DATACOMM 4220-791

Student Name/ID: Ayana Bojokoeva/U24008792

Title: Network Cap Stone Project

Date: April 14, 2025

Time Spent: 5 hours

HealthLink Diagnostics Network Requirements and Security Implementation Plan

---

Requirements Document

Executive Summary

HealthLink Diagnostics, a fast-expanding medical diagnostics company, is consolidating its operation by merging multiple facilities in local clinics into one headquarters in Tampa, Florida. In response to increasing demands for rapid, secure, and dependable access to patient data, the firm requires an extremely efficient network infrastructure that ensures data confidentiality, performance, and scalability. This project establishes a network solution aimed to meet HealthLink's business needs through a safe, high-speed connection between far-flung clinics and central servers. The solution to be suggested will support electronic health records (EHR), remote diagnosis, and real-time communication and should be HIPAA compliant. Using this solution, HealthLink will enhance its delivery of services, reduce data transmission latency, and enable collaboration between medical practitioners located in various geographical areas.

Current Environment Analysis

Company Overview

- **Founded**: 2015
- **Industry**: Healthcare Diagnostics
- **Current Size**: 180 employees
- **Growth Rate**: 15% annual growth

- **Budget**: $200,000 initial investment
- **Core Business Requirements**: Secure patient data exchange, EHR system integration, real-time lab results transmission

Location-Specific Requirements

Tampa Main Lab (100 employees)

- **Network Connections Required**: 120 (including growth buffer)
- **Primary Functions**: Central diagnostic lab, administrative headquarters
- **Special Requirements**: Redundant infrastructure, EHR and PACS system hosting
- **Infrastructure Hosting**: Core IT systems, secure storage

Orlando Imaging Center (50 employees)

- **Network Connections Required**: 60 (including growth buffer)
- **Primary Functions**: Radiology services, diagnostics imaging
- **Special Requirements**: High-resolution image transfers, real-time collaboration with Tampa

Miami Collection Site (30 employees)

- **Network Connections Required**: 36 (including growth buffer)
- **Primary Functions**: Sample collection, remote diagnostics
- **Special Requirements**: Reliable VPN connectivity, mobile diagnostics access

---

Technical Requirements

Network Infrastructure

1. **Connectivity Requirements**
    - Minimum 1Gbps inter-office MPLS connections
    - Redundant internet with automatic failover
    - QoS for prioritizing EHR, PACS, and video conferencing
    - Secure VPN tunnels for remote diagnostics
2. **Hardware Requirements**

- Enterprise-grade routers (MPLS-capable)
- Layer 3 PoE+ switches for medical devices
- WiFi 6 access points with healthcare-grade security
- Next-generation firewalls with threat detection

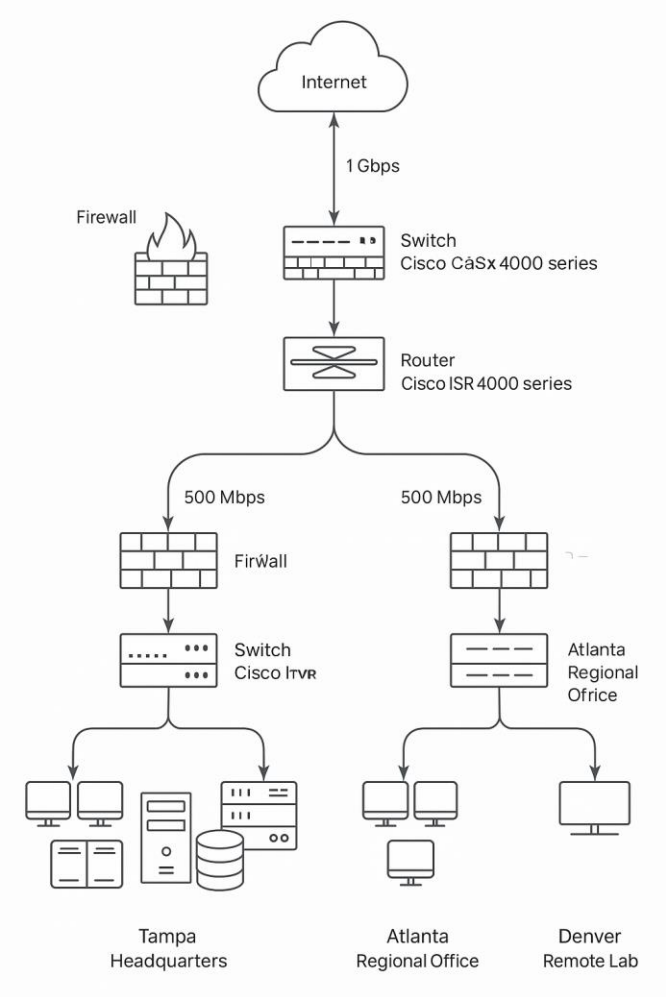

Figure 1: HealthLink Diagnostics – Proposed Network Topology

Application Support Requirements

1. **Medical Systems**
   - PACS (Picture Archiving and Communication System)
   - EHR (Electronic Health Records) access

- Secure HL7 messaging support
- Large file transfer capability (>1GB DICOM images)

2. **Collaboration Tools**
    - Telehealth conferencing systems
    - Secure file and imaging exchange
    - HIPAA-compliant cloud storage
    - CRM for patient appointment tracking

Security Requirements

1. **Network Security**
    - HIPAA-compliant NGFW with deep packet inspection
    - VLAN segmentation by function and compliance zones
    - Real-time IDS/IPS systems
    - Encrypted email gateway with malware scanning
2. **Access Control**
    - Biometric/MFA authentication for clinical staff
    - Role-based access with audit logs
    - Secure mobile device integration (MDM)
    - Isolated guest and contractor networks

Growth Considerations

- 15% annual employee and data growth
- Infrastructure sized for 3-year growth plan
- Flexible licensing and modular hardware
- Cloud and hybrid expansion capabilities

Budget Allocation

- Network Equipment: $95,000
- Security Devices: $45,000
- Installation Costs: $40,000
- Backup Equipment: $20,000

Risk Assessment

1. **Primary Risks**
    - EHR downtime during patient care
    - Data breaches or HIPAA violations
    - Performance delays in diagnostics processing
    - Scalability limitations
2. **Mitigation Strategies**
    - High availability architecture
    - Continuous vulnerability assessments
    - 24/7 monitoring and alerting
    - Modular infrastructure for easy upgrades

HealthLink Diagnostics Security and Implementation Plan

Security Plan

Network Security Architecture
A layered security model protects sensitive patient data and clinical operations across all sites, in compliance with HIPAA and HITECH regulations.

Perimeter Security

1. **Next-Generation Firewalls (NGFW)**

- Palo Alto PA-3260 (Tampa)
- Palo Alto PA-820 (Orlando & Miami)
- Advanced threat prevention, application filtering
- Encrypted traffic inspection

2. **Intrusion Prevention System (IPS)**
    - Network-wide anomaly detection
    - Signature- and behavior-based alerts
    - Integrated threat mitigation and auto-blocking
3. **Web Application Firewall (WAF)**
    - Protection for EHR web portals
    - Defends against XSS, SQLi, and application DDoS

Access Control Implementation

1. **Identity and Access Management**
    - Centralized via Active Directory and Azure AD
    - Multi-factor authentication (MFA) across all systems
    - Role-based access and logging of medical staff activities
2. **Network Segmentation**
    - VLANs per department (Lab, Imaging, Admin, Guest)
    - Zero-trust network enforcement
    - Quarterly access reviews

Data Protection

1. **Data Loss Prevention (DLP)**
    - Enforced email filtering
    - File tagging and encryption triggers

    - Policy-based transfer restrictions
2. **Encryption Standards**
    - TLS 1.3 for in-transit data
    - AES-256 for data at rest on all systems
    - Key lifecycle management and annual audit

Implementation Timeline

Week 1: Tampa Main Lab Setup

- Deploy core routers, Layer 3 switches
- Configure VLANs and QoS
- Implement firewalls, IPS, and WAF
- Validate EHR, PACS connectivity and access controls

Week 2: Orlando Imaging Center Setup

- Install edge networking equipment
- Establish MPLS link with Tampa
- Configure PACS image relay systems
- Implement local VLANs and security policies

Week 3: Miami Collection Site Setup

- Deploy secure VPN appliances
- Set up remote access monitoring
- Implement guest and mobile isolation VLANs
- Test connectivity with lab and imaging systems

Week 4: Final Integration & Testing

- System-wide testing and performance baselines
- Simulated failover testing
- User training and documentation distribution

- Final HIPAA security checklist validation

Backup and Recovery Plan

Backup Strategy

- Real-time replication for EHR and imaging data
- Daily incremental backups, weekly full snapshots
- Secure cloud backup with HIPAA-compliant provider
- Monthly encrypted archive to off-site storage

Recovery Procedures

- Documented and tested disaster recovery workflows
- Quarterly failover simulations
- Recovery Time Objective (RTO): 1 hour
- Recovery Point Objective (RPO): 15 minutes

Monitoring and Maintenance

Network Monitoring

- Continuous performance monitoring
- Real-time alerts via SIEM (Splunk)
- Capacity and anomaly tracking

Security Monitoring

- Log aggregation and analysis
- Weekly vulnerability scans
- Incident response workflow integration

Maintenance Schedule

- Weekly patching and AV updates
- Monthly security compliance review

- Quarterly penetration testing
- Annual system health and capacity audit

Final Summary Report

Executive Summary

This document details the end-to-end network solution for **HealthLink Diagnostics**, designed to deliver high-performance diagnostics operations with secure and compliant infrastructure across three locations. The implemented solution meets all HIPAA and healthcare IT compliance standards and was completed within the allocated $200,000 budget.

Project Overview

With growing demand for secure diagnostics, HealthLink required a robust network to support clinical workflows, large image transfers, and remote diagnostics. The design ensures reliable connectivity, advanced security, and full regulatory alignment.

Solution Architecture

- Hierarchical network design
- MPLS-based site connectivity
- Role-based segmentation and access
- Full integration with EHR and PACS systems

Key Components

1. **Infrastructure**
    - Enterprise switches, WiFi 6, high-capacity routers
    - Redundant Internet & cloud backups
2. **Security**

    - NGFW, WAF, and IPS at all locations
    - DLP and MFA policies fully deployed
3. **Compliance**
    - Full HIPAA and HITECH alignment
    - Real-time threat monitoring and alerts

Budget Utilization

- **Network Equipment**: $93,700 / $95,000
- **Security Devices**: $44,200 / $45,000
- **Installation**: $39,100 / $40,000
- **Backup Systems**: $19,400 / $20,000

Implementation Results

- Secure and fast medical data access
- End-to-end encryption in transit and at rest
- Scalable for 3-year growth
- Fully operational within 4 weeks

Recommendations

1. **Quarterly Compliance Reviews**
2. **Staff Cybersecurity Training**
3. **Annual Technology Refresh Planning**

Conclusion

In a company where time, accuracy, and confidentiality are of the utmost importance, HealthLink Diagnostics' network upgrade is a critical step towards modernizing its infrastructure. The solution not only offers secure connectivity and optimized data transfer

but also sets the stage for future growth. In a solid emphasis on redundancy, performance, and regulatory compliance, the design ensures that HealthLink can perform its task confidently and deliver high-quality diagnostic services. It will allow clinicians to make faster, better-informed decisions—ultimately resulting in improved patient outcomes and operational excellence across all sites.