2012

University of North Carolina Wilmington

Master of Science in

Computer Science and Information Systems

Proceedings

https://csbapp.uncw.edu/mscsis

INFORMATION SECURITY BLUEPRINT FOR NATIONAL HEALTH INFORMATION NETWORK

Selin Benli

A Capstone Project Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
Of the Requirements for the Degree of
Master of Science

Department of Information Systems and Operation Management / Department of Computer Science
University of North Carolina Wilmington
2012

Approved by
Advisory Committee

_____	_____
Dr. Ulku Yaylacicegi	Dr. Ron Vetter
_____	_____
Dr. Stacy Mitchell	Dr. Bryan Reinicke

Accepted by

_____

Dean, Graduate School

Abstract

This study describes design and implementation considerations to provide an information security blueprint for interconnecting healthcare information technology (HIT) networks.

The purpose of this research is twofold. First, it provides background information about technology implementations in healthcare organizations; current HIT services, electronic healthcare records (EHRs) and design considerations for healthcare networks. Second, it explores wide area network (WAN) technologies and different security methods for ensuring the secure exchange of the healthcare information between medical providers. In this study, you will find detailed information on the network design considerations, federal regulations for protecting patient data, healthcare IT interoperability, health information exchange (HIE) and nationwide health information networks (NHINs). Lastly, integrating remote access and WAN services, access control lists and securing the network perimeter are discussed.

List of Figures

List of Tables

Table of Contents

Chapter 1: Introduction

Healthcare represents a significant segment of the U.S. economy and workforce. According to the Centers for Medicare & Medicaid Services, in 2010, total health expenditures reached $2.6 trillion, which translates to $8,402 per person or 17.9% of the nation's GDP [52]. Also, according to the Bureau of Labor Statistics, healthcare is the single largest industry in the United States, providing 14 million jobs through approximately 580,000 establishments [19]. Growth in spending on health care programs is one of the central fiscal challenges facing the US federal government. Healthcare spending per person has grown faster than the nation's economic output per person, on average by nearly 2 percentages per year, for the past several decades. As a result, this rapid growth is creating a challenge for federal health care programs like Medicare and Medicaid, state and local governments, and the private sector [27]. In 2009, the Office of the Actuary at the Centers for Medicare and Medicaid Services (CMS) projected that by 2030, given current trends, national health expenditures will exceed 30% of the GDP [46]. These statistics indicate that the stakeholders of the healthcare industry need to take some precautions in order to control and reduce healthcare spending.

Technology integration and use of healthcare information technology (HIT) in healthcare organizations can help to decrease costs while increasing overall quality of patient care. HIT services involve the use of technology to provide healthcare as well as to enable the comprehensively exchange the digital health information [29]. Currently, one of HIT services is Electronic Healthcare Record (EHR) system. EHR is an electronic record of patient health information generated by one or more encounters in any care delivery setting [9]. EHR improves health information accessibility by making possible for the patient record to be used by multiple providers at once, which enables coordination of care between doctors. Doctors can have a complete picture of the patient's health without repeating unnecessary tests and examinations performed before. EHR implementations can increase the quality of

healthcare delivery and reduce the associated costs [38]. Therefore, to encourage organizations to adopt EHRs, the federal government has set aside funding to use for incentives, grants, and loans as part of the American Recovery and Reinvestment Act of 2009 (ARRA). The funding for transition to EHRs is called the Health Information Technology for Economic and Clinical Health (HITECH) Act, which is approximately $19 billion [6].

By implementing EHRs and meeting interoperability standards, healthcare organizations can join Health Information Exchanges (HIEs) to exchange patient data. One of the primary goals behind the government's initiative for encouraging the adoption of EHRs is to increase HIEs and eventually maintain a Nationwide Health Information Network (NHIN). The NHIN is an initiative that establishes mechanisms and conventions for a nationwide electronic health information infrastructure. The NHIN is being developed to provide a secure and interoperable health information infrastructure that allows stakeholders, such as physicians, hospitals, payors, state and regional HIEs, federal agencies, and other networks, to exchange health information electronically [14]. NHIN will help significantly to reduce healthcare spending in the US while improving the patient care quality.

Besides the advantages they offer; EHRs and HIEs pose several challenges to entities participating in the delivery of healthcare. One of these challenges is the security of the patient data exchanged between the healthcare organizations. Information security is described as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction" [2]. Information security also aims for protecting the confidentiality, integrity and availability of information. Healthcare practices increasingly rely on networks for their core operations; thus, become more vulnerable to information security threats. Compromised security in healthcare organizations can have serious consequences as it disrupts critical functions. Therefore, protecting healthcare information is crucial and regulated by the federal

government. A major section of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 aims to standardize the steps that needs to be taken to protect patient privacy. More specifically, HIPAA mandates healthcare institutions take actions for ensuring the security of personal health information. It also requires The Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and national identifiers for providers, health plans, and employers [31].

US government has plans for enhancing HIEs and establishing the NHIN in near future. Therefore, securing healthcare systems, networks and information exchange are important and time-sensitive tasks for medical providers. To support these efforts, the Office of the National Coordinator (ONC) for Health Information Technology, which sponsors the creation of the NHIN, has established some goals for maintaining the secure information exchange [42]. However, the specific security methods, tools, their implementations and related standards for healthcare organizations have not yet been stated clearly. For example, to encourage creation of HITs, Microsoft published a guideline, which is called the Connected Health Framework Architecture and Design Blueprint [55]. In this study, the Connected Health Framework architectural approach is explained in great details and proposed as a solution for transforming healthcare through technology options that are cost-effective, productive, and connected by design. Although this paper includes information security as one of the architectural challenges, it does not explore the security concerns of interconnected network design extensively. In addition to this research, Dimitris Gritzalis and Costas Lambrinoudakisbby propose security architecture for interconnecting health information systems in their study [56]. However, since their architecture is mainly designed for providing authentication and authorization services in web-based distributed systems, it does not cover the information security considerations in a broader perspective. Therefore,

this study focuses on the information security best practices for interconnecting HIT networks and contributes to a specific research area, which currently is not addressed in the literature.

The objectives of this study are:

- Understanding different Wide Area Network (WAN) technologies, their advantages and disadvantages to analyze how HIT networks can be connected and information exchange can be achieved.
- Understanding the information security requirements in the healthcare industry, related regulations and how these regulations effect healthcare organizations.
- Exploring specific security requirements for interoperable HIT networks and best practice approaches for fulfilling these requirements, in order to secure communications between organizations.

This research proposes an information security blueprint for interconnecting HIT networks with security and privacy concerns in mind. The findings of this research can be utilized as a guide for understanding current wide area network (WAN) technologies, and different security measures that can be implemented for HIT networks.

Chapter 2: Literature Review and Background Technology

2.1 Healthcare Industry in the US

In 2000, the World Health Organization (WHO) ranked US health care systems, among 191 member nations, as the highest in cost, first in responsiveness, 37th in overall performance and 72nd by overall level of health [51]. It was indicated in this ranking; the US spends more than $2.6 trillion annually on the healthcare [52]. However, health outcomes and quality of healthcare delivery in the US are not better, and often worse, compared to the most developed nations in the world. Therefore, it is clear that this amount is not spent efficiently [3] [18].

Healthcare in the US faces multiple problems, including high and rising expenditures, inconsistent quality, and gaps in care and access [3] [57]. According to Commonwealth Fund, a private foundation working toward a high performing health system, healthcare delivery in the US is a "cottage industry" [4], i.e. providers have no relationship or accountability to one another. This comparison mainly indicates the fragmentation at the national, state, community, and practice levels; which is a result of not having a single national entity or set of policies guiding the US healthcare system. Today, states divide their responsibilities among multiple agencies, while providers practicing in the same community and caring for the same patients often work independently from one another [4]. Dr. Elhauge, who published a book about the fragmentation of the US healthcare in collaboration with several scholars and policymakers, summarizes this problem as "U.S. health care suffers from excessive disintegration that worsens outcomes and thus constitutes fragmentation [22]".

The fragmentation of the healthcare delivery system is a fundamental contributor to the increasing spending and poor overall performance of the healthcare system. In this fragmented system, patients navigate unassisted across different providers and care settings; while poor communication and

lack of clear accountability for a patient among multiple providers' leads to medical errors, waste, and duplication. Other contributing factors, such as absence of peer accountability and an established quality improvement infrastructure also foster poor overall quality of care [22]. Furthermore, primary care system, which consists of preventive medicine and the management of chronic illnesses, are not fully supported over the intensive acute care system. Although primary care system is an efficient option to control healthcare costs and present extensive care, failure to provide necessary support leads the collapses in this system and ultimately increases the acute care demand as well as the costs associated [4].

In order to find solutions to the current healthcare problems and make a roadmap for implementations, it is important to characterize the ideal healthcare system and find out the important drivers. To accomplish this, The Commonwealth Fund Commission on a High Performance Health System identified some attributes of an ideal health care delivery system. According to this report, firstly, patients' clinically relevant information should be available to all providers at the point of care and to patients through EHR systems. Second, patient care should be coordinated among multiple providers, and transitions across care settings should be actively managed. Third, providers both within and across settings should have accountability to each other, review each other's work, and collaborate to for delivering high-quality and high-value care. Next, patients should have easy access to appropriate care and information. Lastly, the system should continuously innovate and learn in order to improve the quality, value, and patients' experiences of healthcare delivery [4].

The same commission has also made some policy recommendations, which will promote greater organization of the delivery system to achieve the proposed attributes. These recommendations can be listed as payment reform, patient incentives, regulatory changes, accreditation, provider training,

government infrastructure support, and HIT [4]. HIT, which provides critical infrastructure for an organized delivery system, will be the focus of this research.

2.2. Technology Integration in the Healthcare and Healthcare IT

Information technology (IT) has the potential to improve the quality, safety, and efficiency of healthcare [33]. Therefore, healthcare industry is taking advantage of current technologies and changing the way healthcare is practiced and delivered. Today, a majority of healthcare providers are utilizing computers, applications and networks as part of IT adoption efforts [12].

Use of a common network provides easy and quick access to patient data and enables information sharing for medical providers [33]. Currently, most healthcare environments are utilizing converged networks, which are single IP networks that simultaneously handle data, voice, and video traffic. Converged networks allow medical professional to respond in real time to the needs of a patient's medical care. Both wired and wireless technologies can be integrated into the converged network. Furthermore, a number of portable and mobile devices are being adopted for use in healthcare, especially for accessing patient records and maintaining clinical notes. Additionally, many healthcare providers are using the Internet for medical research and diagnostic tools to access medical articles and supporting research through various healthcare information databases. While solutions like these were once only possible for large hospitals and medical groups, technological innovations and lower prices are making them viable options for smaller practices as well [12].

In general, IT allows health care providers to collect, store, retrieve, and transfer information electronically [33]. By definition, healthcare IT is "the application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making" [8]. Particularly, HIT

provides a framework to describe the comprehensive management of health information across computerized systems and its secure exchange between consumers, providers, government, and insurers [52].

HIT is increasingly viewed as the most promising solution for improving the overall quality and efficiency of the healthcare delivery system in the US [29] [3] [33]. According to a study by RAND Health, if HIT were properly implemented and widely adopted in the healthcare organizations, the US healthcare system could save $77 billion annually, increase safety, and improve the quality of patient care [10]. In addition, the implementation of HIT can complement other productivity features such as competition and deregulation [3].

For understanding the potential uses and benefits, many researchers and government agencies studied HIT so far [3] [5] [10] [33]. According to their findings, the major advantage of utilizing HIT is having easy access to complete and accurate medical and patient information [29]. This functionality helps doctors to diagnose health problems faster and reduce medical errors, provides safer and quality care to the patients, and lowers healthcare costs. HIT also strengthens the coordination of care as it enables enhanced peer-to-peer and professional-patient communication [26]. This coordination can help to improve the consumer-centered care, which aims to give patients access to their medical information for maximizing their involvement in the treatment decisions [52]. Furthermore, HIT strengthens the patient privacy and data protection since its applications offer a way to securely store and share patient information between different entities [29].

HIT applications also increase the administrative efficiency significantly as they store information digitally. This helps to reduce paperwork in the healthcare organizations and enables clinicians to spend more time on the patient care, rather than their administrative responsibilities [29]

[52]. Moreover, as tracking health information digitally provides easier access to patient histories, test results, and can provide automatic alerts; HIT offers an increased early detection of medical conditions. It also prevents the duplication of the tests, control the costs and reduces the diagnose time [12]. Also, utilizing HIT services improve disease prevention and response, as digital tracking of health information makes it easier to observe trends in the general population as well as track successful treatment methods. This functionality promotes public health and preparedness [26]. As a result, widespread use of HIT expands access to the affordable, quality and cost-effective patient care while improving the delivery of healthcare in US [29].

2.3 Common Medical/HIT Software Applications

Medical applications can dramatically increase the efficiency and productivity of a medical group and are integral to the flow of patient care. Currently, one of the most common medical software bundle used in medical practices is practice management system (PMS), which automates basic business functions, including patient registration, scheduling, billing, and reporting [12]. Besides PMS, there are many other types of HIT applications available to medical professionals. In general, these applications fall into three categories: administrative and financial systems that facilitate billing, accounting, and other administrative tasks; clinical systems that facilitate or provide input into the care process; and infrastructure, which supports both the administrative and clinical applications [33].

Some clinical systems examples can be listed as imaging and visualization software, which provides viewing electronic digital images on the desktop; e-prescription software for electronically generating prescriptions through an automated data-entry process among pharmacies; and medical information systems, which manage and analyze public health information [12]. A comprehensive list of HIT examples and their applications in hospitals and physicians' offices can be found in Table 1, at

Appendix A. In addition, one of the most commonly employed HIT applications in the healthcare environment is electronic health records (EHR) software [29], otherwise known as electronic patient records or computerized patient records.

2.3.1 Electronic Healthcare Records (EHRs)

An electronic health record (EHR) is a digital version of information collected by medical providers that is contained in a paper chart. According to the definition provided by the Health Information Management Systems Society (HIMSS), EHR is "a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports [46]". EHR implementations automate access to information and streamline the clinician's workflow. These systems also support other care-related activities such as evidence-based clinical decision support, quality management and outcomes reporting [20].

An EHR system improves patient care by allowing physicians, radiologists, nurses, and laboratory technicians to gather the complete picture of the individual and work in parallel with accurate and current information. Also, EHRs improve health information accessibility by making possible for the patient record to be used by multiple providers at once. Therefore, EHR implementation encourages coordination of care between doctors [5]. By implementing EHRs and meeting interoperability standards, healthcare organizations can join Health Information Exchanges (HIEs). This allows medical practices to share information, have access to already performed tests and lab results and ensure that the complete picture of a patient's health is documented [20]. By making it easier to use and share patient information, EHRs can help health care providers to reduce medical errors, save money and time [5].

EHRs also make data mining and research more successful since health data is easily searched, compiled, and summarized for meaningful results in the individual's record [12]. This functionality helps for tracking community or population-level health issues and trends [8]. In addition, EHRs offer a convenient solution for compliance with HIPAA privacy and security rules since digital records allow data to be encrypted during storage, use, and transfer; and access to medical data can be tightly controlled and audited [20].

Today, many vendors offer EHR systems and as a result, there are some differences for the look and functionality of these products. However, the inner workings of this software are very similar [5]. On the front end, medical data is entered into various screens within software modules. On the back end, all EHRs rely on a database system that manages information from various component systems. The components are contained within the EHR vary according to what the vendor has chosen to include in its product offering. This is often based on the healthcare setting that the EHR product is designed to operate, such as inpatient, outpatient, medical, or behavioral clinics [12]. Administrative system, clinical documentation, computerized physician order entry, laboratory system, radiology system and pharmacy system components are some of the common core components of an EHR. These components enable EHR to combine patient data from various departments and units [12] [17].

Administrative components typically contain information regarding registration, admissions, discharge, and transfer (RADT). It can also include patient data, such as the patient's name, demographics, employer, and symptoms. When a patient registers, administrative component assigns a unique identifier, like PatientID, that is used to link all other information from other components to the patient. The clinical documentation module provides electronic capture of clinical notes from doctors, nurses, and other clinicians. The documentation can include patient assessments, clinical reports, charts, and even records of patient authorizations and consents to treatments. On the other hand, computerized

physician order entry (CPOE) allows medical providers to electronically order tests, such as laboratory and radiology services, as well as place orders for prescriptions with the pharmacy in real time.

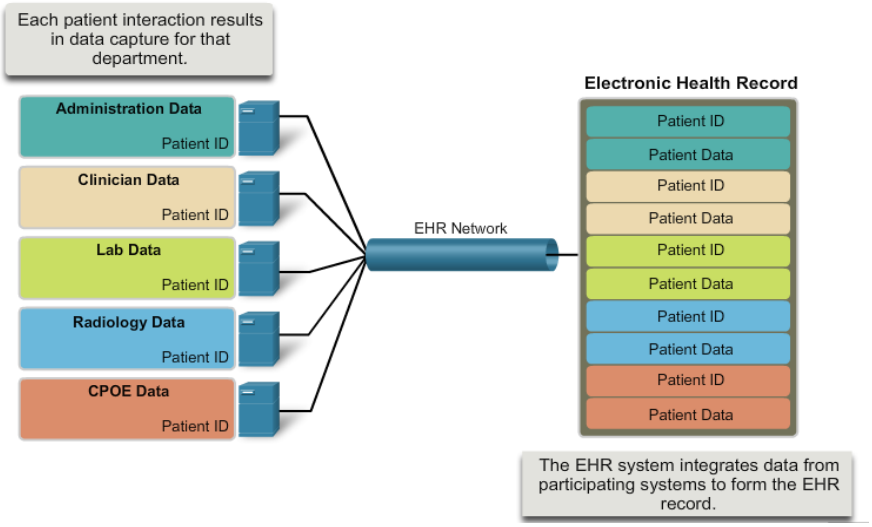

Figure1. EHR Components

Laboratory system components are generally standalone laboratory information systems (LIS) that are dedicated to integrating orders for tests, scheduling, storing results and billing. A radiology information system (RIS), which is used to link patient records to digital radiological images, can be the example for system components. An RIS typically includes patient scheduling, image tracking, and results reporting and is often used in conjunction with picture archiving systems. In addition, pharmacies use a tracking system to manage patient prescriptions, insurance information, and pharmacist notes. This component can link to the CPOE component that physicians use to order patient prescriptions [17]. By implementing an EHR system that integrates each of these components into a single centralized location, clinical data can be collected once and used multiple times. Figure 1 captures the conceptual representation of the EHR components.

2.3.2 Transition to EHRs

Many healthcare organizations, both large and small, may find it expensive to keep up with EHR technologies. For this reason, EHR vendors offer managed services that enable medical providers to have access to HIT services without having to make large investments in equipment and support. In general, there are three different EHR implementation models. In the first model, healthcare provider owns and manages all the equipment and services; they only need the EHR software and support from the EHR vendor. In the second model, vendor owns and manages the equipment installed at the healthcare provider's site. Their responsibilities include setting up, maintaining, and administering the equipment while healthcare provider is responsible for the day-to-day operation of the EHR systems. In the third model, the EHR vendor hosts all EHR applications. The servers that run the applications are located at the EHR vendor's facility. The healthcare organization or the EHR vendor can own these servers, although the vendor maintains both the servers and the applications. Servers are normally kept in server farms and healthcare providers are given a license to access the application over the Internet on demand [12]. The implementation models discussed are shown on Figure 2.

In addition to the implementation models, there are some considerations for successful EHR adoption. According to the Office of National Coordinator for Health Information Technology, there are six EHR implementation steps to achieve to successfully maintain EHR in the healthcare organizations. These steps are: assessing the practice readiness, which is an assessment of the current practice and its goals, needs, and financial and technical readiness; planning the approach, which outlines the practice's EHR implementation plan; selecting a certified EHR vendor; conducting training and implementing an EHR system; achieving meaningful use, which includes successfully attesting to demonstrating meaningful use of EHRs; and lastly, having improvement goals for a continuous quality.

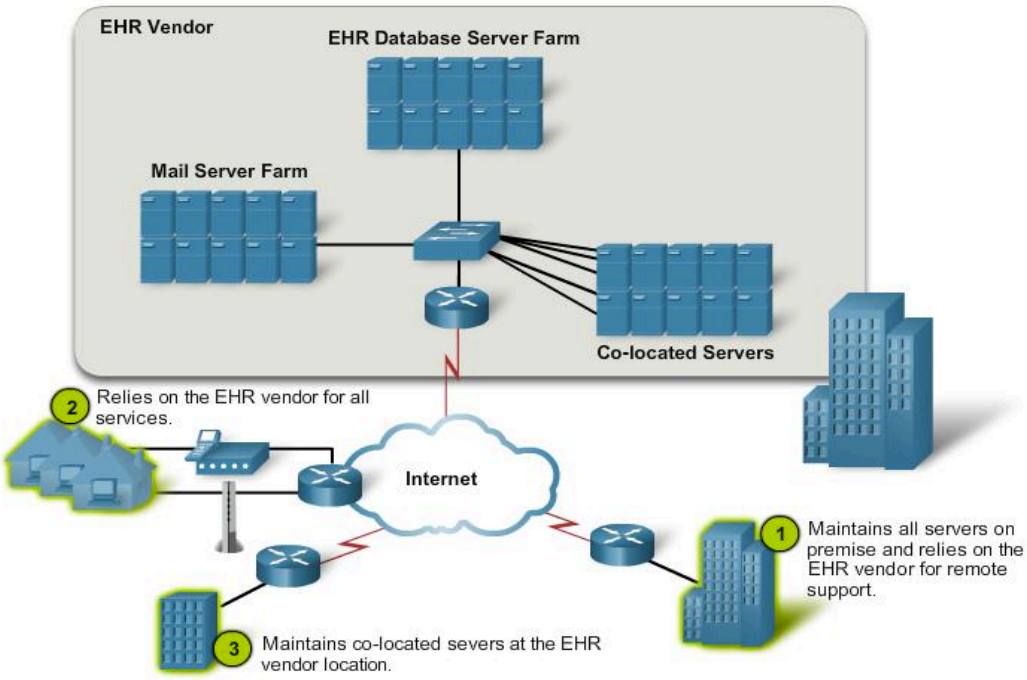

Figure2. EHR Implementation Models

Despite the many benefits that EHR systems offer, physicians in the US have been slow to adopt HIT. According to an EHR adoption study, which is done in 2010, only % 4 of physicians have fully functional electronic medical systems [22]. Healthcare organizations explain these low implementation rates with the insufficient resources or a negative return on investment associated with purchase, implementation, and operation of EHRs [52]. For that reason, the federal government, as part of the American Recovery and Reinvestment Act of 2009 (ARRA), set aside funding to use for incentives, grants, and loans for encouraging medical providers to implement EHR systems. ARRA, also known as the Stimulus Bill, was signed into law to help stimulate the U.S. economy [21]. The funding for the transition to EHRs, which is called the Health Information Technology for Economic and Clinical Health (HITECH) Act, is approximately $19 billion [6]. Under HITECH, eligible health care professionals and hospitals can qualify for Medicare and Medicaid incentive payments when they adopt HIT and use qualified EHR technology [36].

2.3.3 Meaningful Use Priorities for EHR Implementation

There is an increased interest in adopting EHR systems due to the reimbursement incentives authorized by the ARRA. However, to qualify for reimbursement, the EHR system must meet the requirements of the meaningful use priorities. Three main components of meaningful use specified by ARRA are e-prescribing; use of certified EHR technology for electronic exchange of health information to improve quality of health care; and lastly, use of certified EHR technology to provide clinical quality and other measures [21]. In other words, meaningful use refers to the ability of an EHR technology that can be measured significantly in quality and quantity.

According to the Centers for Medicare & Medicaid Services (CMS), the criteria for meaningful use will be staged in three steps. Stage 1, which started in 2011 and will go until 2012, sets the baseline for electronic data capture and information sharing. Stage 2 which is expected to be implemented in 2013; and Stage 3, expected to be implemented in 2015, will continue to expand on this baseline and be developed through future rule making [15]. The incentive payments for organizations, which have implemented EHR systems that meet meaningful use priorities, began in 2011. The healthcare organizations that have not completed these three stages successfully by 2015 will be subject to financial penalties. Therefore, when medical providers are implementing EHR solutions using the government incentives, they need to pay extra attention to meet the requirements of meaningful use priorities [12].

2.4 Healthcare IT Interoperability and Health Information Exchange (HIE)

Interoperability describes the extent to which systems and devices can exchange data, and interpret the shared data. For enabling interoperability between systems and devices, some standards should be in place to provide a common language and a set of expectations [31]. Health Information Exchange (HIE) is defined as the standards and systems used to allow for the transmittal of healthcare

information electronically across multiple healthcare organizations within a region, community, or hospital system [12]. In order to join HIE, a medical provider should adopt an EHR system. US government's overall goal with the incentives for HIT and EHR is to encourage the development of an environment where electronic health information can be exchanged and accessed through the healthcare system [36]. Therefore, HIE is a critical component for the industry's success with HITECH, the meaningful use of HIT, and health reform initiatives [23]. Figure 3 captures the conceptual representation of HIE between healthcare stakeholders.

The terms regional health information organization (RHIO) and HIE are often used interchangeably. RHIO is a group of organizations with a business stake in improving the quality, safety and efficiency of healthcare delivery. RHIOs are the building blocks of the proposed National Health Information Network (NHIN) initiative proposed by the Office of the National Coordinator for Health Information Technology (ONCHIT), while HIE refers to the information exchange practices [28].

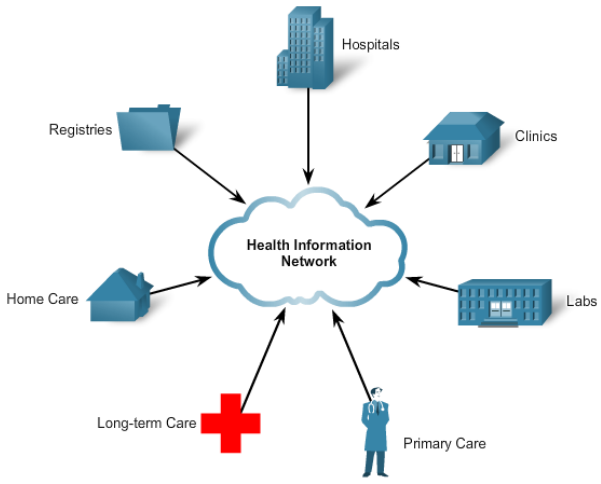

Figure3. Health Information Exchange

HIE offers many benefits to the stakeholders in the delivery of the healthcare. Joining HIE improves care coordination, reduces healthcare disparities, empowers patients, and improves population

health while ensuring adequate privacy and security [36]. More specifically, fully implemented HIE allows medical providers to have comprehensive, high-quality patient information to make the right decision as they have access to the prior patient tests and medical history [36]. Thus, healthcare organizations that exchange information are more efficient and cost effective [12].

Technology is a critical tool in achieving the benefits of HIE [30]. Therefore, when adopting HIE practices, the primary concern is to have adequate technical infrastructure, which is the design and implementation of the architecture, including the hardware, software, applications, network configurations, and other technological aspects that enable data exchange in a secure manner [12]. However, technology alone is not sufficient for successful HIE. Some crucial process and policy decisions must be made in the early stages of HIE development [30]. Therefore, secondarily concern for establishing HIE is business and technical operations which spans all operation and management activities, such as procurement, identifying requirements, process design, functionality development, project management, systems maintenance, change control, program evaluation, and reporting. Furthermore, governance, which is the establishment of accountability measures for the implementation and operation of HIE, is the third concern when adopting HIT. In addition to governance, legal and policy frameworks are the last concerns. These frameworks explain how the HIE is administered, including privacy and security requirements, data-sharing agreements among all business partners, and federal and state laws and regulations [12].

Today, health providers are encountering some roadblocks in the implementation of HIEs. Therefore, many healthcare professionals have raised doubts about sustaining long-term data exchange on a large scale [36]. A survey of healthcare providers, vendors and experts found five issues that constitute the top concerns, which are data sharing, patient consent, standards, complexity costs and competition [48]. For the purpose of this research, only the data sharing and standards will be covered.

Currently, even though the groundwork already in place with incentives and EHR implementations, much of HIE operations still occur in narrow sets of silos. Also, data exchanges through organized state and regional HIEs are uneven in delivery. One of the reasons for the lack of data exchange is the challenge in relation to the standards. Before the exchange of health information can occur, some common standards must be in place to facilitate integration, interoperability, and connectivity among healthcare systems. EHR vendors have been implementing some standards for their EHR products, but, so far, there is a great deal of variation in their implementation methods, which results in systems that cannot interoperate [17]. In order to overcome this issue, the industry should coordinate in the development of the common standards and push for initiatives that improve the chances for interoperability [3].

2.4.1 Interoperability Standards

In order to create interoperable EHRs, standards are needed for clinical vocabularies, healthcare-messaging exchanges (i.e. data transport protocol) and EHR ontologies (i.e., common reference information model, and content and structure of the data entities). In addition, EHR systems must follow appropriate privacy and security standards, especially related to HIPAA regulations [33] [17]. Three main organizations create standards for EHRs: Health Level Seven (HL7), European Committee for Standardization – Technical Committee (CEN TC) 215, and the American Society for Testing and Materials (ASTM) E31. HL7 operates in the US and develops most widely used HIE messaging standards, which are used in communication across health care applications by sending structured and encoded data [17].

The US Department of Health & Human Services (HHS) has many initiatives for developing and adopting information exchange standards. Working with the HL7 in order to define the functions of an

electronic health record and managing the Consolidated Health Informatics (CHI) initiative are the few examples. Through CHI project, HHS is working with other federal agencies to adopt certain private sector standards for government agencies, such as CMS, the VA, DoD, and the Centers for Disease Control and Prevention (CDC). Through this effort, the federal government is hoping to prompt the private sector to standardize clinical and messaging terminology, and logic [33].

When discussing standards in health information technology, it is necessary to be familiar with the concepts of the Clinical Document Architecture (CDA), Continuity of Care Records (CCR), and Continuity of Care Documents (CCD) specifications. CDA is a HL7 document architecture standard that specifies a structure for healthcare documentation so that it can be delivered and shared among systems. CDA does not specify how information is transferred; it focuses on the structure and semantics of the documents. The types of documents that are applicable to CDA include discharge summaries, progress notes, history and physical reports, and prior lab results [50]. CCR is the specification that defines the structure of health information documents. These standards ensure that health information documents contain the most relevant and timely core health information about a patient. CCRs specify sections such as patient demographics, insurance information, diagnosis and symptoms, prescriptions, drug and other allergies, and treatment plans [12]. CCRs are used to generate detailed healthcare summary information or to extract specific data from an EHR and HIEs require the creation and storage of CCR [16]. Lastly, CCD, which is a HL7 standard, is the collaborative effort for representing and mapping CCR data within CDA. The U.S. Health Information Technology Standards Panel has selected the CCD as one of its recommended standards for achieving HIE [32].

2.5 Nationwide Health Information Network (NHIN)

One of the primary goals behind the government's initiatives for encouraging the adoption of EHRs and HIEs is to eventually establish a NHIN [33]. The NHIN is an initiative that establishes mechanisms and conventions for a nationwide electronic health information infrastructure. The NHIN is being developed to provide a secure, nationwide, interoperable health information infrastructure that allows diverse entities to exchange health information electronically [52]. The Office of the National Coordinator (ONC) for Health Information Technology, which is organizationally located within the HHS, sponsors the creation of the NHIN. The core goals of the NHIN include having the ability to find, retrieve and deliver healthcare information within and between HIEs; having ability to support consumer preferences regarding the exchange of health information; supporting secure information exchange; establishing of a common trust agreement that states the obligations and assurances to which all NHIN participants agree; and supporting of harmonized standards, which have been developed by voluntary consensus standards bodies [42]. The conceptual representation of NHIN is shown on Figure 4.

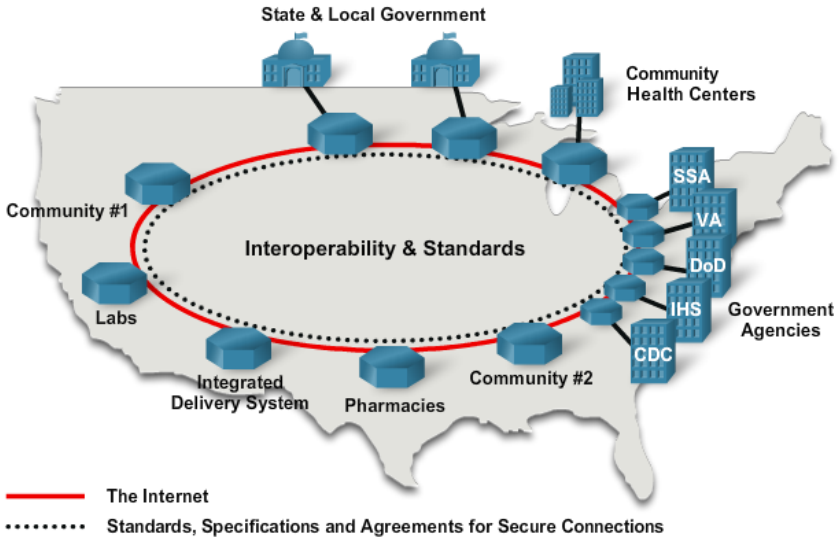

Figure4. Nationwide Health Information Network

The concept of NHIN requires extensive collaboration by a diverse set of stakeholders, especially in the early stages of the implementation [28]. So far, through the Consolidated Health Informatics (CHI) initiative, there has been considerable progress achieved by the Department of Health and Human Services (HHS) with the adoption of interoperability standards and policies, which is the most important component for NHIN establishment [52].

The sharing of patient information through a nationwide network brings some security concerns [33]. Especially, specific requirements regarding access to medical records and breach of such data are the primary concerns; since privacy, disclosure, and breach laws usually differ from state to state. Therefore, exchange of clinical health information across states requires national regulatory guidance, and harmonization of privacy and security regulations. Another issue for interstate exchange of health information is the need to develop national standards for locating and matching patient information across HIE entities and networks as well as across healthcare facilities and organizations in the different states [24].

In the US, Health Insurance Portability and Accountability Act (HIPAA) was the first initiative for ensuring the patient privacy [33]. Then, the HITECH portion of the ARRA expanded the privacy protections in the healthcare delivery. For secure NHINs, these existing regulations must be translated into consistent policies and practices across healthcare entities involved in HIEs, within and across state borders [24].

2.6 Protecting Patient Information: Health Insurance Portability and Accountability Act (HIPAA)

In 1996, The U.S. Congress passed HIPAA to uniform the steps that had to be taken to protect patient privacy. Before HIPAA, rules and regulations varied from state to state, and even from one

healthcare organization to another. HIPAA require HHS to adopt national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. To date, the implementation of HIPAA standards has increased the use of electronic data interchange [31].

2.6.1 HIPAA Titles, Provisions, Covered Entities and Protected Health Information (PHI)

HIPAA is made up of two parts. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II, also known as the Administrative Simplification provisions, enacted federal regulations to protect patient information. Title II HIPAA provisions include the following goals:

- Protecting the confidentiality of an individual's health information,
- Ensuring that health information is properly protected, while allowing the flow of information needed to provide and promote quality healthcare,
- Allowing healthcare providers to become more interconnected, while maintaining the integrity and security of patient information [12].

An organization that must comply with HIPAA is referred to as a covered entity (CE). Providers such as doctors, hospitals, and clinics; health plans that pay for healthcare; healthcare clearinghouses (third parties performing certain financial or administrative transactions); trading partners that exchange health information electronically; and business associates who conduct transactions on behalf of covered entities are considered as covered entities [23].

Under HIPAA, the information that must be secured is called protected health information (PHI). PHI is any information that is individually identifiable, can be related to the individual's past, present, or future physical or mental health; the provision of healthcare to the individual and the past, present, or future payment for healthcare. It is often necessary to de-identify health information for the purpose of

reporting and tracking public health and claim data. To de-identify PHI, all individually identifiable information must be removed [49].

2.6.2 HIPAA Privacy and Security Rules

HIPAA ensures the privacy and security of PHI through two separate rules: the privacy rule and the security rule. Privacy rule mandates the protection and privacy of all health information and defines the authorized uses and disclosures of PHI. According to the privacy rule, safeguards must be put in place to protect health information. In addition, covered entities must reasonably limit uses and disclosures of health information to the minimum necessary to accomplish the intended purposes. Privacy rule applies to written, oral, and electronic types of information. Also, privacy rule states more clearly than the security rule what is actually required to comply [50].

On the other hand, the security rule defines the standards of basic security safeguards to protect electronic protected health information (ePHI). ePHI refers to health information that is created, stored, transmitted, or received electronically. To be covered under the security rule, information must already be in electronic format before transmission. The security rule provides broader protection guidelines, focusing on the confidentiality, integrity, and availability of all electronic information. This allows covered entities more freedom when evaluating and implementing policies and procedures; on the other hand, provides less guidance on what is actually required [49].

2.6.3 Implementing HIPAA Rules in the Healthcare Environment

As healthcare practices implement EHRs and HIEs; they increasingly rely on networks for their core operations and become more vulnerable to attacks. Compromised security in healthcare organizations can have serious consequences as it disrupts critical functions and interfere with a clinician's ability to treat patients [12]. According to HIPAA, the contractual agreement between

business associates (BAs) should ensure that all parties meet all security and privacy requirements. Also, ARRA amends HIPAA to cover business associates (BAs) directly by the requirements of the privacy and security rule [24].

In order to be compliant with HIPAA rules, a covered entity must assign a HIPAA privacy/security officer, which is also called Health Information Officer (HIO). The responsibilities of this officer varies from developing and implementing HIPAA policies and procedures, handling requests from employees (relating to PHI and privacy), managing the complaint process and establishing sanctions for noncompliance, maintaining all compliance records, to responding to investigations by the HHS [12]. According to HIPAA, if any data breach or loss occurs, both CEs and BAs are legally responsible and potentially liable [24].

Chapter 3: Understanding HIT Requirements, Analysis, and Design

3.1 Designing Healthcare IT Networks and Design Considerations for EHRs Solution

Having access to the right information at the right time is critical to deliver quality and cost effective patient care. Therefore, healthcare organizations need an integrated network and advanced technology that provide secure access to the information [12]. This will be the first step for successful implementation of the HIEs, which will eventually lead to the establishment of the NHIN.

When designing and deploying the network architecture, healthcare practices must start by considering the types of applications the network will support initially versus long-term goal. For example, implementing full scale EHR software that must interface with systems outside of the organization for data sharing will require a more complicated infrastructure. Therefore, when installing EHR system, it is important to perform application characterization, which encompasses the understanding of technical requirements and interactions of an application in the network [53]. During the application characterization phase, it is also necessary to gather information about the network and all current applications possible. This includes gathering information from organizational input, network audit and traffic analysis.

Traffic analysis aims to analyze the internal and external traffic flows on a network. The traffic flow of a network utilizing an EHR system is greatly influenced by the implementation model of that system. The implementation model might result in greater internal traffic if the EHR server devices are local, or it might produce greater external traffic if the services are housed remotely [25]. It is important to understand the traffic flow to determine the connection and bandwidth requirements to prevent network congestion and degraded performance [12] [34].

Medical providers are quite concerned about access to patient information. Therefore, when designing a network for HIT applications, every effort must be made to prevent downtime and loss of data. For ensuring this, there is a need to plan for redundancy. There are two types of failures that must be accounted for when planning for redundancy: link failures and device failures. To prevent link failures from causing network downtime, it is necessary to have redundant links between devices. Redundant links are links that are in place for immediate use in the event that a primary link failure occurs. Redundant links should exist in all layers of the network, but especially at locations such as server farms that house patient data. On the other hand, device failures occur when any part of the network or server device fails. A device failure can be more devastating than a link failure because it often affects a larger part of the network and can result in significant data loss [53].

3.1.1 Network Diagramming

Diagramming helps a network designer to evaluate traffic flows and addressing structures as well as identify where topology or equipment changes needed. These diagrams also provide a visual representation of the network and help to understand security picture by identifying information such as the placements of VLANs, access control lists, and other security applications and protocols [53]. When analyzing traffic in the internal network, a network diagram can be utilized in order to show the identified applications and the logical topology of the network, including network devices and how they interconnect. This diagram often includes routers and switches, wireless access points, critical telecommunication equipment (CSU/DSU, modems, etc), firewalls and intrusion detection devices (IDS), management stations, servers and server farms [43].

After the internal LAN is characterized and diagrammed, the network designer should focus on the traffic expectations of remote sites and virtual private networks (VPN). It is also important to

diagram the outgoing traffic flows destined for the Internet and the incoming traffic flows from the Internet to locally provided services. In addition, a diagram for external traffic or WAN should include the information about the central location (healthcare facility), connectivity to EHR vendor sites (for EHR vendor support), connectivity to remote sites and connectivity to business partners [12] [43]. The designer should diagram the WAN connections between the networks and the equipment at each location where WAN terminates. This network diagram illustrates how the information flows from one network to another and helps the designer to locate the problem areas. It can also help the designer assess the need for redundancy and security to facilitate network requirements [53].

3.2 Understanding the Effects of HIT on Network Design

3.2.1 The Network Architecture

Routing and switching infrastructure is the core foundation of any network that enables movement of information and services across the wired and wireless network [53]. In most small-scale physician practices, the logical network architecture includes the network routing and switching foundation for the office, a WLAN, and network security services. But, the size of a medical provider influences the architecture decisions greatly, as network architecture for a large medical practice will require covering a more complicated network [12]. Also, in general, the medical group access router connects with the Internet service provider (ISP) at the network perimeter and this router serves as the gateway to all internal networks [25].

After deciding on the logical network architecture, healthcare organizations need to implement their plan by maintaining the physical network components, systems and software. At this point, it is important to investigate the vendor firms' manufacturer certifications. In order to guide this process, organizations such as the Certification Commission for Health Information Technology (CCHIT) have

created certifications that verify that a manufacturer's systems exceed minimum federal standards requirements, are rated for usability, and are verified to be in successful use at multiple sites [12].

3.2.2 Network Security

Healthcare practices should ensure that the network foundation incorporates with security services, such as port security and quality of service (QoS), to prioritize the most important network services and guarantee consistent performance. In addition, healthcare organizations should use both firewalls and intrusion prevention systems (IPS) to protect their network perimeter. Firewalls act as gatekeepers to a practice's network and as a buffer between it and an "untrusted" network, such as the Internet. Smaller practices with limited IT budgets might prefer to use a multiservice access router with IPS and stateful inspection firewall features, rather than deploying separate firewall and IPS solutions. Larger practices, however, might require the full feature set and scalability of a dedicated firewall [34]. Figure 5 shows the design of a HIT network emphasizing the perimeter security.

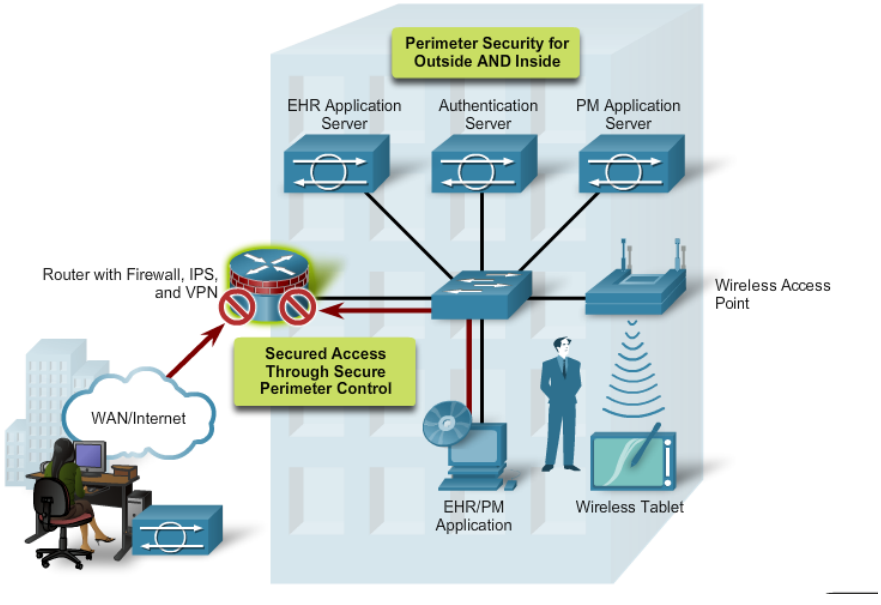

Figure5. Securing the Network Perimeter

Securing access to the office LAN is another security consideration for HIT networks. For most healthcare organizations, the office network contains desktop PCs and servers. Organizations should protect these assets with third-party software solutions, such as antivirus scanners and operating system security patches, and be sure to update security software regularly. In addition, host-based intrusion detection systems (IDS) should reside on network servers, desktops, or other endpoints in order to immediately detect and respond to suspicious operating system activity. Organizations should also implement daily backup systems and all backup storage assets must be protected [25].

Within the routing and switching infrastructure, access controls should be configured to ensure that only authorized devices and traffic are able to access the network. All protocols, including routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP), and switching protocols such as Spanning Tree Protocol (STP), should be properly configured and managed to ensure continuous uptime. Also, healthcare organizations must ensure that WLANs provide the same level of security as wired LANs. The two primary components of WLAN security, authentication and encryption, should be implemented and in use [53].

3.2.3 Designing Server Farms for Healthcare Applications

A locally maintained EHR system relies on the use of one or more servers connected to the access layer in the LAN. As these servers house important patient data, they require additional security, redundancy and management requirements, while increasing the complexity of managing and maintaining them. Therefore, it is a good practice to centralize EHR servers into server farms. A server farm refers to a group of servers that are housed in a single centralized location. Three different types of server farms can be implemented: Internet, Extranet, and Intranet [12] [53].

The users of Internet and internal users utilize Internet server farms. Because of this, Internet farms require additional security controls to prevent external Internet users from using the server farm as a point to access the internal network. There are two types of Internet server farms: dedicated Internet and DMZ Internet service farms. Dedicated Internet server farms support large-scale Internet-facing applications that support the core business function of an organization, such as e-commerce sites. DMZ Internet server farms support Internet-based applications, such as external web servers. On the other hand, intranet server farms are utilized for services only available to the organization's internal users [37]. If medical provider maintains an EHR system in which patient data is stored locally, then intranet server farms are most likely to be implemented.

In order to secure these farms, security measures are typically applied on the server farm edge. From a functional perspective, extranet server farms sit between Internet and intranet server farms. They use web-based applications, but they are only accessed by a select group of trusted external users, such as partners. Therefore, these farms can be used to connect healthcare organizations through the use of HIEs. But, external users should only have access to a subset of the organization's applications to perform the information exchange in a secured manner [12]. Figure 6 captures the conceptual representation of the extranet server farm and where it resides in a greater network design.

While storing the data in server farms offers many benefits, having everything located in a central location can attract malicious attacks. For this reason, server farms must be secured to reduce the chance of such attacks. They also need to be able to handle large amounts of user access and data. Firewalls, IDSs, load balancers, SSL off loaders and caches can improve the security and increase the performance of the server farms. These services should be integrated into the server farm edge in order to filter unwanted traffic prior to gaining access the server farm [25] [34].

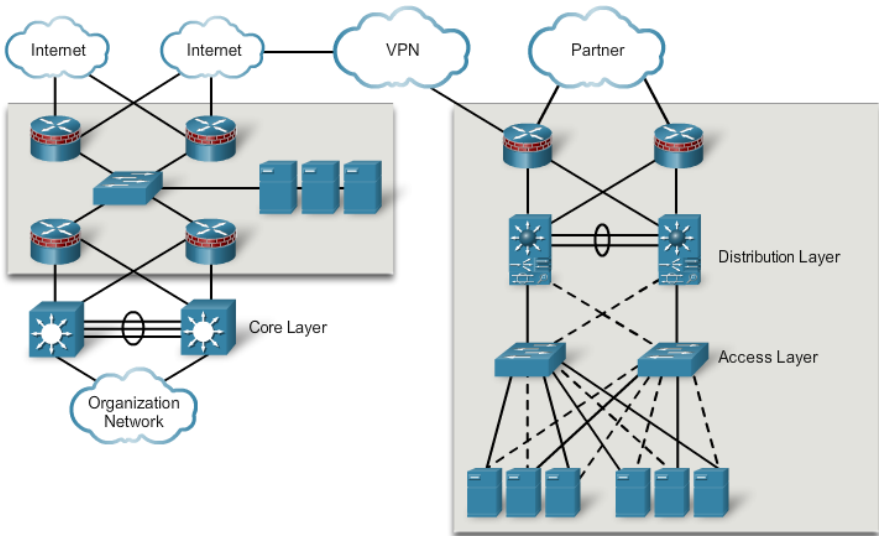

Figure6. Extranet Server Farm

3.3 Securing the HIT Network

In the previous section, a local HIT network design is discussed in detail. Firstly, HIT network requirements gathering methods and design considerations are explored. Secondly, the network architecture, security concerns and server farm design practices analyzed. In addition to these reviews, this part will discuss the integration details of the HIT networks.

3.3.1 Security in the Healthcare Environment

Networks security relates directly to the continuity of a healthcare organization. Network security breaches can disrupt the organization, result in the loss of data, threaten people's privacy, incur legal consequences, and compromise the integrity of the information [25].

One of the first steps to analyze an organization's security needs is to identify likely threats. When identifying threats, it is important to understand the possible vulnerabilities of a system and the consequences if these system vulnerabilities are exploited. For example, an EHR system could be vulnerable to internal system compromise, stolen patient data, insider attack on the system, data input

errors and data center destruction. In general, the high-profile threats are external threats, such as Internet worms and Denial of Service (DoS) attacks [54].

As the information exchange between healthcare organizations will be accomplished with the use of WAN technologies, the appropriate WAN technology should be chosen for the healthcare provider. While making this technology decision, several features of these technologies such as connection types, security, performance, flexibility, costs, complexity and HIPAA compliance should be carefully considered. Since this research aims to provide the best practice applications for securing the information exchange between healthcare entities, the security criteria of these WAN technologies will constitute greater importance in the research findings. In addition, after the WAN technology decision, organizations should take extra precautions and implement various security tools such as firewalls, intrusion detection systems, intrusion prevention systems and access control lists, to the network perimeter. These tools can help to create stronger defense in the event of an attack and stop an intrusion attempt [12].

Securing an internal LAN is just as important as securing the perimeter of a network. Without a secure LAN, users in an organization might not be able to access the network, which can significantly reduce productivity. Many network administrators develop their security strategy from the perimeter of a network and work toward the LAN. Other administrators develop their network security strategy at the LAN and work toward the perimeter. Regardless of the approach, the specific areas that are vital to secure include the network infrastructure are the LAN, the network perimeter to the WAN and the network endpoints [34] [44].

3.3.2 Using Access Control Lists (ACLs)

Access control lists (ACLs) are widely used in network security for mitigating network attacks and controlling network traffic. An ACL can permit specific users access to resources while denying others. For example, if an EHR database server is placed on one VLAN and all non-medical staff on another, an ACL can prevent the non-medical staff from accessing the VLAN that contains the EHR database [34]. Figure 7 illustrates an ACL topology and how it works.

There are two commonly used types of ACLs: standard and extended. Standard ACLs filter packets based solely on that Layer 3 source information (IPv4 or IPv6 addresses). On the other hand, extended ACLs match packets based on Layer 3 and Layer 4 source and destination information (IPv4 or IPv6 addresses as well as TCP and UDP port numbers). Therefore, Extended ACLs give greater flexibility and control over network access than standard ACLs [44].

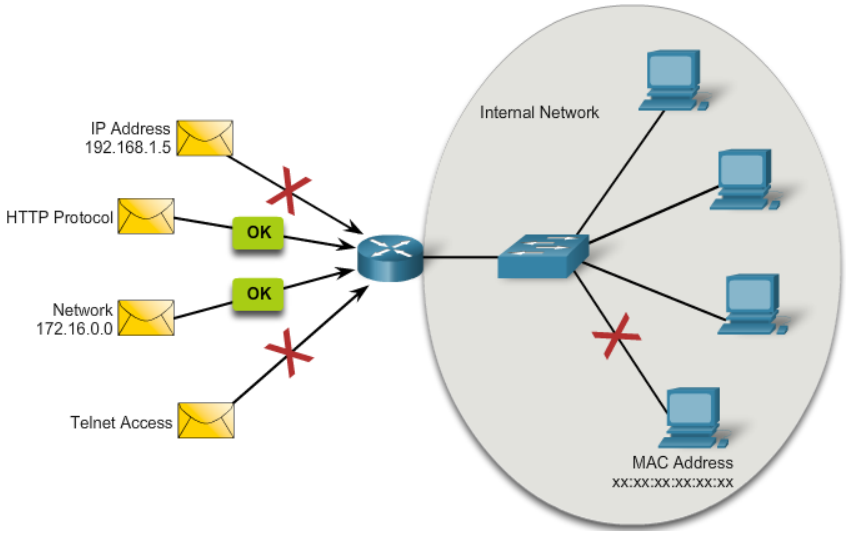

Figure7. ACL Topology

An ACL can filter traffic going through the router, or traffic to and from the router; depending on how it is applied. But, only one ACL per interface, per protocol, per direction is allowed. Also, ACLs

are processed top-down. Once packet meets an ACL test, the ACL processing stops and the packet is either permitted or denied [34].

The direction of traffic through a networking device is specified as inbound or outbound. Inbound traffic refers to traffic that enters into the router. If an inbound ACL is applied, the router compares an incoming packet to the ACL prior to allowing the packet entry into the router for processing. On the other hand, outbound traffic refers to traffic has been processed by the router, meaning that the routing table has been examined to determine where that traffic should be forwarded [44]. Figure 8 represents the working mechanisms of inbound and outbound ACLs.

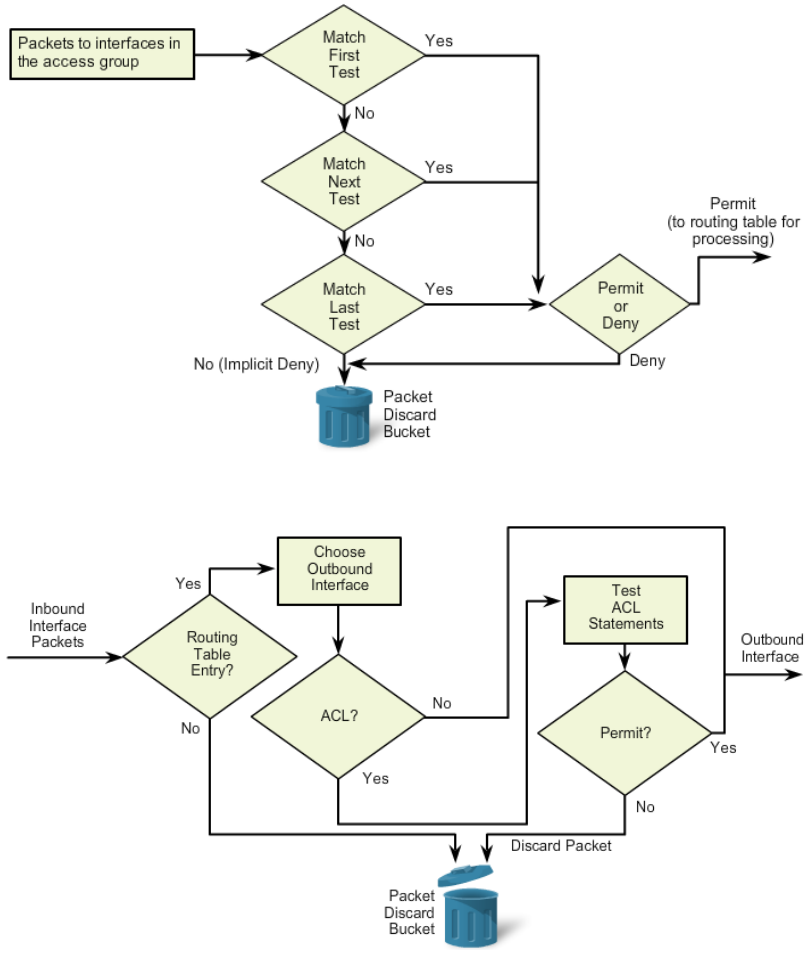

Figure8. Inbound and Outbound ACLs

In addition to flow, it is important to keep the placement of ACLs. Standard ACLs are placed as close to the destination as possible since placing them too close to the source can adversely affect packets by denying all traffic, including valid traffic. Extended ACLs are placed on routers as close to the source as possible. Placing Extended ACLs too far from the source can lead inefficient use of network resources since packets can be sent a long way only to be dropped or denied [25].

ACLs should be configured and applied carefully, because they can slow the transaction process and response time on the network. ACLs are only one aspect of securing a network and should be implemented as part of a greater security design. It is also important to maintain documentation of the ACLs configurations and placements. It provides evidence that the security policy is implemented; ensures that when changes are necessary, all instances of a permit or deny condition are known and evaluated; and assists in troubleshooting problems with access to applications or segments of the network [34].

3.3.3 Securing the Network Perimeter

Although there are many benefits for supporting wide-area communication through the use of WAN technologies and the Internet, these types of connections can leave organizations more vulnerable to attacks. Therefore, it is vital that healthcare organizations secure the perimeter of the network. A firewall is a hardware-based or software-based system that enforces an access control policy between networks and prevents undesirable traffic from entering prescribed areas within a network [34]. Figure 9 captures the conceptual representation of firewalls.

When deployed in HIT networks, firewalls can ensure that only appropriate personnel are allowed access to the provider's network and EHR system. For smaller and mid-sized providers with

limited IT budgets, an integrated router with firewall features can provide a manageable, cost-effective solution. However, larger providers might require the increased capabilities of a dedicated firewall [12].

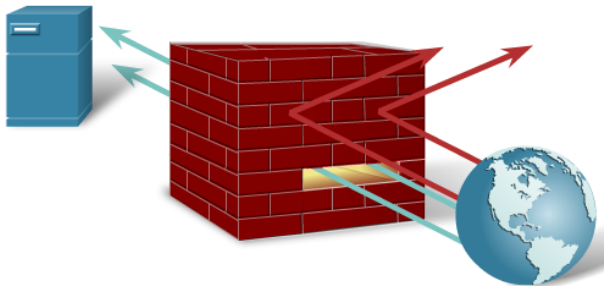

Figure9. Firewalls

Currently, several types of filtering firewalls are available for organizations. Packet- filtering, stateful and application gateway firewalls are the most commonly used on a network perimeter. Application gateway firewall (proxy firewall) filters information at OSI model Layers 3, 4, 5, and 7; and most of the firewall control and filtering is done via software. On the other hand, packet-filtering firewalls work primarily at the Layer 3 and utilize extended ACLs. Since different services rely on specific ports to function, managing these related ports through packet-filtering firewalls provides benefits to a network administrator. Additionally, these firewalls have low impact on the network performance, easy to implement, cost-effective and supported by most of the routers. But, packet filtering is susceptible to IP spoofing and does not filter fragmented packets well. Lastly, since packet filters are stateless, they examine each packet individually rather than in the context of the state of a connection [12] [44].

Stateful firewalls are the most common firewall technologies. Unlike packet filtering, stateful filtering tracks each connection traversing all interfaces of the firewall and confirms that they are valid. For example, they look at the TCP header information such as synchronize (SYN), reset (RST), acknowledgment (ACK) and finish (FIN) to determine the state of the connection. Stateful filtering can

analyze traffic at Layers 3, 4 and 5 while using a state table to keep track of the actual communication process [44]. Stateful firewalls defense against spoofing and DoS attacks. Conversely, stateful firewalls cannot prevent Layer 7 attacks because they do not examine the contents of the HTTP connection. Also, protocols such as UDP and ICMP are not stateful; thus these protocols do not get as much support in this firewall [25]. Figure 10 illustrates stateful packet filtering.

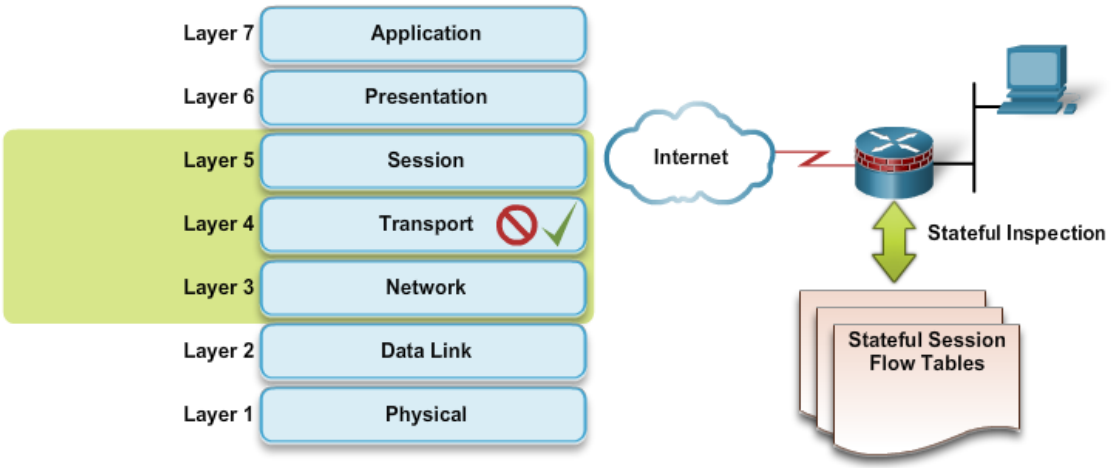

Figure10. Stateful Packet Filtering

When implementing a firewall to the network perimeter, a network administrator should decide on the firewall design according to the security requirements of the network. Some designs are as simple as designating outside and inside networks. The outside network, or public network, is untrusted. The inside network, or private network, is trusted. Traffic from the inside interface is usually permitted to the outside interface with little or no restrictions. Traffic originating from the outside interface, however, is generally blocked from the inside interface. The only traffic from the outside interface that is permitted is response traffic, based on a specific request from a host on the trusted network [43] [44]. Figure 11 illustrates an example firewall implementation.

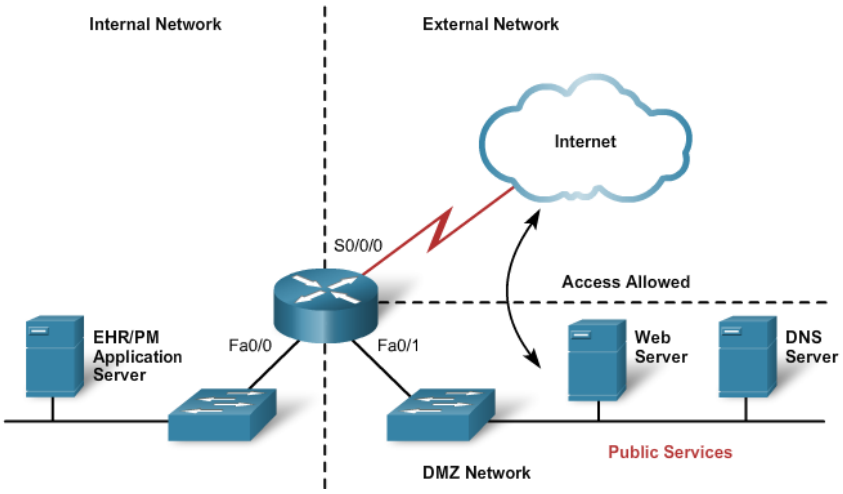

Figure11. Implementing Firewalls

More complicated designs involve three or more interfaces on a firewall or multiple firewalls. In this case, there is typically one public network, one private network, and one demilitarized zone (DMZ). The DMZ acts as a middle stage between the Internet and the healthcare organization's private resources. It allows external users to access public facing services while preventing them from direct access to internal services, such as EHR systems. Many healthcare organizations offer public services such as web-based healthcare portals and patient-scheduling systems that should be placed in a DMZ area for security and control purposes. DMZ should provide service availability and resiliency; prevent intrusions, denial of service (DoS), data leaks, and fraud; ensure user confidentiality, data integrity, and availability of patient information; and protect the EHR server and EHR applications [12] [25].

A single firewall implementation is often referred to as a traditional DMZ. It utilizes a three-interface firewall in which the outside interface connects to the public network, the inside interface connects to the private network, and a DMZ interface connects to the DMZ network. Figure 12 and 13 summarize the working principles of the single and dual firewall implementations.

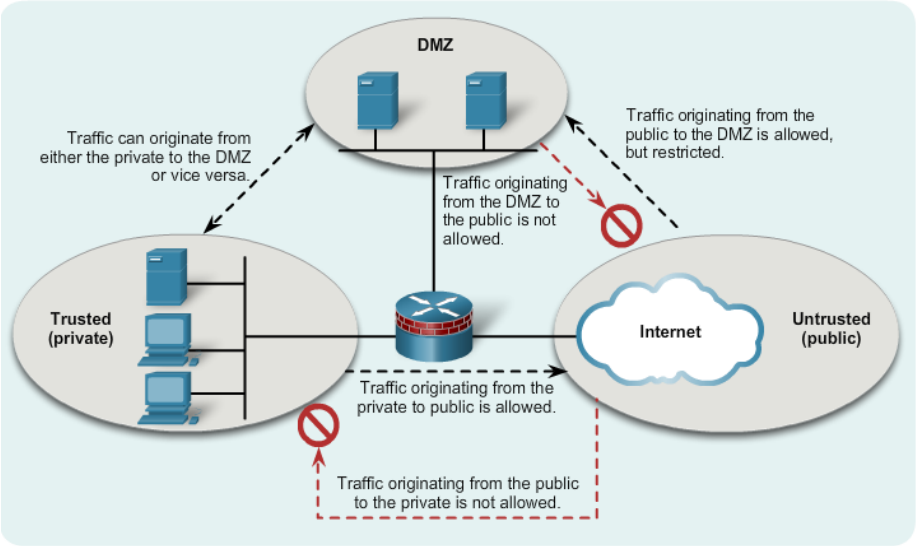

Figure12. Single Firewall Implementation

Dual firewall implementation adds another layer of defense by requiring traffic to travel through two separate firewalls. It reduces the load on each firewall, allows for more granular examinations of traffic and provides redundancy. However, having a second firewall will introduce additional throughput delays, which may negatively impact performance [12] [44].

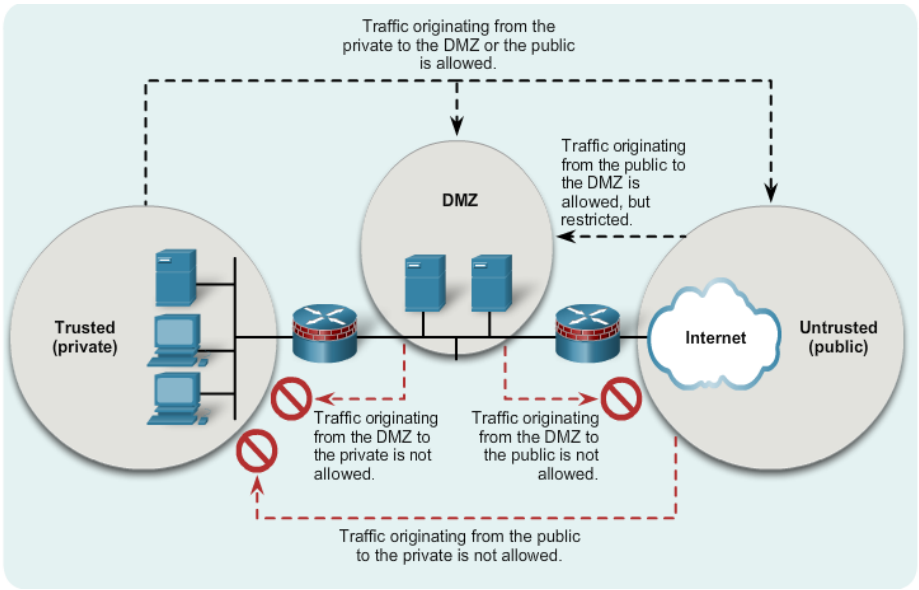

Figure13. Dual Firewall Implementation

While firewalls add a layer of security, they cannot protect against malware and zero-day attacks. To prevent against these types of threats, network traffic must be continuously monitored and analyzed. [25]. An intrusion detection system (IDS) passively monitors the traffic on a network by copying the traffic stream. It compares this stream with known malicious signatures in an offline manner. Thus, IDS does not negatively affect the flow of the forwarded traffic. The disadvantage of using a copy is the delay that is occurred in recognizing an attack and applying a response [25] [34].

Unlike IDS, an intrusion prevention system (IPS) device is implemented in inline mode so that all inbound and outbound traffic must flow through it for processing. It monitors Layer 3 and Layer 4 traffic and analyzes the content of the packets. There are variety of detection technologies, including signature-based and protocol-analysis. This deeper analysis lets the IPS identify, stop, and block attacks that would normally pass through a firewall device. The disadvantage is that a poorly configured IPS solution can negatively affect the flow of the forwarded traffic [25]. IPS device working mechanism is explained in Figure 14.

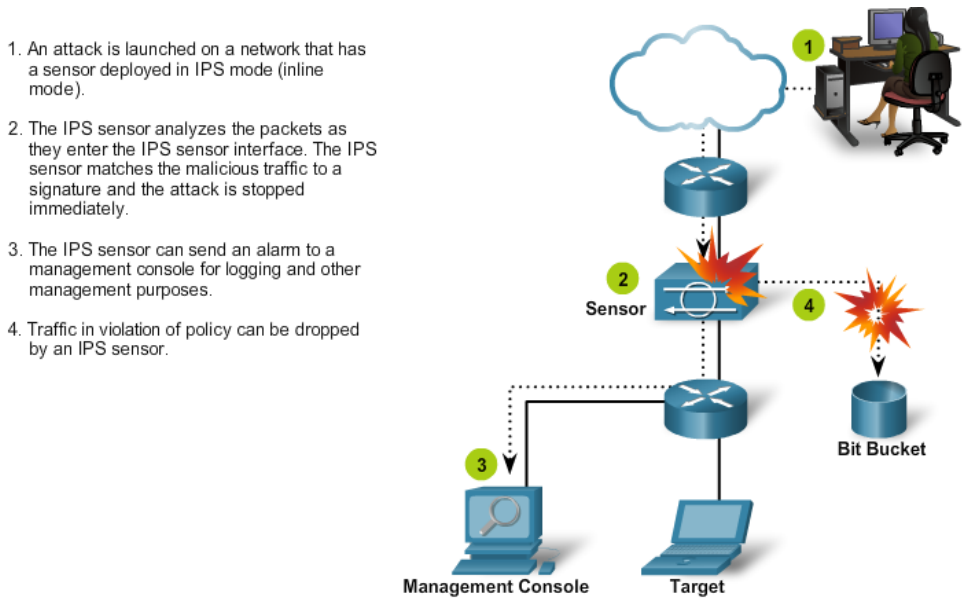

Figure14. Intrusion Prevention System

The protection against viruses and threats requires an end-to-end solution. For this reason, IPS technologies are typically deployed using two implementations: network-based and host-based. Network-based IPS implementations analyze the network looking for malicious activity. Host-based implementations are installed on individual computers using host intrusion prevention system (HIPS) software. HIPS software audits host log files, host file systems, and resources [34]. Figure 15 provides an example of network-based IPS implementation.

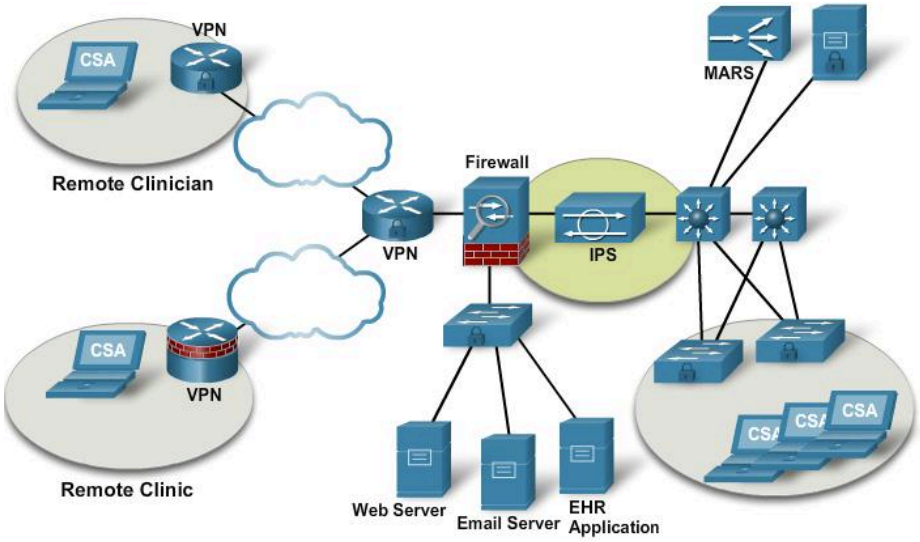

Figure15. Network-Based Implementation

Chapter 4: Development and Implementation Considerations for NHIN

4.1 Designing and Implementing Wide Area Network (WAN) Services

Today, many healthcare organizations use WAN connections to other clinics, hospitals, or suppliers in order to exchange data. WANs use facilities provided by a service provider, such as a telephone or cable company, to connect specific, geographically dispersed organizations or to connect to external services and remote users. For many applications, the Internet is currently being used as an inexpensive alternative to an enterprise WAN. In result, WANs used alone, or with the Internet, allow healthcare organizations, clinicians, and patients to meet their communication needs [12].

The WAN edge is the portion of the network infrastructure that aggregates WAN links that connect geographically distant branch sites to a central site. The objective of the using WAN services is to provide branch site users the same network services as users at the central site. Traditional WAN technologies include leased lines; circuit-switched networks, such as ISDN; packet-switched networks, such as Frame Relay networks; and cell-switched networks, such as ATM networks. Most WAN technologies are leased from a telecommunications service provider [34].

WAN operations focus primarily on Layer 1 and Layer 2 of the Open Systems Interconnection (OSI) model. Layer 1 protocols describe how electrical, mechanical and operational connections to the communications service provider are accomplished. On the other side, The Layer 2 protocols define how data is encapsulated for transmission toward a remote location and the mechanisms for transferring the resulting frames. High-Level Data Link Control (HDLC), Point-to-Point (PPP), Frame Relay, ATM and Multiprotocol Label Switching (MPLS) are the most common methods for Layer 2 encapsulations [53].

When designing and implementing WAN technologies, it is important to know WAN terminology since it is used to describe the physical WAN connections. Different WAN equipment are shown in Figure 16.

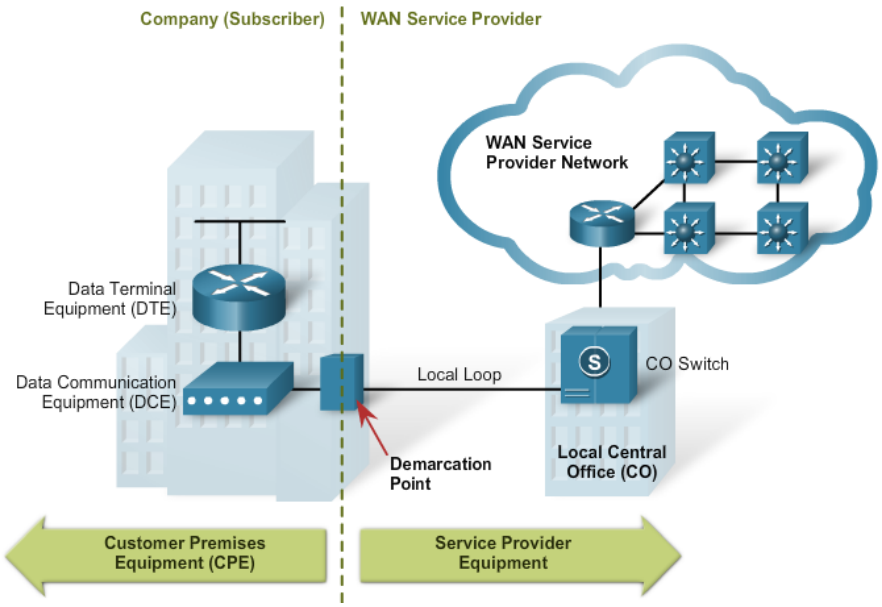

Figure16. WAN Physical Layer Terminology

Customer premises equipment (CPE) refers to the devices and inside wiring located at the premises of the subscriber. The subscriber either owns the CPE or leases the equipment from the service provider. Data communications equipment (DCE) is device that puts data on the local loop. The DCE primarily provides an interface to connect subscribers to a communication link on the WAN cloud. Data terminal equipment (DTE) is a customer device that passes the data from a customer network for transmission over the WAN. The DTE connects to the local loop through the DCE. Demarcation Point is a point established in a building or complex to separate customer equipment (CE) from service provider equipment. The demarcation point is the place where the responsibility for the connection changes from the user to the service provider. Central office (CO) is a local service provider facility or building where local telephone cables link to long-haul, all-digital, fiber-optic communications lines through a system

of switches and other equipment. Local loop is the copper or fiber telephone cable that connects the CPE at the subscriber site to the CO of the service provider [25] [53].

For ensuring the secure HIE, and the establishing the NHIN; it is crucial to have security implementations in the HIT networks. Therefore, when medical providers are implementing WAN services, they should consider information security measures that each technology offers. In this chapter, 5 different WAN technologies, their advantages and disadvantages, successful implementations and information security considerations will be discussed. These WAN technologies are leased lines, frame relay, asynchronous transfer mode (ATM), metro Ethernet and Internet with the use of virtual private networks (VPNs).

4.1.1 Leased Lines

Leased lines are one of the most common WAN technologies in the healthcare environment. With leased lines, each site is connected through a switch at the local telephone company's CO through the local loop and then across the entire network. With this type of configuration, there must be a dedicated, locally leased line to the ISP CO for every connection that a site makes to another geographically dispersed site. For example, if a clinic must make two connections, one to a local hospital and one to a lab; the clinic must purchase two local leased lines to the CO. Depending on the distances; this can be a very expensive investment. The ISP provides the agreed-upon line speed, such as T1 (equivalent to 24 DS0 channels) or ISDN (56 kb/s channels), to the destination. These lines are truly dedicated in that the network provider reserves that line for that clinic's own use. There is no sharing, and the company must pay for the end-to-end circuit regardless of how much bandwidth is actually used [12] [53]. Figure 17 captures the conceptual representation of leased lines.

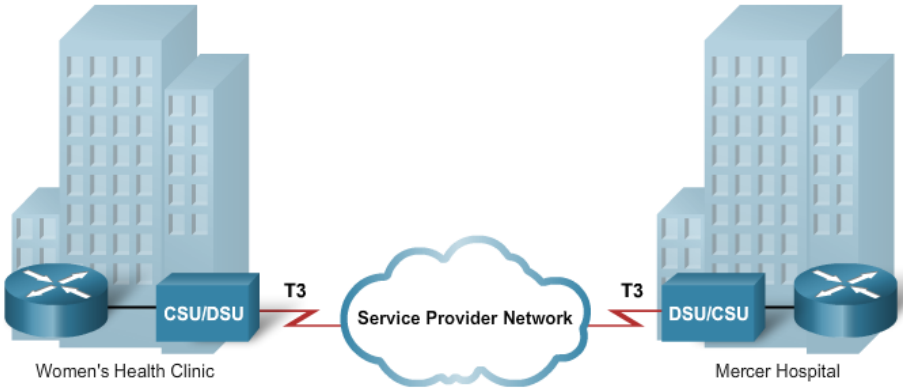

Figure17. Leased Line WAN Topology

In this WAN technology, there are two commonly used methods for Layer 2 encapsulations: High-Level Data Link Control (HDLC) and Point-to-Point Encapsulation (PPP). HDLC is a standard, bit-oriented Data Link Layer encapsulation; and only supports one protocol at a time, such as IP. On the other hand, PPP uses a layered architecture to encapsulate and carry multi-protocol datagrams. Because PPP is standard-based, it enables communication between equipment of different vendors. PPP supports features not available in HDLC such as link quality management, authentication, PPP callback, compression and multilink. Also, PPP has two sub-protocols namely Link Control Protocol and Network Control Protocol. In addition, there are two different types of authentication on a PPP link: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) [25] [53].

Leased lines ensure secure transfer of data. However, they have some disadvantages. As healthcare organizations grow and depend on reliable data transport, this solution become more expensive because organizations must purchase a separate circuit for every new connection. Also, leased line design limits flexibility since connecting new sites requires new circuit installations, which takes considerable time to implement. Finally, as these lines are truly dedicated to the medical provider, they must pay for the end-to-end circuit regardless of how much bandwidth is actually used [12].

4.1.2 Frame Relay

Another WAN technology, frame relay, uses virtual circuits (VCs). A VC is the logical path along an originating frame relay link, through the network, and along a terminating frame relay link to its ultimate destination. In a network with frame relay access, a VC uniquely defines the path between two endpoints, instead of the physical path used by a dedicated connection. This provides greater reliability and resiliency than leased lines since there is more than a single dedicated line [53].

Frame relay provides both cost-effectiveness and flexibility. Customers only pay for the local loop and for the bandwidth they purchase from the network provider. In leased lines technology, customers use dedicated lines provided in increments of 64 kb/s, but frame relay customers can define their virtual circuit needs in far greater granularity. Furthermore, since frame relay shares bandwidth across a larger base of customers, a network provider can service 40 or more 56 kb/s customers over a T1 circuit. Also, frame relay requires less equipment (DSU/CSUs) compared to leased lines [25].

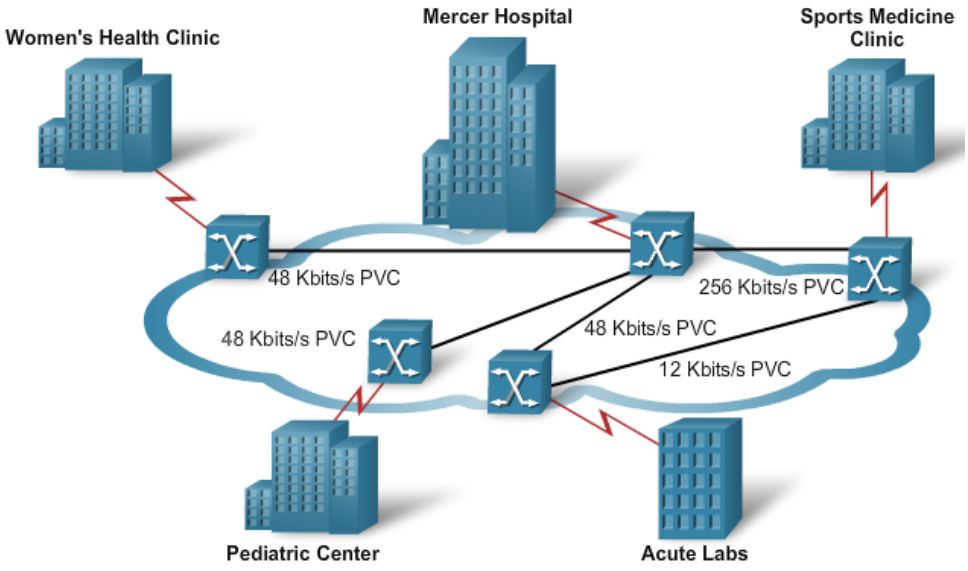

Figure18. Frame Relay WLAN Topology

Frame relay networks transfer data using one of two connection types, switched virtual circuit (SVC) and permanent virtual circuits (PVC). SVC is temporary connection that is created for each data transfer, and then terminated when the data transfer is complete; whereas PVC is preconfigured by the carrier. An example Frame relay topology with the use of PVCs is shown in Figure 18. Frame relay creates a VC by storing input-port to output-port mapping in the memory of each switch; and links one switch to another until a continuous path from one end of the circuit to the other is identified. A VC can pass through any number of intermediate devices located within the frame relay network. A VC is identified by a Layer 2 data-link connection identifier (DLCI), which is assigned by a service provider, typically a telecommunications company [12] [53].

Frame relay providers offer services with guaranteed average data-transfer rates through the provider's packet-switched network. Committed information rate (CIR) specifies the maximum average data rate that the network delivers under normal conditions. Also, to help manage traffic flows in the network, Frame relay implements two mechanisms: forward-explicit congestion notification (FECN) and backward-explicit congestion notification (BECN). A single bit contained in the frame relay frame header controls FECNs and BECNs. Another advantage of frame relay is that one physical interface can support multiple VCs. Therefore, this type of multi-access WAN is less expensive than other dedicated links. However, sharing a single interface can cause problems for distance vector routing protocol updates [25] [53].

4.1.3 Asynchronous Transfer Mode (ATM)

ATM a high speed networking technology used for LAN, MAN, WAN and service provider connections. This technology is built on a cell-based architecture rather than on a frame-based architecture; and it can transfer voice, video and data through private and public networks [25]. Similar

to frame relay, ATM is a connection-oriented technology, and creates and uses end-to-end ATM virtual circuits prior to the transport of any actual data from ATM source. These virtual circuits act like dedicated paths between source and destination, and therefore guarantee bandwidth and QoS. More specifically, ATM offers both PVCs and SVCs; but PVCs are more common with WANs. Also, as with other shared technologies, ATM provides multiple VCs on a single leased-line connection to the network edge [40].

In ATM, data is segmented into fixed-size cells of 53 bytes, instead of variable-size packets. An ATM cell contains a 5-byte ATM header and 48 bytes of ATM payload [7]. During the data transmission, the ATM cells from different or same source are multiplexed together in a cell stream using the asynchronous time division multiplexing technique, which is similar to packet-based multiplexing. The ATM header in each cell contains a connection identifier; thus, the cells belonging the same source (virtual channel), can be uniquely identified within the asynchronously multiplexed flow of cells. Fixed-length cells allow processing to occur in hardware, thereby reducing transit delays. Since voice and video traffic is intolerant of delay; small, fixed-length ATM cells are well suited for carrying this type of traffic [1] [25].

Healthcare organizations can implement an ATM switch on their network in order to have a private use in their backbones as well as establish connections to the service provider's networks. Figure 19 provides an example topology of ATM network. Because the service fee is based on bandwidth used instead of a fixed continual connection, it can be much cheaper compared to leased lines [1]. Also, ATM was designed to be extremely scalable. Therefore, when an organization decides to expand its connections to another site, it can be accomplished easily. In addition, ATM provides data link services with scalable bandwidth from a few megabits per second (Mb/s) to many gigabits per second (Gb/s), which usually run over SONET/SDH Layer 1 links. [7].

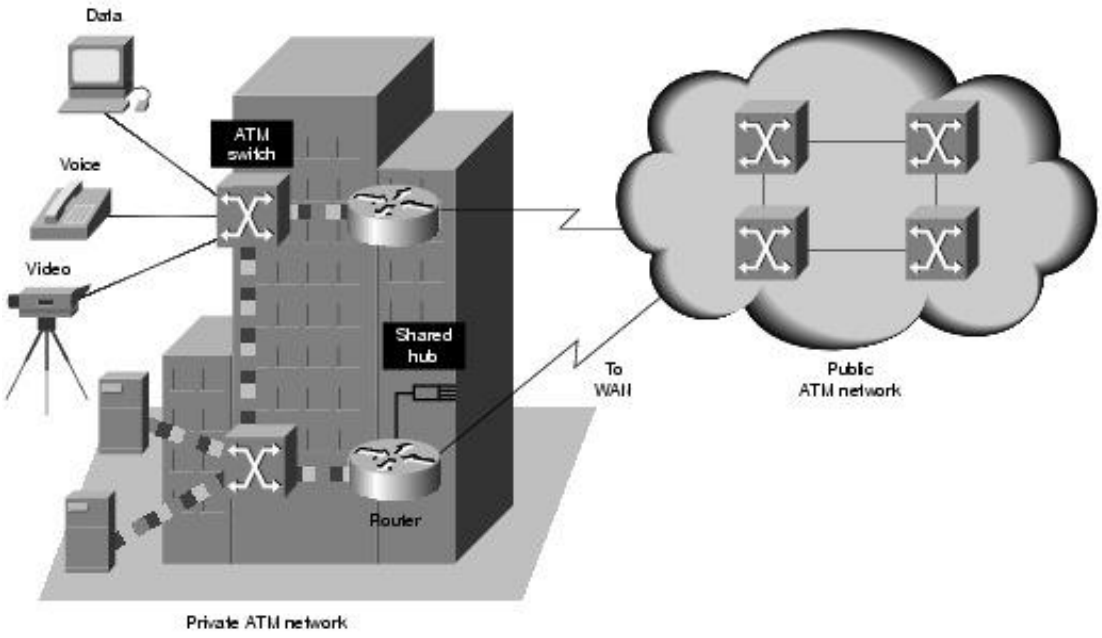

Figure19. ATM Networks

ATM offers flexibility by supporting various interfaces with the help of a Data Service Unit (DSU) device. The DSU device converts the digital signals to a signal type that the ATM network can understand [25]. Another design of ATM network with the DSU device is provided in Figure 20.

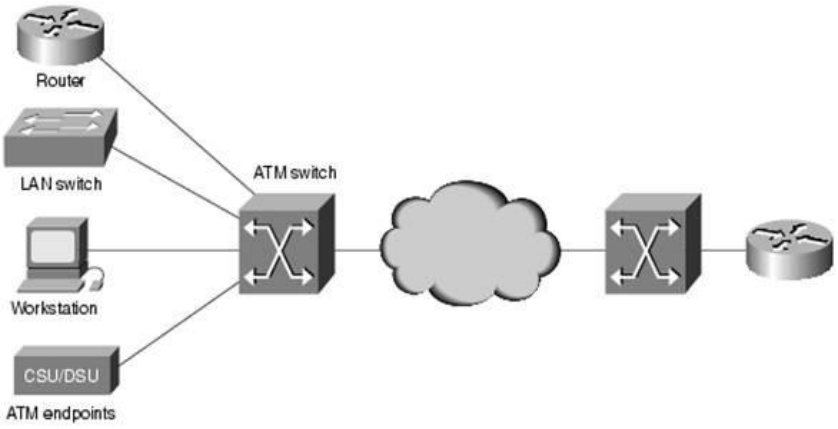

Figure20. ATM Network Design

The regulation of traffic and resource management is an essential aspect of ATM technology. In an ATM network, the effective bandwidth assigned to the ATM virtual circuits is based on a value that is derived from the bandwidth required by the source and the available capacity. This is also referred as "traffic contract" between the ATM traffic (data, voice, or video) and the ATM network [1]. In addition, ATM was the first protocol to provide QoS, and led the computing society to adopt QoS features in other networking technologies [25].

Besides all the advantages listed, ATM technology has also some disadvantages. An ATM cell has at least 5 bytes of overhead for each 48-byte payload. Therefore, a typical ATM circuit needs almost 20 percent more bandwidth than frame relay to carry the same volume of network layer data. Also, fixed, 53-byte cells are less efficient than the bigger frames and packets of other listed WAN technologies. Especially, if the ATM cells are carrying different network layer packets, the overhead will be higher; as the ATM switch must be able to reassemble the packets at the destination. [7] [25].

4.1.4 Metro Ethernet

Metro Ethernet is a carrier Ethernet networking technology that broadens Ethernet to the public networks. It can connect physically dispersed Ethernet LANs that belong to the same organization to a WAN or to the Internet [39]. With the use of IP-processing Ethernet switches, optical and Ethernet technologies, service providers can offer converged voice, data, and video services. By using metro Ethernet services, especially Ethernet VPNs, organizations can extend their Ethernet to the metropolitan area, which enables them to have reliable connections between remote offices and headquarters where they can securely access their applications and data. Ethernet VPNs are very similar to the ATM, private line, or frame relay services [54]. Figure 21 illustrates an example of metro Ethernet network design.

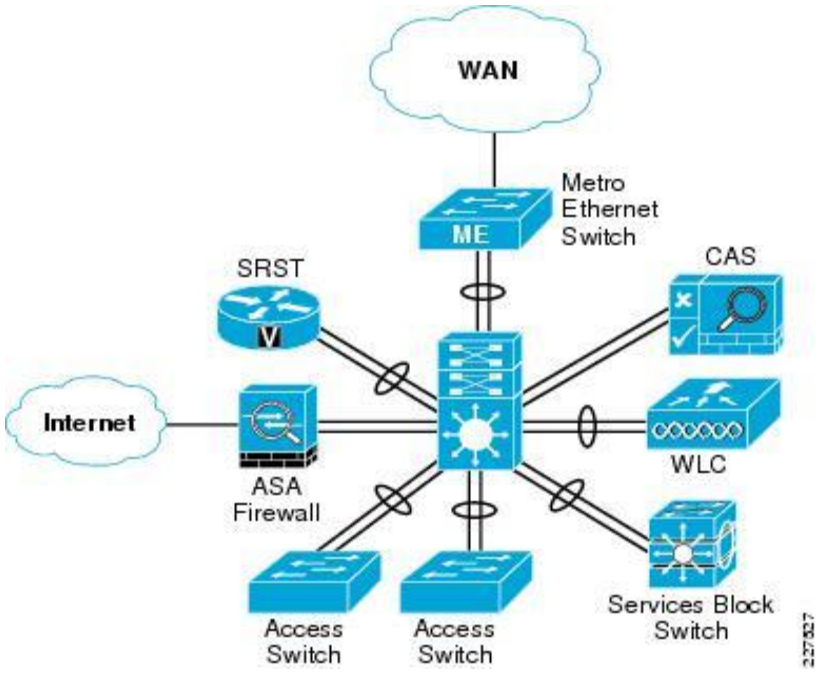

Figure21. Metro Ethernet Network

Metro Ethernet offers many benefits. Firstly, it offers cost-effectiveness, easier administration and network operations as it provides a standard, widely available, well-understood, high bandwidth Layer 2 Ethernet network that can manage data, voice, and video all on the same infrastructure. This functionality enables organizations to inexpensively connect several sites in a metropolitan area to each other and to the Internet [7]. Also, since Ethernet has a broad usage in almost all networking devices, the Ethernet interface itself is inexpensive, due to the lower equipment, service and operational costs. Additionally, Ethernet services usually allow subscribers to add bandwidth more incrementally, which allow purchasing bandwidth as needed, thus controlling the operational costs [45].

Secondly, metro Ethernet connects easily to existing Ethernet LANs, reducing installation cost and time. It offers flexibility by allowing subscribers to maintain their networks in ways that are either more complex or impossible with alternative services. For example, a single Ethernet interface can connect multiple enterprise locations for their Intranet VPNs, connect partners via Extranet VPNs and

provide high speed Internet connection to an ISP [45]. Lastly, it helps organizations to increase productivity since it offers IP applications that are more difficult to implement on point-to-point or frame relay networks [7]. These productivity-enhancing IP applications can be listed as hosted IP communications, VoIP, and streaming and broadcast video. In addition, metro Ethernet provides reliability, scalability and bandwidth management superior to most WAN technologies [39] [45].

In metro Ethernet networks, the Ethernet services are defined from a subscriber-perspective and these services can be supported over a variety of transport technologies and protocols in the MEN like SONET, DWDM, MPLS, GFP, etc. Figure 22 captures an representation of MEN, which has MPLS technology in its core. However, from a subscriber-perspective, the network connection at the subscriber-side is Ethernet since CE attaches to the network at the User-Network Interface (UNI) using a standard 10 Mbps, 100 Mbps, 1 Gbps or 10 Gbps Ethernet interface [35]. In this context, UNI is an Ethernet interface that is the point of demarcation point between the CE and service provider [45].

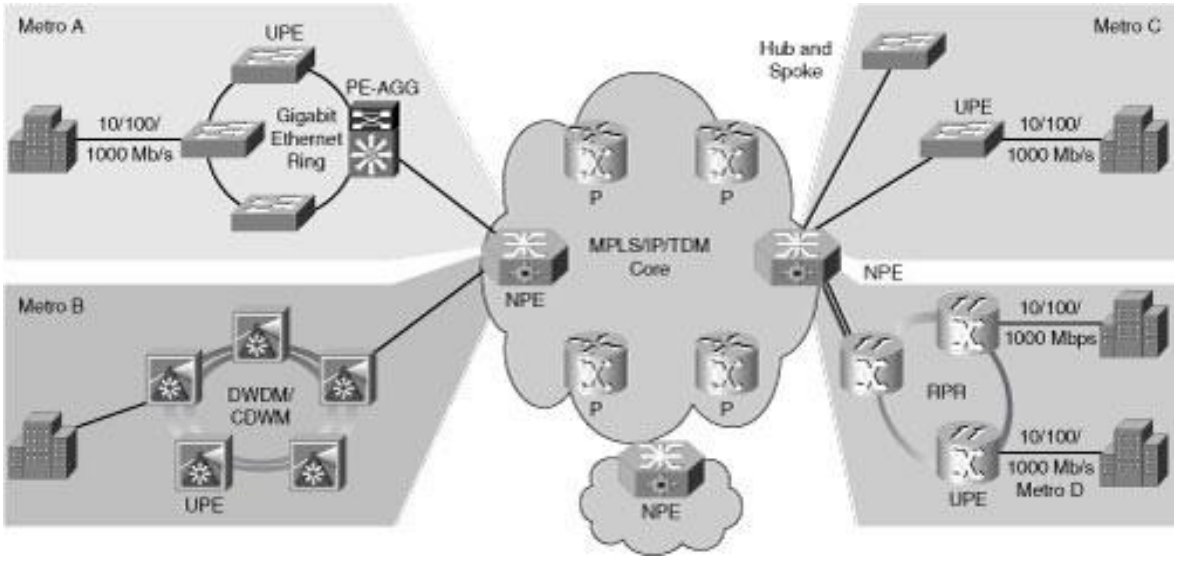

Figure22. Metropolitan Networks and MLPS Technology

One key Ethernet service attribute is the Ethernet Virtual Connection (EVC) and it is defined as an association of two or more UNIs. EVC performs two functions. First, it connects two or more

subscriber sites (UNIs) enabling the transfer of Ethernet service frames between them. Second, it prevents data transfer between subscriber sites that are not part of the same EVC [35]. This capability enables an EVC to provide data privacy and security similar to a frame relay or ATM PVCs. In addition, EVC can be used to construct Layer 2 Private Line or VPN [45].

Metro Ethernet services can be categorized based on the connectivity and service type. Based on the connectivity type, there are two services: point-to-point and multipoint-to-multipoint [35]. Point-to-point is similar to PVC, while multipoint-to-multipoint is similar to a cloud. Based on the service types, metro Ethernet can be considered under two options: Ethernet Line (E-Line) and Ethernet LAN (E-LAN) services. E-Line services provide a point-to-point EVC between two UNIs, similar to the frame relay PVCs or leased lines to interconnect sites. E-LAN services are similar to the Frame Relay and provide multipoint connectivity by connecting two or more UNIs. Each UNI is connected to a multipoint EVC.

When we combine these two categories, four different metro Ethernet services can be generated [45]. These services can be listed as: Ethernet Wire Service (EWS), which is a point-to-point service; Ethernet Relay Service (ERS), which is a VLAN-multiplexed point-to-point service; Ethernet Multipoint Service (EMS), which is a point-to-cloud service; and Ethernet Relay Multipoint Service (ERMS), which is A VLAN-multiplexed point-to-cloud service. One example of EMS and ERMS can be given as Virtual Private LAN Service (VPLS) [54]. In addition, other available Metro Ethernet services can be listed as Ethernet Private Line (EPL); Layer 2 VPN access, which is a Layer 2 access to Multiprotocol Layer Label Switching (MPLS) VPNs; ATM to Ethernet over MPLS; and Frame Relay to Ethernet over MPLS or Ethernet. As it can be understood from the service types, Ethernet packets can be transported over MPLS or Ethernet can be utilized to transport MPLS [35].

Currently, a Metro Ethernet service option with Layer 2 MLPS its in core, which is also called Ethernet over MPLS (EoMPLS), is a preferable WAN service for the healthcare providers for their Internet connections and connections between sites, since it is cheaper than most dedicated circuits and offers greater bandwidth.

4.1.5 Internet with the use of Virtual Private Networks (VPNs)

Many healthcare organizations want to be able to use the benefits of wide-area communication, but do not have the budget to support leased line and frame relay technologies. Additionally, many clinicians prefer the ability to work remotely, while maintaining access to patient files. For these reasons, healthcare organizations are switching to the Internet since it is an easy way to interconnect remote sites. However, the Internet poses security risks to healthcare organizations and their internal networks since it is a public infrastructure. Virtual Private Network (VPN) technology enables organizations to create private networks over the public Internet infrastructure. This helps to ensure confidentiality and security of information.

Healthcare organizations use VPNs to provide a virtual WAN infrastructure that connects branch and home offices, business partner sites, and remote clinicians. Instead of using a dedicated Layer 2 connection, such as leased lines, a VPN uses virtual connections that bundle data and route it across the Internet [12]. Figure 23 presents an example VPN topology.

VPNs offer many benefits while increasing flexibility and productivity in the healthcare settings. With the VPN implementation, remote sites and clinicians can connect securely to the healthcare organization's network, as data on a VPN is encrypted and undecipherable to anyone not entitled to it. VPNs also protect data from unauthorized access as they implement advanced authentication protocols. In addition, VPNs provides cost savings as healthcare organizations can use cost-effective, third party

Internet transport to connect remote clinics and users to the main healthcare organization site. This eliminates expensive dedicated WAN links and modems while offering scalability practices [12] [53].

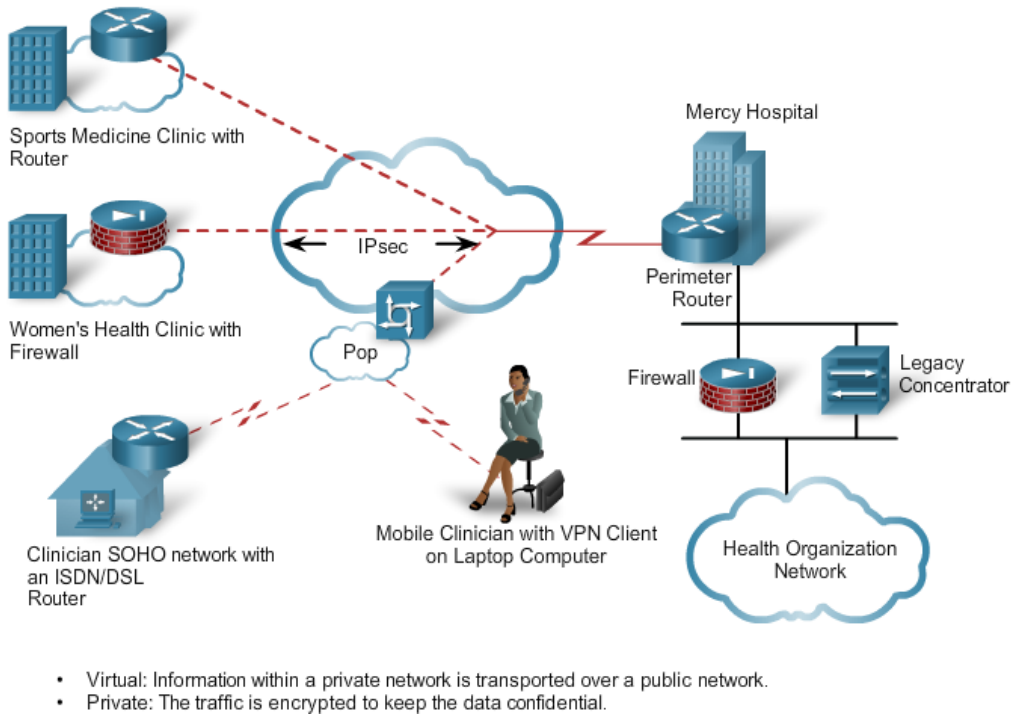

Figure23. VPN Topology

VPNs secure data by encapsulating or encrypting it. Because encapsulation transmits data transparently from network to network through a shared network infrastructure, it is also referred to as tunneling. The tunneling steps are represented in Figure 24. Tunneling encapsulates an entire packet within another packet and sends the new, composite packet over a network. It uses three classes of protocols: passenger, carrier and encapsulating. Passenger protocols are the ones over which the original data was being carried (IPX, AppleTalk, IPv4, IPv6). Carrier protocols are the protocols over which the information is travelling, such as Frame Relay, ATM and MPLS. Lastly, VPN tunnels are created using a number of different encapsulation protocols, such as Generic Routing Encapsulation (GRE), IP

Security (IPsec), Layer 2 Forwarding (L2F) Protocol, Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) [25] [34].

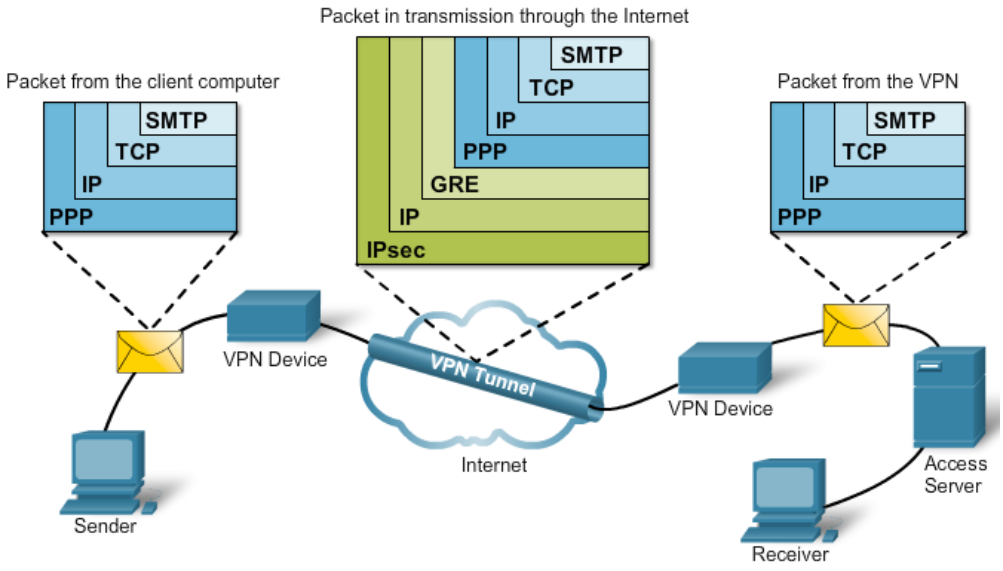

Figure24. VPN Tunneling

Encryption in VPNs ensures that data is not readable by unauthorized persons. For encryption to work, both the sender and the receiver must have the correct key. There are two methods in which keys can be shared: symmetric or asymmetric. With symmetric key encryption, each computer must have the same key and therefore securely exchanging those keys is a challenge. Asymmetric key systems address this challenge because they use two different keys for encryption and decryption. But, asymmetric key systems are extremely slow due to the amount of encryption. Alternatively, Diffie-Hellman (DH) is a secure key exchange method that generates an identical shared secret key on both systems, without them having communicated previously. These keys can be used to symmetrically encrypt traffic between the two systems. DH is commonly used when data is exchanged using an IPsec; data is encrypted on the Internet using either Secure Sockets Layer (SSL) or Transport Layer Security (TLS), or when Secure Shell (SSH) data is exchanged. Additionally, the degree of security provided by any encryption

algorithm depends on the length of the key. The shorter the key, the faster the processing time, but the easier it is to break. Some of the more common encryption algorithms that are used in VPNs include Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) and Rivest, Shamir, and Adleman (RSA) [25] [53] [44].

Another critical VPN function is data integrity. Any data transported over the public Internet, including through VPN tunnels, can potentially be intercepted and modified. Hashed Message Authentication Codes (HMAC) is a data integrity algorithm that guarantees the integrity of the message using a hash value. There are two common HMAC algorithms: HMAC-Message Digest 5 (MD5) and HMAC-Secure Hash Algorithm 1 (SHA-1). HMAC-SHA-1 is considered cryptographically stronger than HMAC-MD5 [53].

Authentication of VPN networks is another consideration. The device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure. There are two methods for peer authentication: Pre-shared key (PSK) and RSA Signature. PSK uses symmetric key algorithms; it is entered into each peer manually and used to authenticate the peer. However, the RSA signature authentication method uses the exchange of digital certificates to authenticate the peers [25].

With the widespread use of the Internet, VPNs have become the logical solution for remote-access connectivity as they provide secure communications with access rights tailored to individual users. For example, VPNs enable clinicians to work from their home office and allow other partner healthcare organizations have access to medical provider's network [12].

There are two primary types of VPNs: site-to-site and remote access. A site-to-site VPN is created when connection devices on both sides of the VPN connection are aware of the VPN configuration in advance. The VPN remains static, and internal hosts have no knowledge that a VPN

exists. Organizations use site-to-site VPNs to connect dispersed locations in the same way that leased lines or frame relay connections are used. Site-to-site VPNs are often implemented as the primary connection between locations. They can also be implemented as a low-cost redundancy solution for backing up other WAN technologies, such as frame relay. In a site-to-site VPN, hosts send and receive TCP/IP traffic through a VPN gateway, which can be a router, firewall or VPN Concentrator. Figure 25 captures the conceptual representation of site-to-site VPN. The VPN gateway is responsible for encapsulating and encrypting outbound traffic and sending it through a VPN tunnel over the Internet to a peer VPN gateway at the target site. Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network [53] [44].

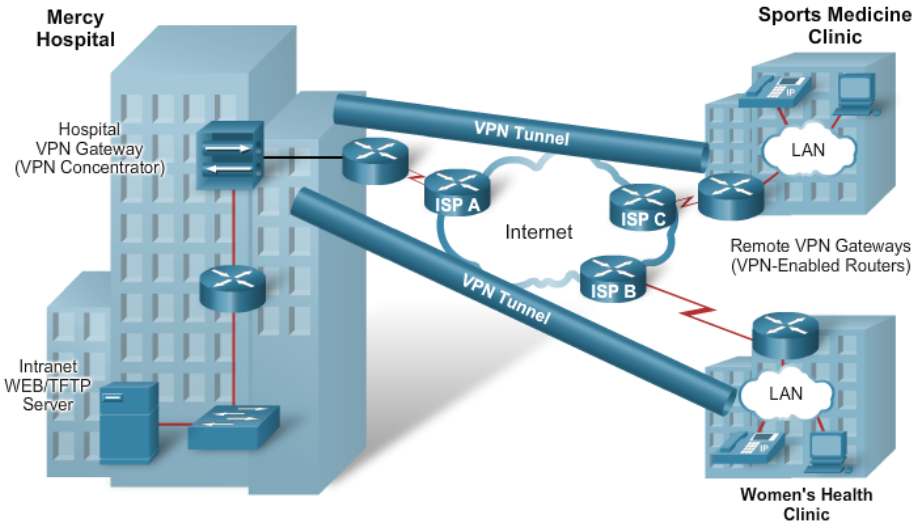

Figure25. Site-to-Site VPN

A remote-access VPN is created when VPN information is not statically set up and there is a need for dynamically changing information. So, this type of VPN can be enabled and disabled. Commonly, remote-access VPNs support the needs of remote clinicians. Many remote clinicians have access to the Internet from their homes and they can establish remote VPNs using broadband connections. Remote-access VPNs support a client- server architecture where a VPN client (remote

host) requires secure access to the enterprise network via a VPN server device at the network edge. In a remote-access VPN, each host typically has VPN client software. Whenever the host tries to send traffic, the VPN client software encapsulates and encrypts that traffic before sending it over the Internet to the VPN gateway at the edge of the target network. Upon receipt, the VPN gateway processes this packet as it does for site-to-site VPNs [25] [53]. Figure 26 illustrates an example topology of remote access VPN.

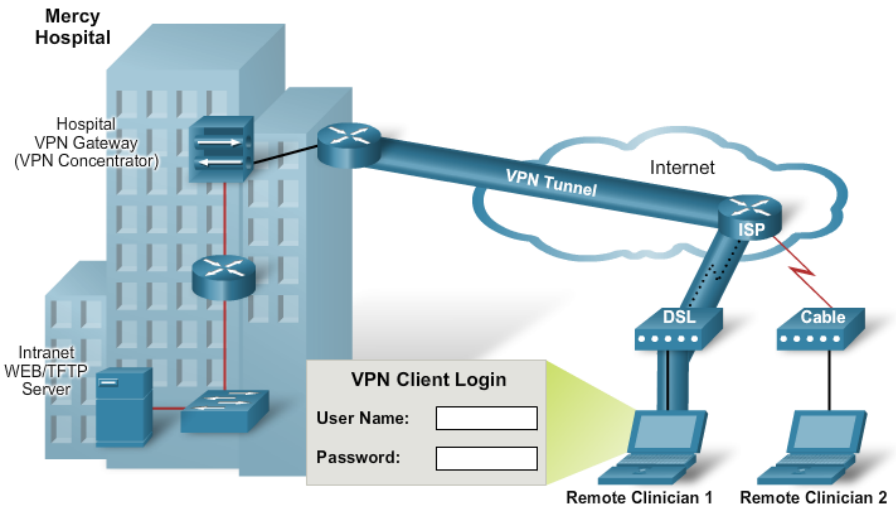

Figure26. Remote Access VPN

One of the primary ways of implementing a site-to-site or remote-access VPN is through the use of IPsec. IPsec is an IETF standard (RFC 2401-2412) that defines how a VPN can be configured using the IP addressing protocol. IPsec is not bound to any specific encryption, authentication, security algorithm, or keying technology; it is a framework of open standards that spells out the rules for secure communications. The administrator chooses the algorithms to implement the security services within that framework. Currently, IPsec uses DES, 3DES, AES, MD5, SHA-1and DH. IPsec works at the Network Layer, protecting and authenticating IP packets between participating IPsec devices [53].

There are two main IPsec framework protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH is used when confidentiality is not required or permitted. AH provides data

authentication and integrity for IP packets passed between two systems. Used alone, the AH protocol provides weak protection. Consequently, it is used with the Encapsulating Security Payload (ESP) protocol to provide data encryption and tamper-aware security features. ESP provides confidentiality and authentication by encrypting the IP packet. IP packet encryption conceals the data and the identities of the source and destination. ESP authenticates the inner IP packet and ESP header. Authentication provides data origin authentication and data integrity [53] [44].

The IPsec framework consists of five building blocks. The first block is the IPsec protocol, either ESP or AH. Second is the type of confidentiality implemented using an encryption algorithm such as DES, 3DES, AES, or SEAL. The third block is the authentication method used to establish integrity and can be implemented using either MD5 or SHA. The fourth one is the shared secret key establishment either pre-shared or digitally signed using RSA. Last block is the DH algorithm group, which establishes how the sharing of key information between peers will occur. There are four separate DH key exchange algorithms to choose from, including DH Group 1 (DH1), DH Group 2 (DH2), DH Group 5 (DH5), and DH Group 7 (DH7) 10] [53]. Figure 27 illustrates the IPSec framework and implementation in the corresponding order.

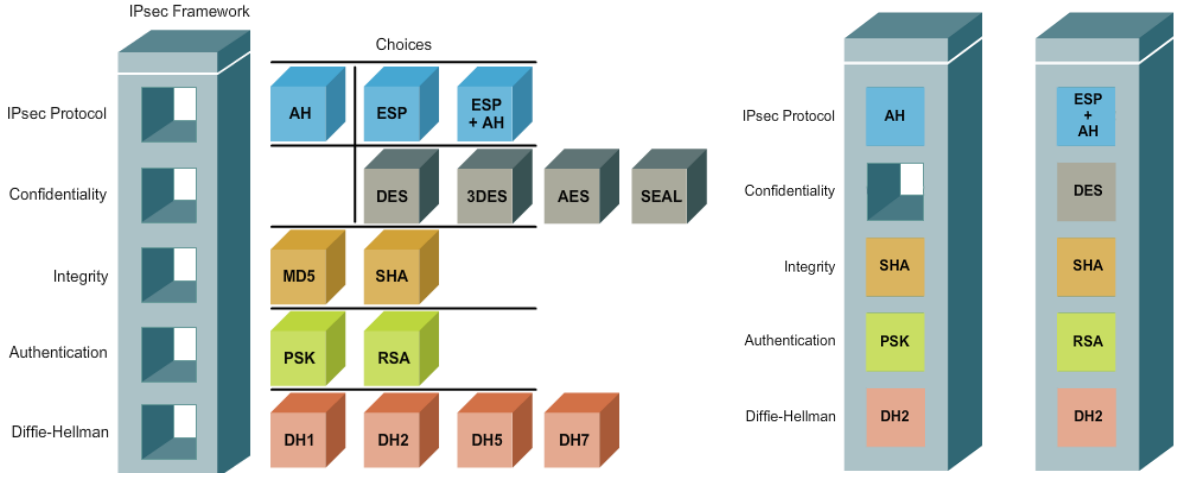

Figure27. IPSec Framework and Implementation

4.1.6 Summary of the WAN Technologies

Table 1-5 below are prepared to summarize five WAN technologies that are widely used today and compare them in a more structured way.

Table 1 Leased Line

LEASED LINE (Dedicated Link or Point-to-Point Link)		
Definition	It is one single link that is pre-established for the purposes of WAN communications between two destinations. It is dedicated, meaning only the destination points can communicate with each other. This link is not shared by any other entities any time.	
Advantages	• These lines are truly dedicated and connect two locations • They are considered very secure as only two locations will be using the same media • Establishing a dedicated link is ideal for two locations that will communicate often will require fast transmission and specific bandwidth	
Disadvantages	• A dedicated line is expensive because organizations have to pay for a dedicated connection for every site they connect and a standard bandwidth, even they do not use. • It is not flexible since when healthcare organizations grow or move to another location, they must purchase a separate circuit for every connection that the organization want to make	
Carrier Technology	• T-carriers are dedicated lines that can carry voice and data information over trunk lines. • The most commonly used T-carriers are T1 lines that provide up to 1.544 Mbps and T3 lines that provide up to 45 Mbps.	
Layer 2 (Data Link) Encapsulation Protocols	High-Level Data Link Control (HDLC)	Point-to-Point Link Protocol (PPP)
	• standard bit-oriented encapsulation • uses synchronous serial transmission, which provides error-free communication between two points • provides flow control and error control through the use of acknowledgments • only supports one protocol at a time (IP) • vendors have developed their own parameters within their versions of HDLC, which has resulted interoperability issues	• uses a layered architecture to encapsulate and carry multi-protocol datagrams • enables communication between equipment of different vendors • provides link quality management • supports multiple protocols at a time • features supported include: authentication, PPP callback, compression and multilink • two authentication methods are supported: PAP and CHAP • has two sub-protocols
PPP Sub-Protocols	Link Control Protocol: • establishes, maintains, and terminates the point-to-point link. • supports authentication, compression, and error detection	Network Control Protocol: • encapsulates multiple network layer protocols, so that they operate on the same communications link

Table 2 Frame Relay

FRAME RELAY		
Definition	It is a high performance WAN solution that uses packet switching technology, which works over the public networks. Frame Relay let multiple companies and networks share the same WAN media.	
Advantages	• Whereas point-to-point links have a cost based on the distance between the endpoints, the frame relay cost is based on the amount of bandwidth used. • Since the infrastructure is shared, if one subscriber is not using the bandwidth, it is available for others to use. • Because several organizations use the same media and devices (routers and switches), costs can be greatly reduced per healthcare provider compared to dedicated links. • It gives companies much more flexibility than leased lines as it offers an easier implementation. • It also provides greater reliability and resiliency than single dedicated lines because one physical interface can support multiple VCs, which provides multiple dedicated lines. • The simplified handling of frames leads to reduced latency.	
Disadvantages	• Frame relay does not implement error or flow control. • When traffic levels increase, the available bandwidth in the frame relay cloud decreases. Therefore, if subscribers want to ensure a certain bandwidth, they need to pay a higher committed rate. • Sharing a single interface can cause problems for distance vector routing protocol updates.	
Carrier Technology	• Frame relay offers data rates up to 4 Mbps. • In a dedicated-line model, customers use dedicated lines provided in increments of 64 kb/s, but frame relay customers can define their virtual circuit needs in far greater granularity, often in increments as small as 4 kb/s. • Since frame relay shares bandwidth across a larger base of customers, a network provider can service 40 or more 56 kb/s customers over a T1 circuit.	
Connection Types for Data Transfer (Virtual Circuits)	Switched Virtual Circuit (SVC)	Permanent Virtual Circuits (PVC)
	• A temporary connection that is created for each data transfer, and then terminated when the data transfer is complete.	• Permanent connection preconfigured by the carrier.
Frame Relay Characteristics	• A VC is identified by a Layer 2 data-link connection identifier (DLCI), which is assigned by the Frame Relay service provider. A DLCI identifies a VC to the equipment at an endpoint. • After establishing DLCI, Inverse Address Resolution Protocol (Inverse ARP) provides a mechanism to create dynamic DLCI-to-Layer 3 address maps. • Frame relay providers offer services with guaranteed average data-transfer rates and committed information rate (CIR), which specifies the maximum average data rate that the network delivers under normal conditions. • A CIR is assigned to each DLCI that is carried on the local loop. If the location attempts to send data at a faster rate than the CIR, the provider network flags some frames with a discard eligible (DE). If there is congestion, it discards any frames marked with the DE. • Many inexpensive Frame Relay services are based on a CIR of zero. A zero CIR means that every frame is a DE frame, and the network can throw any frame away when there is congestion. Since there is no guarantee of service with a CIR set to zero, mission-critical data, such as EHR system data should not be relay on so these services. • Frame Relay implements two mechanisms to help manage traffic flows in the network: Forward-explicit congestion notification (FECN) and Backward-explicit congestion notification (BECN).	

Table 3 Asynchronous Transfer Mode (ATM)

ASYNCHRONOUS TRANSFER MODE (ATM)	
Definition	ATM technology can transfer voice, video and data through private and public networks. It is built on a cell-switching method rather than being packet-switch method. ATM is a high speed networking technology used for LAN, MAN, WAN and service provider connections.
Advantages	• ATM is a high-bandwidth technology that usually has low overhead and low delay. • Data is segmented into fixed-size cells of 53 bytes, instead of variable-size packets • Small, fixed-length cells are well suited for carrying voice and video traffic, because this traffic is intolerant of delay. Video and voice traffic do not have to wait for a larger data packet to be transmitted. • ATM allows multiple VCs on a single leased-line connection to the network edge. • In combination with SVC/PVC capabilities of ATM, the same packet size segmentation provides more efficient and faster use of communication paths. Because with the use of VCs, the path is established before the data transfer, all the packets are routed to the same path and as a result, reassembly overhead of the packets is reduced significantly. • It supports various interfaces to provide flexibility and use of different QoS practices.
Disadvantages	• The 53-byte is less efficient than the bigger frames and packets of frame relay. • The ATM cell has at least 5 bytes of overhead for each 48-byte payload. When the cell is carrying segmented network layer packets, the overhead is higher, because the ATM switch must be able to reassemble the packets at the destination. • A typical ATM line needs almost 20 percent more bandwidth than frame relay to carry the same volume of network layer data.
Carrier Technology	• ATM was designed to be extremely scalable. It can support link speeds of T1/E1 to OC-12 (622 Mbps) and higher.
Connection Types for Data Transfer (Virtual Circuits)	• ATM offers both PVCs and SVCs, although PVCs are more common with WANs. • These VCs can guarantee bandwidth and QoS. Therefore, ATM is a good carrier for voice and video transmission.
ATM Characteristics	• ATM is used by carriers and service providers and makes up part of the core technology of the Internet. It can also be used for a company's private use in backbones and connections to the service provider's networks. • Like frame relay, it is a connection-oriented switching technology and uses a fixed channel. • ATM cells are always fixed length of 53 bytes. The ATM cell contains a 5-byte ATM header, followed by 48 bytes of ATM payload. • ATM sets up a fixed channel for all data to transfer through during a transmission. The fixed channels are preprogrammed into the switches along that particular communication path. • ATM was the first protocol to provide true QoS, but later, QoS integrated into other technologies.

Table 4 Metro Ethernet

METRO ETHERNET	
Definition	Metro Ethernet Networks broaden Ethernet to the public networks run by telecommunications companies. IP-aware Ethernet switches enable service providers to offer enterprises converged network services. This technology enables organizations to inexpensively connect LANs and individual end users to a WAN or to the Internet.
Advantages	• Due to its broad usage in networking products, the Ethernet interface itself is inexpensive. Ethernet services also offer lower equipment, service and operational costs, compared to competing services. • Metro Ethernet provides a switched, high bandwidth Layer 2 network that can manage data, voice, and video all on the same infrastructure. This increases bandwidth and eliminates expensive conversions to ATM and Frame Relay. • Since Ethernet services are provided over a standard, widely available and well-understood Ethernet interface, the network operations, administration and management is simplified in MENs. • Metro Ethernet connects easily to existing Ethernet LANs, reducing installation cost and time. • It enables businesses to take advantage of productivity-enhancing IP applications that are difficult to implement on Frame Relay networks, such as IP communications, VoIP, streaming video. • Many Ethernet services allow subscribers to add bandwidth in smaller increments (1 Mbps). • It offers reliability, scalability, performance guarantees and greater bandwidth management.
Disadvantages	• Metro Ethernet does not have QoS and other traffic-prioritization capabilities.
Carrier Technology	• Standard Ethernet speeds of 10 Mbps, 100 Mbps, 1 Gbps and 10 Gbps are supported in Metro Ethernet. • Physical Media includes 10BaseT, 100BaseT and 1000BaseSX.
Connection for Data Transfer (Ethernet Virtual Connection)	• An EVC is defined as the association of two or more User Network Interfaces (UNIs), where the UNI is a standard Ethernet interface that is the point of demarcation between the Customer Equipment and service provider's MEN. • It connects two or more UNIs enabling the transfer of Ethernet service frames between them. • It also prevents data transfer between subscriber sites that are not part of the same EVC. This capability enables an EVC to provide data privacy and security similar to a Frame Relay or ATM PVC. • Based on these characteristics, an EVC can be used to construct Layer 2 Private Line or Virtual Private Network (VPN). • There are two types of EVCs: point-to-point and multipoint-to-multipoint.
Metro Ethernet Characteristics	• There are two Ethernet service types: Ethernet Line (E-Line) Service and Ethernet LAN (E-LAN) Service. • E-Line Service provides a point-to-point EVC between two UNIs, which is analogous to Frame Relay PVCs or private leased lines to interconnect sites. Such services have some characteristics such as minimal Frame Delay, Frame Jitter and Frame Loss and no Service Multiplexing. • Even though E-Line Service can be used to construct services similar to Frame Relay or private lines, the Ethernet bandwidth range and connectivity options is much greater in E-Line Services. • E-LAN Service provides multipoint connectivity by connecting two or more UNIs. Each UNI is connected to a multipoint EVC. As new UNIs are added, they get connected to the same multipoint EVC, which simplifies provisioning and service activation. • An E-LAN service can be used to create a broad range of services such as Private LAN and Virtual Private LAN services. • An E-LAN service allows UNI to communicate with all other UNIs, whereas an E-Line Service requires separate EVCs to all UNIs. Therefore, an E-LAN Service can interconnect large number of sites with less complexity than point-to-point network technologies, such as Frame Relay or ATM. • E-Line Service and E-LAN Services can provide symmetrical bandwidth for data sent in either direction, with no performance assurances. • They also may provide a Committed Information Rate (CIR) and associated Committed Burst Size (CBS), Excess Information Rate (EIR) and associated Excess Burst Size (EBS) and delay, jitter, and loss performance assurances between two different speed UNIs.

Table 5 Internet with the use of Virtual Private Network (VPN)

INTERNET with the use of VIRTUAL PRIVATE NETWORK (VPN)	
Definition	A virtual private network (VPN) is a secure, private connection through a public network or otherwise unsecure environment. It is a private connection, because the encryption and tunneling protocols are used to ensure the confidentiality and integrity of the data in transit. Today, the Internet has become an attractive way to interconnect remote sites as VPN technology enables organizations to create private networks over the public Internet infrastructure.
Advantages	• Healthcare organizations can use cost-effective, third party Internet transport to connect remote clinics and users to the main healthcare organization site. This eliminates expensive dedicated WAN links and modem banks. • Data on a VPN is encrypted and undecipherable to anyone not entitled to it. • Advance authentication protocols protect data from unauthorized access. • Instead of using a dedicated Layer 2 connection, such as a leased line, a VPN uses virtual connections that bundle data and safely route it across the Internet. • Healthcare organizations using VPNs benefit from increased flexibility and productivity since remote sites and clinicians can connect securely to the healthcare organization's network. • VPNs use the Internet infrastructure within ISPs and carriers, making it easy for organizations to add new users. Organizations are able to add large amounts of capacity without adding significant infrastructure.
Disadvantages	• VPN tunnels are created using a number of different encapsulation protocols and not all protocols offer the same level of security. • IPSec cannot transmit multicast/broadcast traffic; therefore, some routing protocols (EIGRP or OSPF) could not be transmitted in an IPSec tunnel making scalability of multiple site-to-site VPNs unmanageable. (Solution: Dynamic Multipoint VPNs)
Tunneling (Encapsulation) Protocols	• Generic Routing Encapsulation (GRE): provides a specific pathway across the shared WAN. Tunnels do not provide true confidentiality (like encryption does) but can carry encrypted traffic. • IP Security (IPsec): acts at the Network Layer, protecting and authenticating IP packets between participating IPsec devices. IPsec is not bound to any specific encryption, authentication, security algorithms, or keying technology, it is a framework of open standards. • Layer 2 Forwarding (L2F) Protocol: developed by Cisco that supports the creation of secure virtual private dialup networks over the Internet by tunneling Layer 2 frames. • Point-to-Point Tunneling Protocol (PPTP): was developed by Microsoft, widely deployed in Windows client software to create VPNs across TCP/IP networks. • Layer 2 Tunneling Protocol (L2TP): is an IETF standard that incorporates the best attributes of PPTP and L2F. L2TP is used to tunnel Point-Point Protocol (PPP) through a public network, such as the Internet, using IP.
Encryption Protocols	• Data Encryption Standard (DES): developed by IBM, DES uses a 56-bit key, ensuring high-performance encryption. DES is a symmetric key cryptosystem. • Triple DES (3DES): a variant of DES that encrypts with one key, decrypts with a different key, and then encrypts one final time with another key. 3DES provides significantly more strength to the encryption process. • Advanced Encryption Standard (AES): The National Institute of Standards and Technology (NIST) adopted AES to replace the existing DES encryption in cryptographic devices. AES provides stronger security than DES and is computationally more efficient than 3DES. • Rivest, Shamir, and Adleman (RSA): an asymmetrical key cryptosystem.

Data Integrity and Authentication Algorithms/Methods	• Hashed Message Authentication Codes (HMAC): a data integrity algorithm that guarantees the integrity of the message using a hash value. There are two common HMAC algorithms:
	  ○ HMAC-Message Digest 5 (MD5): Uses a 128-bit shared secret key.
	  ○ HMAC-Secure Hash Algorithm 1 (SHA-1) - Uses a 160-bit secret key. HMAC-SHA-1 is considered cryptographically stronger than HMAC-MD5. It is recommended when slightly superior security is important.
	• There are two peer authentication methods.
	  ○ Pre-shared key (PSK): The pre-shared key (PSK) authentication method uses a secret key that is shared between the two parties using a secure channel before it needs to be used. PSKs use symmetric key cryptographic algorithms.
	  ○ RSA signature: The RSA signature authentication method uses the exchange of digital certificates to authenticate the peers.

VPN Characteristics	• VPNs secure data by encapsulating or encrypting the data. Most VPNs can do both. Encapsulation is also referred to as tunneling.

Chapter 5. Proposed Blueprint

5.1 Information Security Blueprint for Interconnecting HIT Networks

This information security blueprint compares five widely used WAN technologies, which are discussed in the previous chapter, in various perspectives. But, in order to help more in the decision-making process, it is important to compare these WAN technologies according to different standards. In general, there are eight main criteria considered for the comparison: general information, connection types, security, performance, flexibility, cost, complexity and compliance. The combination of these chosen criteria can be found in the several textbook, researches, and vendor websites; which indicates the importance of these measures [7] [40] [58].

Under these main categories, more specific features are examined. For connection type, typical bit rate; remote access capability; site-to-site connection functionality; persistence, which examines if the technology requires a constant connection; use of virtual circuits and physical carrier types are discussed. For security criteria, the availability of the SSL, encapsulation (tunneling) protocols, data integrity mechanisms, the use of private or public infrastructure, authentication protocols and encryption methods are examined. For the performance, data segmentation, overhead considerations, error and flow control mechanisms, Quality of Service (QoS) and fixed bandwidth availability are studied. Also, in this section, the major advantages and disadvantages of these WAN technologies are listed. After reviewing these WAN connection options, the best technology that meets the requirements of a specific HIT network design can be adopted in the healthcare organizations.

From the flexibility perspective, the availability of the reproducibility, scalability and location dependency is explored. In this part, reproducibility refers to the ability of re-implementation of the technology in the case a healthcare provider moves to another location. In addition, location dependency

refers to the remote access by questioning if the medical providers have an access to their networks from other locations, such as their homes. Under the cost criteria, general costs and operational costs are discussed. For the complexity, minimum hardware requirements and required protocols for data transfer are compared. Lastly, HIPAA compliances of these technologies are examined. As this compliance can be achieved by the use of technical safeguards, such as encryption, mechanism to authenticate ePHI and integrity controls; the decisions are based on the existence of these functionalities. These criteria and compared WAN technologies can be found in Tables 6 and 7 below, which display the information security blueprint.

Table 6 Information Security Blueprint I

Wide Area Network Technologies	Leased Line	Frame Relay	ATM	Metro Ethernet	Internet with the use of VPN
General Information					
	point-to-point connection between two computers' LAN	connection-oriented, packet-switch method	connection-oriented, cell-switching method	LAN technology, commonly known as the CSMA/CD protocol	connectionless packet switching
Connection Types					
Typical Bit Rate	up to 45 Mbps (E3/T3)	offers data rates up to 4 Mbps	can support 622 Mbps and higher	Standard Ethernet speeds of supported, up to 500 Mbps	depends on service provider offerings
Remote Access	no	no	no	no	yes
Site-to-Site	yes	yes	yes	yes	yes
Persistence	yes	yes (PVC), no (SVC)	yes (PVC), no (SVC)	yes	yes (site-to-site VPN), no (remote-access VPN)
Virtual Circuits?	no	PVC, SVC	PVC, SVC	EVC	no
Carriers	T-carriers, especially T1 and T3	T1, fractional T1, or 56-Kb circuits	T1/E1 to OC-12	10BaseT, 100BaseT and 1000BaseSX.	depends on service provider offerings
Security					
SSL	no	no	no	no	yes
Encapsulation (Tunneling) protocols	HDLC, PPP	no	PVC provides PVP tunneling	Ethernet MAC Sub layer, through PPP	GRE, IPsec, L2F, PPTP, L2TP, DMVPN
Data Integrity	not checked	FCS in the frame	not checked	not checked	HMAC
Public/Private Infrastructure	private	both	both	both	both
Authentication protocols	PPP provides authentication through PAP and CHAP	no	no	EVC and UNI provides port authentication through Layer 2 Control Protocol	PSK, RSA signature
Encryption methods	no	no	no	no	DES, 3DES, AES, RSA
Performance					
Data Segmentation	variable-length LCP packets	variable-length packets	fixed cells of 53 bytes	An Ethernet frame's size depends on the MTU of the underlying network, max frame size is 1526 bytes	An IP datagram's size depends on the MTU of the underlying network
Overhead/Delay	5-9 bytes of header and variable-length data can increase overhead	the simplified handling of frames leads to reduced latency	low (5 bytes of overhead for each 48-byte payload)	Ethernet frame preamble sequences (8 bytes), frame headers (14 bytes) and acknowledge packets constitute the overhead.	TCP and IP headers each take up to 20 byes, which can increase overhead
Error Control	HDLC provides error control	cyclic redundancy check (CRC)	yes (in physical layer)	cyclic redundancy check (CRC)	checksum
Flow Control	HDLC provides flow control	FECN, BECN	yes (in the header)	through the use of a pause frame, generated by the receiving MAC	yes, sliding window method
Quality of Service (QoS)	yes	yes	yes	no	no
Fixed Bandwidth Availability	yes	no, the infrastructure is shared	yes	yes	no, the infrastructure is shared

Table 7 Information Security Blueprint II

Wide Area Network Technologies	Leased Line	Frame Relay	ATM	Metro Ethernet	Internet with the use of VPN
Performance	Performance	Performance			
Major advantage	most secure	highly efficient on the use of bandwidth	best for simultaneous use of video, voice and data	the service is provided over a standard, widely available and well-understood Ethernet interface	least expensive, globally available
Major disadvantage	most expensive	shared media across the link	overhead can be considerable (When the cell is carrying segmented packets)	limited to geographic scope	least secure, use of VPN security protocols can help
Flexibility	Flexibility	Flexibility			
Reproducible	no	yes	yes	yes	yes
Scalable	no	yes	yes	yes	yes
Location Dependant	no	no	no	no	yes
Cost	Cost	Cost			
Cost based on	distance, capacity	capacity	capacity	monthly subscription	monthly subscription
General Costs	most expensive (priced based on bandwidth required and distance between the two connected points)	based on the bandwidth usage	pay for use, bandwidth on demand	based on the bandwidth usage	least expensive
Complexity	Complexity	Complexity			
Min Hardware Requirements	CSU/DSU, DTE	DTE (customer-owned terminals, personal computers, routers, and bridges), DCE (service providers' switches), DCU/CSU	DSU, ATM switch, DTE for ATM interfaces	Ethernet switch, CE (all networking equipment connect to network using Ethernet)	VPN gateways (routers, firewalls, VPN concentrators and ASAs)
Protocols Required	PPP or HDLC	Frame Relay	ATM	Layer 2 Control Protocols (MAC Control Protocol, LACP, GARP, STP..)	TCP/IP
Compliance	Compliance	Compliance			
HIPAA	yes	no	no	no	yes

According to the findings presented in the blueprint above, the major advantage of the lease line technology is security. They are considered most secure technology among all the option. However, since they are the most expensive option, they don't offer the cost efficiency. Frame relay, on the other hand, provides highly efficient on the use of bandwidth and offers more affordable WAN technology. In spite of this advantage, frame relay share media across the link, which causes some security concerns.

ATM networks can be utilized for simultaneous use of voice, video and data effectively. It creates fixed-cells during the segmentation, and these cells can provide an advantage during the transmissions. However, in ATM, overhead can be considerable disadvantage. As an alternative to ATM technology, metro Ethernet services are provided over a standard, widely available and well-understood Ethernet interface. Therefore, this option can be utilized by the healthcare organizations in a convenient way. Although, metro Ethernet does not have QoS and other traffic-prioritization capabilities, which can create some security and performance concerns. On the other hand, Internet with the use of VPN technology is the least expensive, globally available WAN technology. However, it offers least secure way of data transmission over the wide area networks. Thus, VPN security protocols should be implemented.

5.2 Feedback from IT Professionals

After finalizing information security blueprint, a survey with IT professionals in the healthcare industry was conducted. The purpose of this survey was twofold. First, it was aimed to explore current industry practices in HIT, how they are deployed in healthcare settings, challenges and benefits experienced, and security countermeasures that are implemented. The second part was intended to obtain a feedback on the blueprint by asking respondents to compare these technologies according to eight major criteria. In parallel with the purpose, the scope of this survey were the topics which cover

the background information on healthcare industry in the US, HIT, HIE, NHIN, LAN design, HIT security concerns, WAN technologies and information security blueprint.

Due to the nature of the healthcare settings, the questionnaire type of survey was preferred over the interview type. Since HIT professionals work in busy environments and perform critical operations, this more flexible and time-efficient way of surveying well suited to the purpose of this review. In the questionnaire, there were 28 questions. The structure of the questions and the answers were carefully chosen to reduce the questionnaire time and ensure consistent feedback. More specifically, dichotomous (yes/no), filter/contingency questions and questions based on level of measurement were asked. The questionnaire can be found in Appendix B.

When conducting the survey, two different communication mediums used. For a group of respondents, who are located in Wilmington, NC and willing to meet in person, the work place drop-off method utilized. For the other group of respondents, who are located in other cities and states, the questionnaire sent by e-mail and the responses were gathered through the same medium. Since the same questions are being asked in these two different approaches, the survey responses can be considered impartial.

In addition to this survey practice, an ISP was contacted in order to receive a feedback on the information security blueprint. The purpose of this attempt was to assess the accuracy of the WAN technologies information provided in this research and make any corrections, if needed. Another reason to contact with an ISP was to understand their product offerings to their customers who operate healthcare industry and question if they could combine the features of these five WAN technologies according to their requests.

5.3 Evaluation of the Survey and Information Security Blueprint

Six healthcare/security professionals who work in NHRMC, Southeastern Regional Medical Center (SRMC), and Coastal Carolinas Health Alliance Coastal Connect, Inc. (CCHIE) took this survey. NHRMC is a not-for-profit health care system serving southeastern North Carolina and northeastern South Carolina. It is also a teaching hospital, regional referral center, and Level 2 Trauma Center; providing a wide range of health care services. SRMC is a non-profit healthcare system, which offers a combination of acute care, intensive care and psychiatric services. Lastly, CCHIE was established in 1991 to build stronger peer relationships among hospitals on the coast of North Carolina. Over the years, CCHIE has grown into one of the top hospital alliances in the country. The participants who took this survey have the average of 15.16 years of experience in the healthcare and 2.8 years of experience in the security industry. 2 out of the 6 participants were involved in day-to-day security operations in their organizations.

The respondents listed the major problems in the healthcare industry as patient care accessibility; cost of doing business with both doctors and patients and defensive medicine efforts; security of the patient data; identity management and the issues surrounding bring your own device (BYOD); lack of care transition when patients leave the hospital; and limited resources for filled Rx information. Five of the respondents agreed that widespread use of HIT expands access to affordable, quality and cost-effective patient care while improving the delivery of healthcare in the US. They also all agreed that having access to the complete and accurate medical and patient information; faster diagnosis, reduced medical errors; stronger coordination of care; improved consumer-centered care; increased early detection of medical conditions; and increased administrative efficiency are the advantages of using HIT. However, there was not a consensus on the other listed advantages, which were: safer and higher quality; lower healthcare costs; stronger patient privacy and data protection; and

improved disease prevention and response. These differences among the responses can be explained as extend of HIT implementation and day-to-day exposure in each organization. Since there are possible disparities between these medical providers in terms of HIT adoption and utilization in a daily basis, the advantages would vary according to their experience.

Among HIT applications, Practice Management System and Medical Information Systems were used in all organizations, while NHRMC both used and owned all the HIT applications listed in the questionnaire. SRMC did not have the EHR implementation in its facility, but instead it had an extensive use of Imaging and Visualization software. Also, for the EHR implementation method, both NHRMC and CCHIE owned and managed all the equipment and services, but their purpose of utilizing EHR was different. CCHIE had a role to establish HIEs between EHRs and therefore they had the EHR system in their facility for the testing purposes, while NHRMC had to utilize it for their daily operations. Lastly, they all agreed that the use of EHR would improve the delivery of healthcare within the next 5 years. This result points out that the organizations, whether they already adopted EHR or not, believe that EHR offers benefits and it will help the increase the efficiency of healthcare in the US.

When the professionals were asked to order the complexity of the roadblocks that are faced in the implementation of HIEs, their responses were not in consensus; therefore the weighted average method was utilized. In the results, the average weight of data sharing was found as 2.2, while patient consent was 4.4, interoperability standards was 3, complexity costs was 1.8 and competition was 3.6. These variances among the respondents' results can be explained with the challenges that they face in their own organizations while implementing information exchange practices. Also, one of the respondents added that user adoption and workflow changes will be another major roadblock for HIE adoption. Furthermore, 3 out of the 6 respondents were confident that a long-term health data exchange on a large-scale could be sustained between healthcare organizations. However, everyone agreed that the

federal government would have to mandate the minimum standards of accessing health information and security measures since healthcare is very competitive and secretive. Therefore they mentioned that it would take a lot of efforts to maintain the sustainable information sharing and overcome the potential risks. These results underline the importance of the federal regulations in the healthcare industry and their guidance to the HIE implementation.

The participants indicated that their organizations had implemented interoperability standards for joining HIE. More specifically, NHRMC was working with EPIC, an EHR software, to create an HIE for EPIC customers while CCHIE was already implemented these standards and are a part of HIE which covers 80 practices and 5 hospitals in the region. SRMC was one of these hospitals, which had the standards and currently on the HIE in alliance with CCHIE. According to the responses, it is clear that these three healthcare organizations have started or already implemented these interoperability standards. For understanding the feasibility of the National Health Information Network (NHIN) goal, this survey asked if this initiative was achievable goal within the next 10 years. All the respondents either were neutral or disagreed. One of the participants explained this response from his experience with IBM's failed NHIN alpha project and added that at least 15 years needed. The reason why all the participants were pessimistic about the creation of NHIN can also be explained with the roadblocks faced in the HIE adoption process. Since information exchanges are the initial steps of this nationwide project, the challenges experienced so far can negatively impact the final goal, which is the information exchange in the national level.

For another survey question, the participants in CCHIE indicated that they did not have a HIPAA privacy/security officer (also called Health Information Officer) while NHRMC and SRMC did. According to HIPAA, all the covered entities must assign a privacy/security officer. Therefore, it is expected that NHMC and SRMC will have these officers in their organizations. However, CCHIE is a

health alliance and it is not listed under covered entities. Thus, legally, they do not have to employ this officer in their facility.

In the survey, there were some questions related to LAN and network perimeter security measures. For the LAN security methods, all the participants pointed out that they have antivirus scanners, operating systems security patches, host based intrusion detection systems, daily back-up systems, access control and physical security countermeasures implemented in their organization. Also, for their contingency plan for link and device failures, they explained that they have daily back-ups and off-site storages, in addition to the e-mail notifications for downtime procedures. According to the responses, all organizations have Standard ACLs and IPS applied; and mainly using stateful and application gateway firewalls with the dual firewall implementation design. All these responses are expected since they are crucial tools utilized for securing the LANs and the network perimeter. In addition, it was noted that NHRMC also added a new workstation, which works as a subset of data at the endpoint level, and aimed to be utilized during the link or device failures.

The second part of the survey was intended to understand the WAN technologies that are in use and receive a feedback on their overall performance. It also had some questions on the blueprint by asking participants to compare WAN technologies according to eight major criteria, which explained in the previous section. Participants from CCHIE indicated that they were using leased lines, frame relay and ATM technologies. As a major advantage, they mentioned that these technologies are secure. But, since there is limited access to the resources, they explained that they would prefer to have remote access to their organization's network. They also added that there is a project in pending status for the implementation of the VPN technology. On the other hand, NHRMC was using VPN and Metro Ethernet. The respondent explained the major advantage as the high bandwidth and low cost, while indicating the major disadvantage for being a new technology. These responses indicate that the

healthcare organizations tend to prefer WAN technologies that offer more flexibility, cost-efficiency, higher security and remote access. In addition, during my interview with CCHIE, it was underlined that they are following the technologies that NHRMC adopts, thus they be implementing metro Ethernet and VPN technologies in the near future.

Lastly, for the blueprint evaluation, the weighted average method utilized again. According to the ratings, VPN and metro Ethernet were the most flexible; and VPN, leased lines and metro Ethernet were the most secure WAN technologies. Also, ATM and metro Ethernet had the best network performance, while VPN was rated as the least expensive choice. Lastly, leased lines were indicated as the least complex WAN option. In overall, metro Ethernet was rated as the best technology choice while VPN was closely following it. These results are well matched with the information provided in the WAN technologies blueprint. Therefore, it can be claimed that the industry feedback on the blueprint supports findings presented in this research.

In overall, the feedback received from the industry professionals confirmed that information provided on HIT practices, their implementations healthcare settings, HIEs, security methods and WAN technologies was accurate and in parallel with the industry practices.

Chapter 6. Conclusions

6.1 Discussion

According to the findings of this research and feedback have been gathered from the industry professionals, the metro Ethernet technology is the best alternative for interconnecting the HIT networks. Since it offers site-to-site connections over Ethernet and remote access services through Ethernet VPNs, organizations can extend their LAN to the metropolitan area, which enables them to have reliable connections between remote offices and headquarters where they can securely access their applications and data.

As stated in the WAN technologies review, most healthcare providers are converting to metro Ethernet for Internet connections and connections between sites; since it offers high transmission, high bandwidth and cost savings. The major advantage of this WAN option is having a standard, widely available and well-understood Ethernet, as a core technology. Also, with the use of Ethernet VPN service, Metro Ethernet provides the services that VPN technology over the Internet offers. With this functionality, healthcare professionals are given the flexibility to connect their networks remotely, from anywhere and anytime.

6.2 Implications

Implementing HIT services in the medical providers and utilizing them in daily operations improves disease prevention and response. Digital tracking of health information makes it easier to observe trends in the general population as well as track successful treatment methods. This functionality promotes public health and preparedness. As a result, widespread use of HIT can help to expand access to the affordable, quality and cost-effective patient care while improving the delivery of healthcare in US.

This research provided comprehensive background information on specific technologies for interoperable HIT networks and best practice approaches for fulfilling security requirements, in order to secure communications between organizations. Also, information security requirements in the healthcare industry, related regulations and how these regulations effect healthcare organizations are discussed in detail.

The findings of this study can be utilized as a technology guide by the healthcare entities. They can use this research to understand and compare the current information security practices that can be applied to their HIT networks; and WAN technologies for interconnecting their networks. In combination, this research can help to offer the information security blueprint for interconnecting HIT networks, where the information exchange will be achieved.

References

[1] Ahmad, Khalid. "Chapter 2 - ATM Principles and Basic Definitions". Sourcebook of ATM and IP Internetworking. IEEE Press. 2002. Books24x7. <http://common.books24x7.com/toc.aspx?bookid=3179> (accessed June 2, 2012)

[2] Allen, Julia H. (2001). The CERT Guide to System and Network Security Practices. Boston, MA: Addison-Wesley.

[3] Anthony G. Bower, P. D. (2005). "The Diffusion and Value of Healthcare Information Technology." RAND Cerner Quarterly (2005): 1-5.

[4] A. Shih, K. Davis, S. Schoenbaum, A. Gauthier, R. Nuzum, and D. McCarthy, Organizing the U.S. Health Care Delivery System for High Performance, The Commonwealth Fund, August 2008.

[5] (2012). Benefits of Electronic Health Records (EHRs), HealthIT.gov.

[6] Blumenthal, D. (2011). "Implementation of the Federal Health Information Technology Initiative." New England Journal of Medicine 365(25): 2426-2431.

[7] Bob Vachon, R. G. (2009). Accessing the WAN. Indiana, Cisco Press.

[8] Brailer, D., & Thompson, T. (2004). Health IT strategic framework. Washington, DC: Department of Health and Human Services.

[9] Caldis TG. The long-term projection assumptions for Medicare and aggregate national health expenditures. Baltimore: Office of the Actuary/National Health Statistics Group. May 12, 2009

[10] (2005). "Can HIT Lower Costs and Improve Quality?". 2012, from http://www.rand.org/pubs/research_briefs/RB9136/index1.html.

[11] (2012). "CDA Release 2." Section 3: Clinical and Administrative Domains. Retrieved 03/25/2012, from

[12] Cisco Health Information Networking Curriculum

[13] 2012). "Cisco Healthcare Solutions Related to EHR." Industry Solutions. Retrieved 04/05/2012, from http://www.cisco.com/web/strategy/healthcare/breathe_life_into_ehr.html.

[14] Cline, S. (2012). About Health IT in North Carolina. N. D. o. H. a. H. Services, NC Department of Health and Human Services.

[15] (2012). CMS EHR Meaningful Use Overview. D. o. H. H. Services, Centers for Medicare & Medicaid Services.

[16] (2010). "Continuity of Care Record (CCR)." Retrieved 03/25/2012, from http://searchhealthit.techtarget.com/definition/Continuity-of-Care-Record-CCR.

[17] Corporation, M. (2006). Electronic Health Records Overview. McLean, Virginia, National Institutes of Health National Center for Research Resources.

[18] C. Peterson and R. Burton, "U.S. Health Care Spending: Comparison with Other OECD Countries," ed. Domestic Social Policy Division (Washington D.C.: Congressional Research Service, 2007).

[19] (2010). Databases, Tables and Calculators by Subject. B. o. L. Statistics. Washington, DC, Bureau of Labor Statistics.

[20] (2012). Electronic Health Records. T. D. o. H. a. H. Services, Centers for Medicare & Medicaid Services.

[21] (2012). Electronic Health Records and Meaningful Use. U. D. o. H. H. Services, The Office of the National Coordinator for Health Information Technology.

[22] Elhauge, E. (2010). The Fragmentation of US Health Care Cases and Solutions, Oxford University Press.

[23] (2012). For Covered Entities. U. S. D. o. H. a. H. Services, U.S. Department of Health and Human Services.

[24] Group, A. H. H. P. S. J. W. (2011) The Privacy and Security Gaps in Health Information Exchanges.

[25] Harris, S. (2008). Certified Information Systems Security Professional. New York, McGraw-Hill.

[26] Harvey V. Fineberg, M. D., Ph.D. (2012). "A Successful and Sustainable Health System - How to Get There from Here." New England Journal of Medicine 366: 1020-1027.

[27] (2010). Health Care C. B. Office, Congressional Budget Office.

[28] (2012). "Healthcare Information Exchange." RHIO/HIE. Retrieved 04/15/2012, from http://www.himss.org/asp/topics_hie.asp.

[29] (2012). Health IT. U. S. D. o. H. H. Services, The Office of National Coordinator for Health Information Technology.

[30] (2012) HIM Principles in Health Information Exchange (Practice Brief). American Health Information Management Association (AHIMA)

[31] (2012). "HIPAA - General Information." Retrieved 03/17/2012, from http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/index.html.

[32] (2012). "HL7/ASTM Implementation Guide for CDA Release 2- Continuity of Care Document (CCD) Release 1." Retrieved 03/25/2012, from http://www.hl7.org/implement/standards/product_brief.cfm?product_id=6.

[33] (2004). Information Technology in Healthcare. Report to the Congress: New Approaches in Medicare, Medpac.

[34] Jackson, C. L. Network Security Auditing: The Complete Guide to Auditing Network Security, Measuring Risk, and Promoting Compliance. Cisco Press. 2012. Books24x7. <http://common.books24x7.com/toc.aspx?bookid=45402> (accessed March 5, 2012)

[35] Keith Hutton, Mark Schofield and Diane Teare. “Chapter 4: Advanced WAN Services Design Considerations”. Designing Cisco Network Service Architectures (ARCH) (Authorized Self-Study Guide), Second Edition. Cisco Press. 2009. Books24x7. <http://common.books24x7.com/toc.aspx?bookid=35313> (accessed June 3, 2012)

[36] Leslie, T. (2011) Realizing the Promise of Health Information Exchange.

[37] Mauricio Arregoces , Maurizio Portolani . Data Center Fundamentals: Understand Data Center Network Design and Infrastructure Architecture, Including Load Balancing, SSL, and Security. Cisco Press. 2003. Books24x7. <http://common.books24x7.com/toc.aspx?bookid=45396> (accessed March 7, 2012)

[38] McLean, M. C. f. E. M. (2006). Cost and Return on Investment, National Institutes of Health National Center for Research Resources: 18.

[39] (2009). "Metro Ethernet." Telecom Resources. Retrieved 5/12/2012, 2012, from http://searchtelecom.techtarget.com/definition/Metro-Ethernet.

[40] Minoli, Daniel. "Chapter 9 - Evolving SAN, GbE/10GbE, and Metro Ethernet Technologies". Enterprise Architecture A to Z: Frameworks, Business Process Modeling, SOA, and Infrastructure Technology. Auerbach Publications. 2008. Books24x7. <http://common.books24x7.com/toc.aspx?bookid=26424> (accessed May 12, 2012)

[41] (2012). National Health Expenditure Data. C. f. M. M. Services. Baltimore, The National Health Expenditure Accounts (NHEA).

[42] (2012). Nationwide Health Information Network (NHIN): Background & Scope. U. D. o. H. a. H. Services, US Department of Health and Human Services.

[43] Priscilla Oppenheimer. Top-Down Network Design, Second Edition. Cisco Press. 2004. Books24x7. <http://common.books24x7.com/toc.aspx?bookid=35337> (accessed March 5, 2012)

[44] Richard Deal. CCNA Cisco Certified Network Associate Security Study Guide (Exam 640-553). McGraw-Hill/Osborne. 2009. Books24x7. <http://common.books24x7.com/toc.aspx?bookid=33002> (accessed March 7, 2012)

[45] Santitoro, R. (2006) Metro Ethernet Services - A Technical Overview. 19

[46] Society, H. I. M. S. "Electronic Health Record." Retrieved 04/04/2012, 2012, from http://www.himss.org/asp/topics_ehr.asp.

[47] Society, H. I. M. S. (04/04/2012). "Interoperability & Standards." from http://www.himss.org/ASP/topics_FocusDynamic.asp?faid=665.

[48] Staff, Government Health IT. (2011) The Top 5 roadblocks HIEs face.

[49] Summary of the HIPAA Privacy Rule. U. S. D. o. H. H. Services, U.S. Department of Health & Human Services: 2-4.

[50] Summary of the HIPAA Security Rule. U. S. D. o. H. H. Services, U.S. Department of Health & Human Services.

[51] (2000). The World Health Report 2000, World Health Organization (WHO): 155.

[52] Thompson, T. G., Brailer, D. J. (2004). The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care. D. o. H. H. Services. Washington D.C, Office of the Secretary National Coordinator for Health Information Technology.

[53] Wayne Lewis. (2009). LAN Switching and Wireless: CCNA Exploration Companion Guide. Indiana, Cisco Press.

[54] Wei Luo, Carlos Pignataro, Dmitry Bokotey and Anthony Chan. “Chapter 4 - LAN Protocols”. Layer 2 VPN Architectures. Cisco Press. 2005. Books24x7. <http://common.books24x7.com/toc.aspx?bookid=35340> (accessed June 3, 2012)

[55] (2006) Connected Health Framework Architecture and Design Blueprint. Microsoft Corporation.12.

[56] Gritzalis, D., Lambrinoudaki, C. (2004). "A Security Architecture for Interconnecting Health Information Systems." International Journal of Medical Informatics 73: 305-309.

[57] Varshney, U. (2009). Pervasive Healthcare Computing. New York, Springer.

[58] Circadence (2010) WAN optimization made easy.

Appendix A

Examples of HIT for hospitals and physicians [33]

Type of Information Technology	Applications
Hospitals	
Administrative and financial	Billing
	General ledger
	Cost accounting systems
	Patient registration
	Personnel and payroll
	Electronic materials management
	Electronic health record
	Picture archiving and communication systems
	Results reporting of laboratory and other tests
	Clinical decision support systems
	Computerized provider order entry for drugs, lab test, procedures
	Prescription drug fulfillment, error-alert, transcriptions
	Electronic monitoring of patients in intensive care units
Infrastructure	Desktop, laptop, cart-based, and tablet computers
	Servers and networks
	Wireless networks
	Voice recognition systems for transcription, physician alerts, and medical records
	Bar-coding technology for drugs, medical devices, and inventory control
	Information security systems
Physicians	
Administrative and financial	Accounting
	Scheduling
	Personnel and payroll
Clinical	Online references
	Receiving lab results and other clinical information online
	Electronic prescribing
	Computerized provider work entry
	Clinical decision support systems
	Electronic health record
	E-mail communication with patients
Infrastructure	Desktop and laptop computers
	Handheld technology
	Servers and network

Appendix B

Survey Questions

1. What is your current job title?
2. How many years have you been working in the industries below? Please indicate.
   - Healthcare industry:
   - Security industry:
3. Are you involved in day-to-day security operations in your healthcare organization?
   Yes No
4. In your opinion, what are the major problems in the healthcare industry?
5. Do you think widespread use of Healthcare Information Technology (HIT) expands access to affordable, quality and cost-effective patient care while improving the delivery of healthcare in the US? Why or why not?
6. What are the advantages of using the HIT? Please check all that apply.

Having access to the complete and accurate medical and patient information	
Faster diagnosis, reduced medical errors	
Safer and higher quality care	
Lower healthcare costs	
Stronger coordination of care	
Improved consumer-centered care	
Stronger patient privacy and data protection	
Increased early detection of medical conditions	
Improved disease prevention and response	
Increased administrative efficiency	
Other	

7. Please check the applications that are owned and/or used in your healthcare environment.

Applications	**Owned**	**Used**
Practice Management System (including patient registration, billing, scheduling and reporting components)		
Imaging and Visualization Software		
E-Prescription Software		
Medical Information Systems		
Electronic Healthcare Records (EHR) (if you select this option, please answer questions 8, if do not select this option, please answer question 9)		

8. Please select the EHR implementation method that your organization (healthcare provider) pursued.
   - Provider owns and manages all the equipment and services.
   - An EHR vendor owns and manages the equipment installed at the healthcare provider's site.
   - An EHR vendor hosts all EHR applications; the servers that run the applications are located in the vendor's facility.
   - Other: _____
9. Please select the reason(s) for not adopting the EHR in your healthcare organization.
   - Insufficient resources
   - Negative return on investment
   - Resistance to change from the medical personnel
   - Lack of required infrastructure
   - Other: _____

10. In your opinion, will the use of EHR improve the delivery of healthcare within the next 5 years?

Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

11. Please order the complexity of the roadblocks below that are faced in the implementation of the Health Information Exchanges (HIEs) where '1' = most complex, '2' = next most complex, and so on.
    ____Data sharing
    ____Patient consent
    ____Interoperability standards
    ____Complexity costs
    ____Competition
12. Do you think a long-term health data exchange on a large-scale can be sustained between healthcare organizations? Why or why not?
    Yes No
13. Has your organization implemented any interoperability standards for joining an HIE? If yes, please explain.
    Yes No
14. Do you think a National Health Information Network (NHIN) is an achievable goal within the next 10 years? Why or why not?

Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

15. Do you have a HIPAA privacy/security officer (also called Health Information Officer) in your organization? If no, who is responsible for the related operations?
    Yes No
16. Please select the LAN security method(s) that is/are currently implemented in your organization.
    - Antivirus scanners
    - Operating systems security patches
    - Host based intrusion detection systems
    - Daily back-up systems
    - Access control
    - Physical security
17. What is your contingency plan for link and device failures?
18. If you are using Access Control Lists (ACLs), please indicate the type of ACL applied:
    - Standard ACL (examines the incoming traffic according to Layer3 information)
    - Extended ACL (examines the incoming traffic according to Layer 3 and 4 information)
19. If you are using Firewalls, please indicate the type of the Firewall applied:
    - Packet-filtering firewall
    - Stateful firewall
    - Application gateway firewall
20. Please select the design of your organization's firewall implementation:
    - Single firewall implementation (3 interfaces with public, private and DMZ networks)
    - Dual firewall implementation (3 interfaces with public, private and DMZ networks – DMZ is surrounded by firewalls in both sides)

21. Do you currently have Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS) implemented in your organization? Please select.
    - Intrusion Detection System (IDS)
    - Intrusion Prevention System (IPS)
22. Which Wide Area Network Technology is implemented in your organization? Please select.
    - Leased Lines
    - Frame Relay
    - ATM
    - VPN
    - Metro Ethernet
23. What are the major advantages and disadvantages of the preferred WAN technology in your organization?
    Major Advantage:
    Major Disadvantage:
24. Please rate the flexibility (reproducible, scalable, location dependent…etc) of the given WAN technologies with NHIN perspective, where '1' = most flexible, '5' = least flexible, and so on.
    ___ ATM
    ___ Frame Relay
    ___ Internet with the use of VPN
    ___ Leased Line
    ___ Metro Ethernet
25. Please rate the security features (encapsulation, authentication, data integrity…etc) of the given WAN technologies with NHIN perspective, where '1' = most secure, '5' = least secure, and so on.
    ___ ATM
    ___ Frame Relay
    ___ Internet with the use of VPN
    ___ Leased Line
    ___ Metro Ethernet
26. Please rate the network performance (overhead, Quality of Service, error check…etc) the given WAN technologies with NHIN perspective, where '1' = best performance, '5' = worst performance, and so on.
    ___ ATM
    ___ Frame Relay
    ___ Internet with the use of VPN
    ___ Leased Line
    ___ Metro Ethernet
27. Please rate the overall costs of the given WAN technologies with NHIN perspective, where '1' = most expensive, '5' = least expensive, and so on.
    ___ ATM
    ___ Frame Relay
    ___ Internet with the use of VPN
    ___ Leased Line
    ___ Metro Ethernet
28. Please rate the complexity (hardware requirements, protocols needed…etc) of the given WAN technologies with NHIN perspective, where '1' = most complex, '5' = least complex, and so on.
    ___ ATM
    ___ Frame Relay
    ___ Internet with the use of VPN
    ___ Leased Line
    ___ Metro Ethernet