:

- View all patients (no restrictions)
- View all violations and audit logs
- Access EDR security panel
- Generate reports
- Reset system
- Manage users

Nurse Role □ Can:

- View own assigned patients only
- Edit patient contact info (email, phone, address)
- Complete training and assignments
- View own compliance score
- View own audit trail entries

Nurse Role □ Cannot:

- View other nurses' patients

- View other nurses' violations
- Access EDR panel
- Generate compliance reports
- Reset system
- View admin-level logs

Why RBAC matters:

- HIPAA §164.312(a)(1) requires access controls
- Prevents unauthorized access to PHI
- Limits exposure if an account is compromised

6.0 Logging Out

6.1 Manual Logout

Steps:

1. Click your username (top right corner)
2. Select "Logout" or "Sign Out"
3. Redirected to login page
4. Message: "Logged out successfully"

What happens:

- Session ends immediately
- Audit log entry created: `LOGOUT`
- You must log in again to access the system

6.2 Automatic Logout

Triggered when:

- Inactivity exceeds 2 minutes (demo) or 15-30 minutes (production)
- You close browser without logging out
- System detects suspicious activity

Message on return:

```
Your session has expired.
Please log in again.
```

7.0 Troubleshooting Tips

7.1 "You Are Logged Out Unexpectedly"

Cause: Session timeout is intended behavior in demo mode (2 minutes)

Solution:

- Click "Stay Logged In" when 90-second warning appears
- Or log back in - process takes 10 seconds
- In production, timeout extended to 15-30 minutes

7.2 "Tasks Not Submitting Correctly"

Cause 1: Directory entry mismatch (exact text/code required)

Solution:

- Compare your answer to directory exactly
- Check for typos or wrong code
- Directory lookup is case-insensitive but must be exact
- Example: "SM-1847" correct, "SM-1848" incorrect

Cause 2: Wrong recipient selected

Solution:

- Verify you selected the RIGHT recipient from directory
- Read task description carefully
- Match the name exactly
- Use directory lookup feature

7.3 "EDR Panel Not Loading"

Cause: Flask backend not responding

Solution:

1. Check terminal where Flask is running
2. Verify you see: `Running on http://127.0.0.1:5000`
3. If Flask crashed, restart: `python webapp.py`
4. Refresh browser page (F5 or Cmd+R)
5. Try logging out and back in

7.4 "Can't Edit Patient Information"

Cause 1: You're trying to edit protected fields

Solution:

- Only email, phone, and address are editable
- MRN, name, DOB, SSN cannot be edited
- If need to change protected info, contact admin

Cause 2: You don't have permission

Solution:

- Only admins can add/delete patients
- Nurses can only edit contact info
- If you need different access, contact your admin

7.5 "My Compliance Score Dropped"

Cause: Training failure or wrong task submission

Solution:

- Review training module again
- Correct answers are worth +20 points
- Incorrect answers are 0 points
- Score = (correct / 9) × 100%
- To improve: Complete all 3 modules with high accuracy

7.6 "Can't Find a Patient"

Cause 1: Patient may not be assigned to you (nurse)

Solution:

- Nurses only see assigned patients
- Ask admin to assign patient to you
- Or ask admin to verify patient exists

Cause 2: Search is case-sensitive for some fields

Solution:

- Try different search variations
- Search by MRN instead of name

- Contact admin if patient seems missing

8.0 Best Practices

8.1 For Nurses

1. **Complete Training Fully**
    - □ Finish all 3 modules (9 scenarios)
    - □ Aim for 80%+ score (Excellent rating)
    - □ Review incorrect answers to learn
2. **Keep Patient Info Current**
    - □ Update email/phone if you know it changed
    - □ Use correct phone format: (XXX) XXX-XXXX
    - □ Verify address with patient when updating
3. **Use Directory for Task Validation**
    - □ Always verify recipient in directory BEFORE submitting task
    - □ Match task recipient exactly to directory entry
    - □ Use correct code (case-insensitive but exact)
4. **Don't Ignore Session Warning**
    - □ Click "Stay Logged In" if you need more time
    - □ Manually logout before leaving desk
    - □ Never share login credentials
5. **Report Issues**
    - □ Tell admin about bugs or unclear tasks
    - □ Report security concerns immediately
    - □ Ask for help with training scenarios

8.2 For Admins

1. **Use Quick Setup for Demos**
    - □ Generate sample data before presentations
    - □ Use Demo Reset between demos
    - □ Prepare realistic scenarios for training
2. **Monitor EDR Panel Regularly**
    - □ Check for new vulnerabilities

- □ Mark resolved vulnerabilities after fixing
- □ Review organizational violations

3. **Review Audit Logs**
   - □ Monthly or quarterly audit log review
   - □ Investigate unusual access patterns
   - □ Keep logs for 6 years (HIPAA requirement)
4. **Track Training Compliance**
   - □ Monitor which staff completed training
   - □ Ensure all staff score 80%+
   - □ Retrain staff with scores below 80%
5. **Generate Reports Regularly**
   - □ Monthly compliance reports
   - □ Share with compliance officer
   - □ Use for board/auditor presentations

9.0 Conclusion

This guide covers all essential procedures for using SecureMed:

- □ Logging in with appropriate credentials
- □ Understanding your role and dashboard
- □ Managing patient information securely
- □ Completing HIPAA compliance tasks
- □ Completing interactive training
- □ Monitoring threats (for admins)
- □ Reviewing audit trails
- □ Following security best practices

For additional help:

- **Installation issues**: See `INSTALLATION_GUIDE.md`
- **Feature details**: See `FEATURES.md`
- **Test suite**: See `TESTING.md`
- **System design**: See `FINAL_REPORT.md`

SecureMed is designed to make HIPAA compliance practical, measurable, and achievable for healthcare organizations of all sizes.

Document Information:

- **Version**: 1.0 - Final
- **Last Updated**: December 2025
- **Author**: SecureMed Team
- **Institution**: Florida International University
- **Course**: CIS 4914 - Cybersecurity Capstone Project II
- **Audience**: Nurses, Medical Assistants, System Administrators, Compliance Officers