Cisco Medical-Grade Network: Build a Secure Network for HIPAA Compliance

What You Will Learn

The Cisco® Medical-Grade Network (MGN)\(^1\) provides a network foundation that enables reliable, transparent, and secure health data communications among the healthcare community while providing the framework to meet your specific Health Insurance Portability and Accountability Act (HIPAA) compliance requirements. This framework allows integration and interoperability at each functional area to optimize interactions among healthcare participants, processes, applications, and hardware components.

Cisco's implementation of MGN includes connecting a main ambulatory health center on a corporate campus to satellite clinics at geographically dispersed campus locations and remote clinician sites.

LifeConnections Health Center

Cisco is a world leader in providing employee benefits that foster a work-life balance promoting health and well-being as a priority. This philosophy came to life with the onsite LifeConnections Health Center (LCHC) in San Jose, California, Research Triangle Park (RTP), North Carolina, and Bangalore, India.

The health center gives Cisco employees and their families onsite access to a full range of medical care services from primary care that includes physical examinations, immunizations, travel medicine, lab work, health coaching, ancillary services, and an onsite pharmacy.

Unique to Cisco in the onsite healthcare model is Cisco's technologies powered by a secure Medical-Grade Network that enables:

- Communication needs for clinicians, patients, administrators, and partners
- Patient privacy and data security compliant with healthcare regulatory requirements
- The health center’s unique information, technology, bandwidth, and integration capabilities
- Anytime, anywhere information capture and access for wired and wireless applications and devices
- Converged data, voice, and video networks to enhance patient care and collaboration
- Identity- and policy-based security from inside the network to beyond organizational walls
- Ability for Cisco employees to stay connected while they are waiting for their appointments

As shown in Figure 1, Cisco MGN is the foundation for bringing together a rich patient experience integrating Cisco and partners’ technologies.

Partner technologies and solutions include the following:

- Data center connectivity
- Electronic medical records
- Patient self-service kiosk for check-in, check-out, co-pay, and eSignatures

\(^1\) Cisco Medical Grade Network (MGN) is a set of Cisco recommended guidelines for building an optimal healthcare network.
Cisco technologies include:

- Cisco TelePresence® systems, Cisco HealthPresence® technology, and WebEx® meeting applications
- Context Aware Solution: Asset tracking and temperature monitoring
- Unified Communications: Speech Connect for Cisco Unity® Connection
- Digital media
- Secure wired and wireless infrastructure
- Security and compliance management
- Website

**Figure 1.** LCHC Logical Architecture Premise Diagram

---

**Network Architecture**

The network architecture direction is to provide network services using existing standards and infrastructure to the best possible extent. However, Cisco wanted to ensure the scope of HIPAA audits is contained within the health center infrastructure only.

Therefore, for the LCHC implementation, network design and support processes for voice and video (Cisco TelePresence conferencing and digital media) co-existed with Cisco corporate infrastructure, maximizing resources.
and reducing the total cost of ownership (TCO). Data traffic that contains electronic protected health information (ePHI) data is isolated from the corporate infrastructure.

Voice services, Cisco TelePresence systems, and physical wireless network infrastructure are shared between the LCHC network and Cisco corporate network. Logical IP connectivity between the LCHC and Cisco corporate data networks is not nor will be enabled.

Network Design

Wired Network

The LCHC voice and Cisco TelePresence systems use the Cisco internal network, with strict security imposed on the physical voice ports and their configuration.

The LCHC data network connects to the Internet via Cisco’s corporate DMZ and communication that has medical information goes through encrypted tunnels or SSL connections. Data traffic between the LCHC and the medical service provider (MSP) is sent through dedicated circuits. Thus, the flow of specific data complies with HIPAA requirements. Key Cisco resource sites required for MSP’s operational purposes such as access to Cisco’s corporate directory for employee eligibility verification and other Cisco intranet sites for internal safety and security protocols and issue case management can be accessed through the DMZ over an IP Security (IPsec) tunnel to the corporate network. Device monitoring by Cisco’s centralized network management system can be performed through the DMZ as well. The San Jose based LCHC provides connections to satellite sites in Stanford Hospital and Clinics and RTP campus in a hub and spoke model.

The LCHC network offers a high service-level agreement (SLA); thus the design requires redundant devices in the network topology. For redundancy, there is a dedicated pair of every networking component in the hierarchy. As shown in Figure 2, the equipment includes Cisco 3845 Integrated Services Router (ISR) DMZ gateways, Cisco 3750 ISR DMZ switches, Cisco Adaptive Security Appliances (ASAs) configured as active and standby, respectively, Cisco Catalyst® 6000 distribution switches, and a Cisco 3845 headend gateway. The ASAs are configured as the firewall and Network Address Translation (NAT) device; they provide routing for the LCHC network. Data traffic from a host on a LCHC LAN subnet traverses the distribution switches into the ASA, where it undergoes inspection by the firewall feature of the ASA and then, if permitted, either is passed onto another LAN segment or follows the default route to the medical service provider through its ASA. Return traffic from the other LAN subnet or the service provider follows the reverse route into the LCHC ASA. The ASA inspects the packet and, if permitted, forward it back to the host.

The Cisco 3845 LCHC DMZ gateway provides the uplink to DMZ access gateways for access into the DMZ. The same internal Enhanced IGRP (EIGRP) Autonomous System (AS) runs on the Cisco 3845 for reachability to the DMZ and the internal network. Downlinks from the DMZ gateways and the outside interface from the ASAs are connected through Cisco 3750 Layer 2 switches, connected in a stackable configuration in order to establish a Hot Standby Router Protocol (HSRP) relationship for redundancy. The ASA outside interfaces and the DMZ gateway downlink interfaces are in an Internet routable IP subnet. This subnet should be large enough to accommodate static NAT addresses of the LCHC network devices for management traffic and connectivity to satellite clinics. The distribution switches connect to the ASA inside interfaces through trunks, where all LCHC VLANs are trunked. The ASA has a physical connection to the MSP ASA for all traffic destined to the MSP and Internet traffic. The LCHC internal networks are configured as subinterfaces on the inside interface on the ASA, and static routing is used to direct traffic, with default route to the MSP or DMZ, depending on requirement.

Cisco uses 3rd party tool Splunk for LCHC network compliance auditing and real time alerting of anomalies. The audit includes network traffic, user access, change management activities, and system errors.
Extension of Network and Connectivity of Services to Other Campus and Clinician Locations

An extension to LCHC, the LifeConnections clinic at RTP uses Cisco HealthPresence technology to provide care-at-a-distance with physicians located in San Jose providing care to employees at the RTP campus.

Although the ASA can be used to terminate VPN tunnels from the remote spoke routers, Cisco suggests using a separate headend router from a scalability, performance, and flexibility point of view. The Cisco HealthPresence design is built on the Dynamic Multipoint VPN (DMVPN) technology where the headend (hub) router is used to terminate IPsec tunnels from the remote Cisco HealthPresence router.

The headend router is physically connected to the LCHC Layer 2 switch, and logically connected to the ASA through the existing trunk on the switch and subinterfaces on the ASA. The headend router is connected to the LCHC “inside” network on two interfaces: Gig0/0 for encrypted traffic to and from the Cisco HealthPresence router and Gig0/1 for decrypted traffic for routing within the LCHC network. Correspondingly, two additional subinterfaces are created on the ASA (Gig 0/1.xx for encrypted traffic and 0/1.yy for decrypted traffic) for the headend router connectivity.

The Cisco HealthPresence design implemented at the LifeConnections clinic at RTP is replicated to extend care for specialty care services in partnership with Stanford Hospital and Clinics.

Figure 2. LCHC and Cisco HealthPresence Network
Wireless Network

Wireless infrastructure plays a crucial role in providing true mobility throughout the facility for LCHC clinicians. The wireless infrastructure that is deployed by Cisco IT is highly reliable, easy to manage, and resilient for voice and other patient care applications.

The LCHC wireless network consists of a pair of Cisco 5500 Series Wireless LAN Controllers along with more than 46 Cisco Aironet® 3500 Series Access Points installed throughout the facility. The Cisco Unified Wireless Network Architecture offers redundancy at several levels. At the RF level, the system “self-heals” when one or more access points becomes inactive. The architecture also supports port redundancy per controller and controller device redundancy.

The LCHC wireless network supports both wireless voice and data access anywhere in the facility. The IEEE 802.11a,b,g,n Cisco Aironet 3500 Series Access Points can be centrally managed with Cisco 5500 Series Wireless LAN Controllers in high-availability architecture along with the Cisco Wireless Control System (WCS) management software. The Cisco WCS provides centralized network management, security monitoring, and localization of rogue devices, and it automatically associates each new access point with the controller, eliminating manual configuration and saving many hours in maintenance time.

The LCHC wireless network contains not only LCHC local Service Set Identifiers (SSIDs) but also Cisco corporate wireless SSIDs. The broadcast of LCHC SSIDs is limited to the relevant groups for access. The Cisco Corporate wireless infrastructure is logically extended to LCHC premises through trunk links.

In addition to centralized management and rapid deployment of all of the access points, the Cisco Unified Wireless Network offers segmentation of user groups. This feature enables LCHC IT staff to configure separate virtual LANs for voice and data, helping to ensure both data security and quality of service (QoS) for voice traffic. Voice receives top priority to support the ability to roam seamlessly from access point to access point without dropping a call. QoS and the reliability of the network are further enhanced through support for Wi-Fi Multimedia (WMM), which prioritizes delay-sensitive traffic to provide uninterrupted service and voice optimization.

LCHC technology stack also includes the Cisco Context-Aware Mobility Solution for automated regulatory compliance and risk management, where the wireless network is used to locate people, objects, and measure temperature using Radio Frequency identification (RFID) tags. Integrated with the AeroScout MobileView server, the solution provides LCHC IT staff the ability to monitor refrigerator temperature, room temperature, and track LCHC-managed mobile assets.
Figure 3 depicts the LCHC wireless network infrastructure.

**Figure 3.** Wireless infrastructure Connection Between LCHC and Cisco Corporate Network

The Cisco Unified Wireless Network offers LCHC a feature-rich wireless network. The LCHC Wi-Fi capability of the network enables patients to do self-service check-in and medical staff to retrieve, update, and file patient records while carrying out visits using tablet PC or mobile devices, and to locate life-saving medical equipment in a time-critical manner.

The LCHC uses the following Cisco Unified Communications Solutions:

- Cisco IP Contact Center Express
- Cisco Unified Communications Manager
- Cisco Unified Wireless IP Phone 7925

The LCHC uses the following Cisco routers and switches:

- Cisco Catalyst 6500 Series Supervisor Engine 720
- Cisco Catalyst 3750 Series Switch
The LCHC uses the following Cisco Unified Wireless Network applications:

- Cisco 5500 Series Wireless LAN Controllers
- Cisco Aironet 3500 Access Points with CleanAir technology
- Cisco 3310 Mobility Service Engine
- Cisco Wireless Control System

The LCHC uses the following products provided by Cisco technology partners:

- AeroScout RFID tags
- AeroScout MobileView Server
- Personal digital assistants (PDAs)
- Laptops

**Conclusion**

In keeping with our Cisco on Cisco vision and technology evolution, the MGN will follow technology and product upgrades.

This scalable and regulatory-compliant connected architecture has been used and replicated for the new LifeConnections Health Center at Bangalore and three satellite clinics, resulting in a 50-percent productivity and implementation cost savings.

**For More Information**

For more information about Cisco MGN, please visit: [http://www.cisco.com/web/strategy/healthcare](http://www.cisco.com/web/strategy/healthcare).