SecureMed - How to Use Guide

Quick Reference for Team Presentations

Quick Start (5 Minutes)

1. Start the Application

```
# Navigate to project folder
cd Project_dev1

# Install required packages (first time only)
pip3 install -r requirements.txt

# Run the application
python3 webapp.py

# Open browser to: http://127.0.0.1:5000/login
```

2. Login

- **Admin**: `admin` / `Admin123!`
- **Team Members**: See LOGIN_CREDENTIALS.txt

Admin Dashboard Guide

Initial Setup (Before Demo)

Step 1: Quick Setup

- Click **"⚡ Quick Setup (Patients + Demo Data)"**
- Generates 5 patients, assignments, vulnerabilities, violations
- Takes ~3 seconds
- **Use this before every presentation!**

Step 2: Verify Data

- Check dashboard shows:
  - Total Patients: 5
  - Pending Assignments: 5+
  - Critical Vulnerabilities: 5+
  - Compliance Violations: 32+

Key Features & How to Use

Feature 1: View System Security Status

Where: Admin Dashboard (home page) **Purpose**: Show overall security metrics

1. Login as admin
2. See real-time stats:
   - Total patients in system
   - Pending task assignments
   - Active vulnerabilities
   - Unresolved violations
3. **Demo Tip**: Point out color-coded severity levels

Feature 2: Simulate a Data Breach

Where: Admin Dashboard **Purpose**: Demonstrate incident response

1. Click **"□ Simulate Breach"**
2. Choose breach type (1-5):
   - 1 = Ransomware Attack (most dramatic)
   - 2 = Insider Data Theft
   - 3 = Phishing Attack
   - 4 = Database Exposed
   - 5 = Laptop Theft
3. Enter affected records (default: 100)
4. Click through confirmation
5. **Result**: Breach appears in EDR panel

Demo Flow:

- Simulate breach → Go to EDR → Show red alert → View response steps → Resolve

---

Feature 3: EDR Panel (Threat Detection)

Where: Admin Dashboard → **"□ EDR Panel"** button **Purpose**: Show active threats and incident response

What You'll See:

- **Red Banner**: Active breach incidents
- **System Hardening Status**: Green/red lights for security controls
- **Technical Vulnerabilities Table**: All security issues
- **Nurse Violations Table**: Staff compliance errors

How to Demo:

1. Point out color-coded severity (Critical=red, High=orange)
2. Click **"□ View"** on breach to show response playbook
3. Scroll through 20+ step incident response procedure
4. Click **"□ Resolve"** to mark as handled
5. Show green checkmark indicates resolution

Feature 4: Generate Compliance Report

Where: Admin Dashboard → **"□ HIPAA Report"** button **Purpose**: Create audit-ready PDF report

1. Click button
2. Wait 2-3 seconds
3. PDF downloads automatically
4. **Contains**:
    - All unresolved violations
    - HIPAA section references
    - Severity levels
    - Timestamps
    - Signature section

Demo Tip: Open PDF and show professional formatting

Feature 5: Audit Trail

Where: Admin Dashboard → **"□ Audit Trail"** button **Purpose**: Show complete activity logging (HIPAA requirement)

Displays:

- Every login/logout
- All patient record access
- Task completions
- Violations acknowledged
- System changes

Filters Available:

- By user
- By action type
- By date range

Demo Tip: Show your own login is logged with IP address

Feature 6: User/Nurse Dashboard

Where: Login as team member (stefan, ana, jordan, jeremiah, mumin) **Purpose**: Show staff interface and compliance tracking

Key Elements:

1. **Compliance Scorecard**: Shows personal HIPAA compliance (0-100%)
2. **Patient Records**: Encrypted PHI access
3. **Task Assignments**: Directory-based secure tasks
4. **Training Access**: Link to training simulator

How to Demo:

1. Logout from admin
2. Login as team member
3. Show compliance score (starts at 0%)
4. Click **"Training Simulator"**
5. Complete 1-2 scenarios
6. Return to dashboard - score updated!

Feature 7: Training Simulator

Where: User Dashboard → **"Training Simulator"** button **Purpose**: Interactive HIPAA compliance training

5 Scenarios:

1. **Faxing Records**: Enter correct fax number (555-1234)
2. **Emailing Labs**: Use secure email (records@securemed.com)
3. **USB Request**: DENY copying PHI to personal device
4. **Hallway Discussion**: DECLINE discussing patient in public
5. **Unauthorized Access**: DO NOT access celebrity records

Scoring System:

- Correct answer: +20 points
- Wrong answer: -10 points (creates violation for admin)
- Maximum: 100%

Demo Flow:

1. Answer questions (try one wrong intentionally)
2. Show score updating in real-time
3. Wrong answer triggers alert
4. Login as admin → EDR shows your violation!

Reset Option: Click **"□ Reset My Training Progress"** to start over

---

Feature 8: Patient Management

Where: Admin or User Dashboard → Patients section **Purpose**: Show PHI encryption and access control

Features:

- **Encrypted SSN**: Automatically encrypted in database
- **MRN**: Unique medical record numbers
- **Created By**: Tracks who added each patient
- **Access Logging**: All views logged in audit trail

Demo Flow:

1. View patient list
2. Point out SSN field (encrypted)
3. Show "Created By" column
4. Check Audit Trail - your view was logged!

Feature 9: Task Assignments (Directory System)

Where: User Dashboard → **"Directory"** or pending assignments **Purpose**: Show "minimum necessary" HIPAA principle

How It Works:

- Nurses assigned tasks to send PHI to approved locations
- Must select from pre-approved directory (25 locations)
- Wrong selection = HIPAA violation

5 Categories:

1. Fax Approved (5 hospitals)
2. Email Secure (5 internal addresses)
3. Hospital Transfer (5 locations)
4. Courier Service (5 vendors)
5. Secure Messaging (5 contacts)

Demo Flow:

1. Show pending assignment

2. Open directory
3. Select correct location
4. Submit → Success!
5. Select wrong → Violation logged!

Feature 10: Password Security

Where: Forgot Password → Reset Password **Purpose**: Show multi-factor verification

Requirements:

- 8+ characters
- Uppercase letter
- Lowercase letter
- Number
- Special character
- Not a common password

Verification Uses:

- Date of Birth
- SSN Last 4 digits

Demo Tip: Try resetting password to show security checks

Demo Reset Functions

Full Demo Reset

Button: **"□ Full Demo Reset" Clears**: EVERYTHING

- All patients
- All assignments
- All violations
- All audit logs
- All breaches

Keeps: User accounts only

Use When: At end of day, or for complete fresh start

Common Demo Workflows

Workflow A: Security Incident Response (5 min)

1. Admin → Quick Setup
2. Admin → Simulate Breach (Ransomware)
3. Admin → EDR Panel (show red alert)
4. Click "View" → Show 20-step response
5. Click "Resolve" → Mark as handled
6. Show green checkmark

Workflow B: Staff Compliance Training (5 min)

1. Login as team member
2. Show 0% compliance score
3. Training Simulator → Complete 2 scenarios
4. Intentionally fail one
5. Return to dashboard → Score updated
6. Login as admin → Show violation in EDR

Workflow C: Audit & Reporting (3 min)

1. Admin → Perform various actions
2. Admin → Audit Trail
3. Show all logged activities
4. Generate HIPAA Report → PDF
5. Open PDF, show professional format

Workflow D: Complete Demo Showcase (10 min)

1. Admin → Quick Setup (30 sec)
2. Admin → Show Dashboard metrics (30 sec)
3. Admin → Simulate Ransomware breach (1 min)
4. Admin → EDR Panel (2 min)
    - Show red alert
    - View response playbook
    - Resolve incident
5. Logout → Login as team member (30 sec)
6. User → Training Simulator (2 min)
    - Complete 2 scenarios
    - Show score update
7. Admin → EDR Panel (1 min)
    - Show training violation
8. Admin → Generate Report (1 min)

9. Admin → Audit Trail (1 min)

Troubleshooting

Session Timeout (2 minutes)

Problem: Logged out automatically **Solution**: Click "Stay Logged In" when warning appears, or just login again

No Data Showing

Problem: Dashboard empty **Solution**: Click "Quick Setup" button

Can't Login

Problem: Wrong password **Solution**: Check LOGIN_CREDENTIALS.txt for correct passwords

Breach Not Showing in EDR

Problem: Simulated breach but don't see it **Solution**: Click "□ EDR Panel" button, look in "Technical Vulnerabilities" table

Score Not Updating

Problem: Completed training but score still 0% **Solution**: Refresh page, or check if you selected correct answers

---

Keyboard Shortcuts & Tips

Navigation Tips

- Always use buttons, don't manually edit URLs
- Use browser back button sparingly
- Refresh page if something looks wrong

Demo Tips

1. **Before Each Presentation**: Run Quick Setup
2. **Show Scrolling**: EDR response playbooks are long - demonstrate scrolling
3. **Highlight Colors**: Point out red (critical), orange (high), yellow (medium)
4. **Mention Timeframes**: "60-day HIPAA notification requirement"
5. **Show Encryption**: Mention SSN fields are encrypted at rest

---

Best Practices

For Smooth Demos

□ Test before presenting □ Have LOGIN_CREDENTIALS.txt open □ Close other browser tabs □ Use full screen mode □ Keep mouse movements smooth □ Explain as you click

What to Emphasize

□ Real-world HIPAA requirements (60-day breach notification) □ Encryption of sensitive data (SSN, PHI) □ Complete audit trail (every action logged) □ Role-based access control (admin vs nurse) □ Incident response procedures (20+ steps) □ Compliance scoring system (0-100%)

What to Avoid

□ Don't edit database directly □ Don't refresh during important actions □ Don't skip Quick Setup □ Don't mention this is a student project (present professionally!)

Quick Reference - All Passwords

Admin: Admin123! **Stefan**: Stefan123! **Ana**: Ana123! **Jordan**: Jordan123! **Jeremiah**: Jeremiah123! **Mumin**: Mumin123!

All passwords follow same pattern: [Name]123!

Support & Questions

During Presentation: Stay confident, if something breaks → use Full Demo Reset or restart server **Can't Remember Feature**: Check FEATURES.md **Technical Issue**: Restart server (Ctrl+C, then python3 webapp.py)

Last Updated: December 2025 For Capstone Project Presentations