SecureMed Team Contributions

Project Overview

- **Team**: 5 Members
- **Duration**: 8 Weeks (4 Sprints - Official Scope)
- **Extended Duration**: 12 Weeks (6 Sprints - Final Completion with Polish & Submission)
- **Total Development Hours**: ~600 hours (official project scope)
- **Project**: SecureMed Healthcare Security & HIPAA Compliance Platform
- **Capacity per Sprint**: ~150 hours (75 hours/week × 2 weeks)
- **Individual Velocity**: ~15 hours/week per member

Team Members & Contributions

1. Stefan Dumitrasku - Backend Lead & System Architect

Primary Responsibilities:

- Database schema design and implementation
- Backend API development (Flask)
- Encryption system (Fernet AES-128)
- System integration and testing
- Performance optimization and debugging

Sprint Contributions:

- **Sprint 2**: Implemented database CRUD functions with encryption layer
- **Sprint 3**: Integrated Flask backend with React frontend, resolved API issues
- **Sprint 4**: Conducted end-to-end system testing and performance optimization
- **Sprint 5**: Advanced testing suite development (20+ tests), system validation
- **Sprint 6**: Final system validation & bug fixes, testing documentation

Key Deliverables:

- backend.py - Main Flask API server
- setup_database.py - Database initialization
- encrypt_data.py - Data encryption utilities (Fernet AES-128)
- risk_analysis.py - Threat modeling and risk matrix

- test_advanced.py - Advanced test suite (20+ tests)
- Integration and end-to-end testing documentation

Hours: ~120 hours

---

2. Ana Salazar - Security Engineer & Authentication Specialist

Primary Responsibilities:

- Authentication & authorization systems
- Security testing and vulnerability assessment
- HTTPS/TLS implementation
- API security (JWT tokens, rate limiting)
- HIPAA compliance validation
- Password reset and verification systems

Sprint Contributions:

- **Sprint 2**: Built secure Flask API endpoints with authentication
- **Sprint 3**: Implemented JWT authentication, enforced HTTPS, conducted penetration testing
- **Sprint 4**: Performed comprehensive security audit, documented findings
- **Sprint 5**: Password reset implementation with DOB + SSN verification, multi-factor authentication enhancements
- **Sprint 6**: Security & HIPAA compliance review, final security compliance report

Key Deliverables:

- Password reset system with multi-factor verification
- JWT authentication implementation
- Role-based access control (RBAC) system
- Session management with credential obfuscation
- Security audit documentation
- HIPAA compliance report
- Input sanitization and SQL injection prevention
- Security questions and authentication enhancements

Hours: ~120 hours

---

3. Jordan Burgos - Frontend Developer & UI/UX Designer

Primary Responsibilities:

- React component development
- User interface design and styling
- Tailwind CSS implementation

- Frontend-backend integration
- Responsive design implementation
- Presentation materials and visuals

Sprint Contributions:

- **Sprint 2**: Built React + Tailwind prototype (patient list, forms)
- **Sprint 3**: Expanded frontend functionality (audit display, edit forms, PDF triggers)
- **Sprint 4**: UI/UX polish, responsive layouts, accessibility improvements
- **Sprint 5**: React dashboard optimization, resolved React/JSX vs Jinja2 template conflicts, PowerPoint presentation creation (10 slides)
- **Sprint 6**: Finalized presentation slides and demo flow, coordinated demo rehearsals

Key Deliverables:

- dashboard_react.html - Admin dashboard components
- user_dashboard_react.html - Nurse dashboard
- edr.html - EDR panel interface
- directory.html - PHI destinations directory
- Complete React component library
- 10-slide PowerPoint presentation with feature screenshots
- Presentation materials and demo visuals
- Responsive design implementation

Hours: ~120 hours

---

4. Jeremiah Luzincourt - Cybersecurity Analyst & Scanner Developer

Primary Responsibilities:

- Vulnerability detection module development
- Threat demonstration and analysis
- Scanner integration and enhancement
- EDR (Endpoint Detection & Response) features
- HIPAA violation tracking
- Integration testing and demo support

Sprint Contributions:

- **Sprint 2**: Demonstrated SQL injection and prevention methods
- **Sprint 3**: Built threat detection module prototype (2+ vulnerability types)
- **Sprint 4**: Enhanced scanner to detect 5+ vulnerability types, integrated with reports
- **Sprint 5**: Advanced testing suite support, integration testing coordination, demo setup
- **Sprint 6**: Testing summary compilation, final test validation, demo support

Key Deliverables:

- Vulnerability scanner engine with 5+ detection types
- EDR panel with real-time threat detection
- HIPAA violation logging system
- Threat demonstration scripts
- Live remediation features ("Apply Patch" buttons)
- Integration testing framework
- Testing summary and validation documentation

Hours: ~120 hours

---

5. Mumin Tahir - Documentation Lead & Report Generation Specialist

Primary Responsibilities:

- PDF report generation and formatting
- Technical documentation creation
- ReportLab integration
- Report design and branding
- User guides and manuals
- Submission packaging and preparation

Sprint Contributions:

- **Sprint 2**: Built PDF generation prototype with ReportLab
- **Sprint 3**: Automated PDF reporting integration with backend
- **Sprint 4**: Finalized PDF layout with SecureMed branding, prepared demo materials
- **Sprint 5**: Complete documentation package (installation guide, demo script, design documentation, requirements specification, team contributions)
- **Sprint 6**: Final documentation finalization, submission package assembly, deployment preparation

Key Deliverables:

- generate_report.py - PDF generation system
- Risk analysis reports (JSON + visual)
- 130+ page comprehensive documentation package
- Installation guide and setup instructions
- User guides and system overview documentation
- Demo script and instructions
- Design documentation
- Team contributions documentation
- Presentation materials
- Final submission packaging and README

Hours: ~120 hours

Sprint Summary

Sprint 2 (Weeks 3-4) - September 15-29, 2025

Focus: Core Development & API Implementation

- Database schema implementation with encryption (Stefan)
- Secure Flask API endpoints with authentication (Ana)
- React/Tailwind prototype with patient list and forms (Jordan)
- SQL injection vulnerability demonstration (Jeremiah)
- PDF generation prototype (Mumin)

Sprint 3 (Weeks 5-6) - September 29, 2025

Focus: Integration & Security Enforcement

- Backend-frontend integration (Stefan)
- JWT authentication, HTTPS enforcement, penetration testing (Ana)
- Expanded UI functionality with audit display and PDF triggers (Jordan)
- Threat detection module prototype with 2+ vulnerability types (Jeremiah)
- Automated PDF integration with backend (Mumin)

Sprint 4 (Weeks 7-8) - October 13, 2025

Focus: Testing, Audit & Polish

- End-to-end system testing and debugging (Stefan)
- Comprehensive security audit and documentation (Ana)
- UI/UX improvements with responsive layouts (Jordan)
- Enhanced scanner with 5+ vulnerability types (Jeremiah)
- Final PDF formatting with SecureMed branding (Mumin)

Sprint 5 (Weeks 9-10) - October 27, 2025

Focus: Final Features & Presentation Prep

- Advanced testing suite development (20+ tests) (Stefan)
- Password reset with DOB + SSN verification, credential obfuscation (Ana)
- React dashboard optimization, React/JSX vs Jinja2 conflict resolution (Jordan)
- Integration testing support and demo setup (Jeremiah)
- Complete documentation package assembly (Mumin)

Key Deliverables:

- Password reset fully functional
- React dashboards operational and error-free
- 20+ advanced tests executed
- Complete documentation package
- 10-slide PowerPoint presentation
- Code review and cleanup completed

Sprint 6 (Weeks 11-12) - November 10-24, 2025

Focus: Final Validation & Submission

- Final system validation and bug fixes (Stefan)
- HIPAA compliance verification and compliance report (Ana)
- Presentation finalization and demo rehearsal (Jordan & Mumin)
- Testing summary compilation and final validation (Jeremiah & Stefan)
- Deployment packaging and submission preparation (Mumin)

Key Deliverables:

- All critical bugs resolved
- HIPAA compliance verified
- Documentation and testing summary completed
- Presentation rehearsed and demo-ready
- Final project packaged for submission

Collaborative Efforts

Pair Programming Sessions:

- Stefan & Ana: API security implementation
- Jordan & Stefan: Frontend-backend integration
- Jeremiah & Ana: Vulnerability testing and validation
- Mumin & Jeremiah: Scanner output formatting
- Jordan & Mumin: Presentation materials and demo coordination

Code Reviews:

- All code changes reviewed by at least 2 team members
- Security-critical changes reviewed by Ana + one other member
- UI changes reviewed by Jordan + Stefan
- Documentation changes reviewed by Mumin + Stefan

Weekly Meetings:

- Sprint planning every 2 weeks
- Daily stand-ups (async via Slack)
- Demo sessions at end of each sprint
- Retrospectives for continuous improvement

Technology Stack (Team Decision)

- **Backend**: Python + Flask
- **Frontend**: React 18 + Vanilla JS + Tailwind CSS
- **Database**: SQLite with Fernet AES-128 encryption
- **Security**: HTTPS, JWT, RBAC, HIPAA compliance
- **Testing**: unittest + requests + integration tests
- **Documentation**: Markdown + ReportLab
- **PDF Generation**: ReportLab
- **Version Control**: Git + GitHub

Final Statistics

- **Total Lines of Code**: ~4,000+
- **API Endpoints**: 20+
- **React Components**: 8
- **Database Tables**: 5
- **Test Cases**: 34 automated tests (unit, integration, security, performance)
- **STRIDE Threat Analysis Items**: 27 analyzed and mitigated
- **Sprint Meetings**: 6 completed (original 4 sprints + 2 extension sprints)
- **Development Hours**: ~600 hours (official scope)
- **Documentation Pages**: 130+
- **Training Modules**: 3
- **Breach Simulation Playbooks**: 5

Individual Strengths Utilized

- **Stefan**: System architecture, database design, integration, performance optimization
- **Ana**: Security expertise, authentication, HIPAA compliance, vulnerability assessment
- **Jordan**: UI/UX design, frontend development, responsive design, presentation visuals
- **Jeremiah**: Cybersecurity analysis, threat modeling, vulnerability detection, testing coordination
- **Mumin**: Technical writing, documentation, report formatting, submission packaging

---

Project Outcomes

This project represents a true team effort where each member's expertise contributed to a professional, production-ready healthcare security solution. The SecureMed application successfully integrates:

- Secure patient data management with HIPAA compliance
- Comprehensive threat detection and vulnerability scanning
- Role-based access control and authentication
- Automated security audit reporting
- User-friendly dashboard interface
- Professional documentation and presentation materials

Project Status: Complete and Ready for Submission (as of November 24, 2025)