Volume 6, Issue 4
November 2013
ISSN: 1946-1836

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

In this issue:

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer-reviewed academic journal published by **EDSIG,** the Education Special Interest Group of AITP, the Association of Information Technology Professionals (Chicago, Illinois). Publishing frequency is currently quarterly. The first date of publication is December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 45%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org.

JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

Editors

JISAR Editorial Board

Information Security Blueprint For Nationwide Health Information Network

Ulku Yaylacicegi
yaylacicegiu@uncw.edu
University of North Carolina Wilmington
Wilmington, NC 28403, USA

Selin Benli
Credit Suisse
Research Triangle Park, NC 27560, USA

Stacy Mitchell
mitchells@uncw.edu

Ron Vetter
vetterr@uncw.edu
University of North Carolina Wilmington
Wilmington, NC 28403, USA

Abstract

With the increasing costs and the decreasing quality of care in the US healthcare industry, there are substantial incentives by the US government to move towards an integrated national health network. The sensitive nature of the healthcare data to be exchanged requires the integrated network to address the privacy and information security concerns. This study describes the design and implementation considerations to provide an information security blueprint for the Nationwide Health Information Network (NHIN). The objective of this research is twofold. First, it aims to provide background information about technology implementations in healthcare organizations, current Healthcare Information Technology (HIT) services, electronic healthcare records (EHRs) and design considerations for healthcare networks. In addition, it explores current wide area network (WAN) technologies and various security methods for assuring the secure healthcare information exchange between medical providers. The positive preliminary feedback from several HIT professionals validates the proposed blueprint.

Keywords: Healthcare information technology, information security, nationwide health information network, wide area network technologies, electronic health records

1. INTRODUCTION

Healthcare represents a significant segment of the U.S. economy and workforce. In 2010, total health expenditures reached $2.6 trillion, which translates to $8,402 per person or 17.9% of the nation's GDP (Thompson & Brailer, 2004). Healthcare is the single largest industry in the United States, providing 14 million jobs through approximately 580,000 establishments (Bureau

of Labor Statistics, 2010). 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. 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 (HIMMS, 2012).

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 (The Office of National Coordinator for Health Information Technology, 2012b). Currently, one of HIT services is Electronic Healthcare Record (EHR) system, which is an electronic record of patient health information generated by one or more encounters in any care delivery setting (Caldis, 2009). With EHR doctors can have a complete picture of the patient's health without redundant tests and examinations. EHR implementations can increase the quality of healthcare delivery and reduce the associated costs (National Institutes of Health National Center for Research Resources, 2006). To encourage organizations to adopt EHRs, the federal government has set aside funding as part of the American Recovery and Reinvestment Act of 2009 (ARRA) (Blumenthal, 2011). One of the primary goals behind the government's initiative for encouraging the adoption of EHRs is to increase Health Information Exchanges (HIEs) and eventually maintain a Nationwide Health Information Network (NHIN), which aims 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 (Cline, 2012). 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. Healthcare practices increasingly rely on networks for their core operations; thus, become more vulnerable to information security threats. 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 (HIPAA, 2012).

The US government intends to enhance HIEs and establish the NHIN in near future, which makes securing healthcare systems, networks and information exchange 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 (US Department of Health and Human Services, 2012c). However, the specific security methods, tools, their implementations and related standards for healthcare organizations have not yet been stated clearly. There are a few guidelines and research studies addressing this loophole. The Connected Health Framework Architecture and Design Blueprint, a Microsoft published guideline (2006), proposes a solution for transforming healthcare through technology options that are cost-effective, productive, and connected by design. Even though information security is discussed as one of the architectural challenges, the guideline does not explore the security concerns of interconnected network design extensively. The security architecture for interconnecting health information systems proposed by Gritzalis and Lambrinoudakisbby (2006) is mainly designed for providing authentication and authorization services in web-based distributed systems and fails to cover the information security considerations in a broader perspective.

This study focuses on the information security best practices and proposes an information security blueprint for the NHIN 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 various security measures that can be implemented for HIE networks.

2. 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 (The World Health Organization, 2000). It was indicated in this ranking; the US spends more than $2.6 trillion annually on healthcare (Thompson & Brailer, 2004). The poor quality of healthcare delivery in the US compared to the most developed nations in the world indicates that this amount is not spent efficiently (Bower, 2005; Peterson & Burton, 2007).

Healthcare in the US faces multiple problems, including high and rising expenditures, inconsistent quality, and gaps in care and access (Bower, 2005; Varshney, 2009). According to Commonwealth Fund, a private foundation working toward a high performing health system, healthcare delivery in the US is a "cottage industry" (Shih, Davis, Schoenbaum, Gauthier, Nuzum, & McCarthy, 2008), 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 (Shih et al., 2008). The fragmentation of healthcare delivery system is a fundamental contributor to increased 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 the patient among multiple providers' leads to medical errors, waste, and duplication.

Technology Integration in the Healthcare and Healthcare IT

Brailer & Thompson (2004) define healthcare IT as the application of information processing involving both computer hardware and software dealing with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making. 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 (Thompson & Brailer, 2004). HIT is increasingly viewed as the most promising solution for improving the overall quality and efficiency of the healthcare delivery system in the US (The Office of National Coordinator for Health Information Technology, 2012b; Bower, 2005; Medpac, 2004). 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 (RAND, 2005).

For understanding the potential uses and benefits, many researchers and government agencies studied HIT so far (Bower, 2005; US Department of Health and Human Services, 2012a; RAND, 2005; Medpac, 2004; Mitchell & Yaylacicegi, 2010). According to their findings, the major advantage of utilizing HIT is having easy access to complete and accurate medical and patient information (The Office of National Coordinator for Health Information Technology, 2012b). 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 (Fineberg, 2012). 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 (The Office of National Coordinator for Health Information Technology, 2012b). 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 (The Office of National Coordinator for Health Information Technology, 2012b; Thompson & Brailer, 2004). 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 (Cisco HIN Curriculum, 2012). In addition, 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 (Fineberg, 2012). 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 (The Office of National Coordinator for Health Information Technology, 2012b). One of the most commonly employed HIT applications in the healthcare environment is electronic health records (EHR) software (The Office of National Coordinator for Health Information Technology, 2012b), otherwise known as electronic patient records or computerized patient records.

Electronic Healthcare Records (EHRs)

According to the definition provided by the Health Information Management Systems Society (HIMSS), electronic health record (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 (HIMMS, 2012). 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 (US Department of Health and Human Services, 2012a). 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 (US Department of Health and Human Services, 2012b). By making it easier to use and share patient information, EHRs can help health care providers to reduce medical errors, save money and time (US Department of Health and Human Services, 2012a).

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 (Elhauge, 2010). 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 (Thompson & Brailer, 2004). The federal government, as part of ARRA of 2009, 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 (The Office of National Coordinator for Health Information Technology, 2012a). 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 (Blumenthal, 2011). 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 (Leslie, 2012).

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 (HIPAA, 2012). 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 (Cisco HIN Curriculum, 2012). In order to join HIE, a medical provider should adopt an EHR system. Joining HIE improves care coordination, reduces healthcare disparities, empowers patients, and improves population health while ensuring adequate privacy and security (Leslie, 2012). 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 (Leslie, 2012).

Technology is a critical tool in achieving the benefits of HIE (AHIMA, 2012). Adoption of HIE practices requires an 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 (Cisco HIN Curriculum, 2012). The main roadblocks the health providers are encountering

in the implementation of HIEs are data sharing, patient consent, standards, complexity costs and competition (Government Health IT, 2011).

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 (Medpac, 2004). 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 (US Department of Health and Human Services, 2012c). The conceptual representation of NHIN is shown on Figure 1.

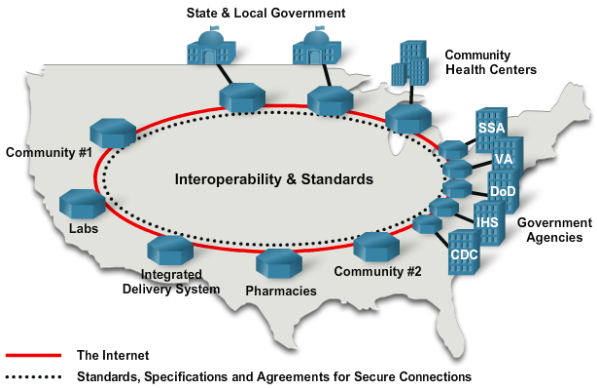

Figure 1. Nationwide Health Information Network

The sharing of patient information through a nationwide network brings some security concerns (Medpac, 2004). 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 (AHIMA/HIMMS, 2011). In the US, Health Insurance Portability and Accountability Act (HIPAA) was the first initiative for ensuring the patient privacy (Medpac, 2004). 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 (AHIMA/HIMMS, 2011).

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

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 (HIPAA, 2012).

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 and has provisions including 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 (Cisco HIN Curriculum, 2012).

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 (US Department of Health and Human Services, 2012d).

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. Privacy rule applies to written, oral, and electronic types of information (US Department of Health and Human Services, 2012d). On the other hand, the security rule defines the standards of basic security safeguards to protect electronic protected health information (ePHI), which refers to health information that is created, stored, transmitted, or received electronically. The security rule provides broader protection guidelines, focusing on the confidentiality, integrity, and availability of all electronic information (US Department of Health and Human Services, 2012d).

3. DESIGNING HIT NETWORKS

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 (Cisco HIN Curriculum, 2012). 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 a 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 (Lewis, 2009). The EHR 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 (Harris, 2008). It is important to understand the traffic flow to determine the connection and bandwidth requirements to prevent network congestion and degraded performance (Cisco HIN Curriculum, 2012; Jackson, 2012).

Medical providers are quite concerned about access to patient information; thus, every effort must be made to prevent downtime and loss of data. For ensuring this, there is a need to plan for redundancy for any possible link and/or device failures (Lewis, 2009).

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 (Lewis, 2009).

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 (Cisco HIN Curriculum, 2012; Oppenheimer, 2004).

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. Organizations should also implement daily backup systems and all backup storage assets must be protected (Harris, 2008). 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 (Lewis, 2009).

4. DEVELOPMENT AND IMPLEMENTATION CONSIDERATIONS FOR NHIN

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 (Cisco HIN Curriculum, 2012). 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. The healthcare organizations currently use the leased lines, frame relay, asynchronous transfer mode (ATM), metro Ethernet and Internet with the use of virtual private networks (VPNs) as WAN technologies for interconnectivity. Characteristics of each of these technologies are detailed in Table 1a-1e of Appendix A. In an attempt to create a blueprint and recommend best practices for NHIN security, Table 2 in Appendix B compares the WAN technologies using eight criteria capturing the most essential measures for securing the interconnected health networks (Vachon & Graziani, 2009; Minoli, 2008; Circadence, 2010). The criteria used for comparison are general information, connection types, security, performance, flexibility, cost, complexity and HIPAA compliance.

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. 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 another 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. Furthermore, in this section, the major advantages and disadvantages of these WAN technologies are listed. Review of these WAN connection options enables the adoption of the best WAN technology that meets the requirements of a specific HIT network design in the healthcare context.

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. Multiprotocol Label Switching (MPLS) based Ethernet is a preferred method used to provide high performance telecommunications networks.

In an attempt to validate the recommended best practices, a preliminary survey was conducted with regional HIT professionals. The feedback received showed that 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.

5. CONCLUSIONS

This study provides a comprehensive review of the background information necessary selecting the most viable WAN solution for the integrated health networks. 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.

According to one of the local health organization's information security expert, most healthcare providers are converting to MPLS based metro Ethernet for Internet connections and connections between sites due to high transmission, high bandwidth and cost savings characteristics of metro Ethernet. 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 offers. With this functionality, healthcare professionals are given the flexibility to connect their networks remotely, from anywhere and anytime.

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.

6. REFERENCES

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

AHIMA/HIMMS. (2011) The Privacy and Security Gaps in Health Information Exchanges. Retrived March 10, 2012 from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049023.pdf.

Bower, A. (2005) The Diffusion and Value of Healthcare Information Technology. Pub. no. MG-272-HLTH.

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

Bourgeois, S., & Yaylacicegi, U. (2010). Electronic Health Records: Improving Patient Safety and Quality of Care in Texas Acute Care Hospitals. *International Journal of Healthcare Information Systems and*

Informatics (IJHISI), 5(3), 1-13. doi:10.4018/jhisi.2010070101

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

Bureau of Labor Statistics. (2010). Databases, Tables and Calculators by Subject.

Caldis TG. (2009). The long-term projection assumptions for Medicare and aggregate national health expenditures. Baltimore: Office of the Actuary/National Health Statistics Group.

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

"CDA Release 2." Section 3: Clinical and Administrative Domains. (2012). Retrieved March 12, 2012, from Cisco Health Information Networking Curriculum.

Circadence (2010) WAN optimization made easy. Retrieved May 2, 2012 from http://www.circadence.com/files/Circadence_WAN_Optimization_Made_Easy.pdf.

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

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

Fineberg, H.V. (2012). A Successful and Sustainable Health System - How to Get There from Here. *New England Journal of Medicine* 366: 1020-1027.

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

Government Health IT. (2011). The Top 5 roadblocks HIEs face. Retrieved March 19, 2012 from http://www.govhealthit.com/news/top-5-roadblocks-hies-face.

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

HIMSS. (2012). Retrieved March 4, 2012 from http://www.himss.org/ASP/topics_ehr.asp.

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

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

Leslie, T. (2012) Realizing the Promise of Health Information Exchange. Retrieved May 10, 2012 from http://www.boozallen.com/media/file/Realizing-the-promise-of-HIE.pdf.

Lewis, W. (2009). LAN Switching and Wireless: CCNA Exploration Companion Guide. Indiana, Cisco Press.

Medpac. (2004). Information Technology in Healthcare. Report to the Congress: New Approaches in Medicare. Retrieved on January 5, 2012 from http://www.medpac.gov/publications%5Ccongressional_reports%5CJune04_ch7.pdf.

National Institutes of Health National Center for Research Resources. (2006). Cost and Return on Investment, National Institutes of Health National Center for Research Resources: 18.

Microsoft. (2006). Connected Health Framework Architecture and Design Blueprint.

Minoli, D. (2008) "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. Retrieved May 12, 2012 from http://common.books24x7.com/toc.aspx?bookid=26424.

Peterson, C. L. & Burton, R. (2007). U.S. health care spending: Comparison with other OECD countries. (RL34175) [Electronic copy]. Washington, DC: Congressional Research Service. http://digitalcommons.ilr.cornell.edu/key_workplace/311/

Oppenheimer, P. (2004) Top-Down Network Design, Second Edition. Cisco Press. 2004. Books24x7. Retrieved March 5, 2012 from http://common.books24x7.com/toc.aspx?bookid=35337.

Shih, A., Davis, K., Schoenbaum, S., Gauthier, A., Nuzum, R. & McCarthy, D. (2008). Organizing the U.S. Health Care Delivery System for High Performance. The Commonwealth Fund.

The Office of National Coordinator for Health Information Technology. (2012a). Electronic Health Records and Meaningful Use. US Department of Health and Human Services, The Office of National Coordinator for Health Information Technology.

The Office of National Coordinator for Health Information Technology (2012b). Health IT. Department of Health and Human Services, The Office of National Coordinator for Health Information Technology.

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

Thompson, T.G. & Brailer, D.J. (2004). The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care. US Department of Health and Human Services. Washington D.C, Office of the Secretary National Coordinator for Health Information Technology.

US Department of Health and Human Services. (2012a). Benefits of Electronic Health Records. Retrieved May 1, 2012, from http://www.healthit.gov/providers-professionals/benefits-electronic-health-records-ehrs.

US Department of Health and Human Services (2012b). Electronic Health Records. Department of Health and Human Services, Centers for Medicare & Medicaid Services.

US Department of Health and Human Services (2012c). Nationwide Health Information Network (NHIN): Background & Scope. Department of Health and Human Services.

US Department of Health & Human Services. (2012d). Summary of the HIPAA Privacy Rule. US Department of Health & Human Services. Retrieved April 23, 2012 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.

Vachon, B & Graziani, R. (2009). Accessing the WAN: CCNA Exploration Companion Guide. Indiana, Cisco Press.

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

Editor's Note:

This paper was selected for inclusion in the journal as a CONISAR 2012 Meritorious Paper. The acceptance rate is typically 15% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2012.

Appendix A: Characteristics of the five widely used WAN technologies.

Table 1a. 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 1b. 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 1c. Asynchronous Transfer Mode

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 1d. Metro Ethernet

METRO ETHERNET NETWORK (MEN)	
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. ♦ Eth. services allow subscribers add bandwidth in small increments (1Mbps). ♦ 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 1e. Internet with the use of Virtual Private Network

VIRTUAL PRIVATE NETWORK (VPN)	
Definition	A 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 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. ♦ The sending and receiving ends must have the necessary hardware and software to set up an encrypted tunnel, which provides the private link. ♦ Tunneling encapsulates an entire packet within another packet and sends the new, composite packet over a network. Tunneling uses three classes of protocols: the passenger protocol, the encapsulating protocol, and the carrier protocol.

Appendix B: Comparison of the widely used WAN technologies.

Table 2. Comparison of WAN Technologies

WAN Type	Leased Line	Frame Relay	ATM	Metro Ethernet	Internet with 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 2. Comparison of WAN Technologies Continued

WAN Type	Leased Line	Frame Relay	ATM	Metro Ethernet	Internet with 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