



UNIVERSITY OF OREGON  
APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary  
Studies Program:  
Applied Information Management  
and the Graduate School of the  
University of Oregon  
in partial fulfillment of the  
requirement for the degree of  
Master of Science

# Wireless Local Area Network Security: A Study of Available Controls for HIPAA Compliance

CAPSTONE REPORT

**Gary Mayer**  
Technology Architect  
The Regence Group

University of Oregon  
Applied Information  
Management  
Program

**Wednesday, June 09,**  
---

722 SW Second Avenue  
Suite 230  
Portland, OR 97204  
(800) 824-2714

Wireless Local Area Network Security: A Study of Available Controls for HIPAA Compliance. a Capstone prepared by Gary Mayer in partial fulfillment of the requirements for the Master of Science degree in the Graduate School of the University of Oregon. This Capstone has been approved and accepted by:

---

Dr. Linda F. Ettinger, Academic Director

---

Date

© 2004 Gary Mayer

An Abstract of the Capstone of Gary Mayer for the degree of Master of Science in the  
University of Oregon Graduate School to be taken June 2004

Title: Wireless Local Area Network Security: A Study of Available Controls for HIPAA  
Compliance

Approved: \_\_\_\_\_

Dr. Linda F. Ettinger

#### Abstract

Security controls that comply with HIPAA security and privacy rules are available to mitigate the risks of Wireless Local Area Networks (WLAN). Controls are classified according to effectiveness in meeting HIPAA requirements. Content analysis on selected literature published from 2002 to 2004 was done to identify threats, vulnerabilities and controls that affect the security and privacy of information transmitted on WLAN systems. Effective controls are discussed and a recommendation is made to enable HIPAA compliance.

## Table Of Contents

Chapter I: Purpose of the Study .....	1
Brief Purpose .....	1
Full Purpose .....	2
Limitations .....	8
Problem Area .....	10
Definitions.....	12
Chapter II: Review of References.....	16
Chapter III: Method .....	24
Collection of Data .....	24
Data Analysis .....	26
Presentation of Data .....	28
Chapter IV: Analysis of Data.....	32
Chapter V: Conclusions .....	39
Appendix A.....	46
Specialized Dictionary: Security Preservation Characteristics.....	46
Appendix B.....	48
Raw Terms identified during coding of Vulnerabilities and Threats .....	48
Appendix C .....	49
Source documents used for content analysis .....	49
Appendix D.....	51
Raw Data – Vulnerabilities.....	51
Appendix E .....	52
Raw Data - Threats .....	52
Appendix F.....	53
Raw Data - Controls.....	53
Bibliography .....	54

**Table of Figures and Tables**

Figure 1 – OSI Reference Model..... 5  
Table 1 – Identified Risks Template ..... 30  
Table 2 – Categorized Risks Template ..... 30  
Table 3 – Categorized Controls Template..... 31  
Table 4 – Control Effectiveness Template..... 31  
Table 5 – Identified Risks ..... 34  
Table 6 – Categorized Risks ..... 36  
Table 7 – Categorized Controls..... 37

## **Chapter I: Purpose of the Study**

### **Brief Purpose**

The current economic environment requires that healthcare organizations deploy Wireless Local Area Networks (or WLANs) in ways that are not only cost effective (Messmer & Cox, 2002), but also secure. Addressing security and privacy of the information transmitted is required by the Health Insurance Portability and Accountability Act (HIPAA). The economic question becomes more clear with the realization that information transmitted over WLAN systems must remain secure and that information security professionals must account for not only the same risks that would be considered on a wired Local Area Network (LAN), but also those risks unique to WLAN (Karygiannis & Owens, 2002).

The purpose of this study is to outline the problem of maintaining information security when WLAN systems are deployed. Information systems security professionals benefit from being able to make well informed and cost effective decisions. Literature review is selected as the larger method of study (Leedy & Ormrod, 2001). Literature is collected in a number of areas: (1) about WLANs; (2) about LANs; and (3) government regulations, in particular, HIPAA. Content Analysis (Krippendorff, 2004) (Palmquist, 2001) is conducted to determine what currently available technical and administrative controls best enable design of a secure WLAN.

In the first stage of data analysis, content analysis (Palmquist, 2001) is conducted to collect information on the risks applicable to LAN and WLAN systems. A “risk” refers to both vulnerable features internal to LAN or WLAN systems and related

threats, within the external LAN or WLAN environment. Content analysis is also used to determine controls (tools, systems and protocols as well as the policies and processes) that are being used to provide mitigation of risks (vulnerabilities with identified threats) with respect to the information security preservation characteristics of confidentiality, integrity, and availability of the data being transmitted (ISO/IEC, 2000). A second stage of content analysis is conducted to identify which of these controls is most often identified as a means to reduce risk in these categories.

The results of the data analysis are intended to be a foundation for the development of a set of recommendations of effective risk controls for use by healthcare organizations; including providers, clearing houses, and payers. Recommendations are framed within the HIPAA requirements concerning information security and privacy: both HIPAA security and privacy rules require controls to prevent compromise of Personal Health Information (PHI). The intention is that these recommendations provide support in making decisions about what controls to use in relation to specific kinds of security and privacy risks. Although the information is designed to be relevant to organizations under information security and privacy requirements such as HIPAA, it should also be applicable to unregulated organizations that need to ensure that proprietary information is not accidentally disclosed.

### **Full Purpose**

The purpose of this study is to identify ways to design Wireless Local Area Networks (WLAN) securely in order to mitigate information security and privacy risks in organizations regulated by laws, including the Health Insurance Portability and Accountability Act (HIPAA) (Gainer, Van Eckhardt, Williams, & Marks, 2003). Literature

related to HIPAA regulations concerning information security and privacy were first released in August 1998 the initial notice of proposed rulemaking was released (Owen, 2000). Final regulations for Privacy took effect on April 14, 2003 and the Security rule will be in effect starting in April 2005. In addition to HIPAA many new state laws are defining how organizations protect information. For example, California Civil Code 1798.80 – 1798.84 (previously known as SB 1386) requires notification of individuals whose personal information has been disclosed.

As a covered entity under HIPAA, health care organizations including providers, clearing houses, and payers must meet HIPAA regulations (CMS, 2003b). This creates the need to ensure that WLAN communications remain secure and private (Gainer et al., 2003), which in turn presents a serious problem to Information systems security professionals who must protect sensitive data from inadvertent release over WLAN systems.

According to ISO-17799 (an International standard for a code of practice for information security management) Information Security relies on the preservation of the following three primary characteristics (2000):

- a) “Confidentiality: ensuring that information is accessible only to those authorized to have access;
- b) Integrity: safeguarding the accuracy and completeness of information and processing methods;

- c) Availability: ensuring that authorized users have access to information and associated assets when required” (p. viii).

HIPAA security and privacy rules are focused on maintaining the confidentiality, integrity, and availability of personal health information (PHI) (Gainer et al., 2003). Specifically the privacy rule is meant to protect the confidentiality of PHI. A core principal of the security rule is to ensure the confidentiality, integrity, and availability of electronic PHI. These two rules mandate that the information security preservation characteristics listed above are maintained. In the HIPAA security rule, transmission security is defined as addressable. This enables a HIPAA covered entity to determine how to address risk, such as “a). implement one or more of the addressable implementation specifications; b) implement one or more alternative security measures; (c) implement a combination of both; or (d) not implement either an addressable implementation specification or an alternative security measure” (CMS , 2003a). While the rule provides flexibility in implementation based on risk analysis, there are many known vulnerabilities in WLAN systems and the associated known threats that constitute a high level of risk to WLAN systems (Arbaugh, Shankar, Wan, & Zhang, 2002; Cox, 2001).

Wired LAN and WLAN share the same Open Systems Interconnection (OSI) reference model that is listed in Figure 1 below (Stallings, 2001). However, the implementation of both is different at the physical layer (Stallings, 2001). While a wired LAN has physical isolation characteristics (e.g. the hacker must have access to the wire), the WLAN does not (e.g. the hacker must only be able to intercept radio frequency signals). Access points (hardware communications hub for users of WLAN)

are points of aggregation for wireless client access (Zahur & Yang, 2004). In other words, to interfere with service in a WLAN, the hacker only needs to create a radio frequency field strong enough to interfere with signal reception of the access point or the wireless client attempting to access it (Geier, 2003; Zahur & Yang, 2004). This is one of many problems identified with early implementations of WLAN, one that increases the complexity and cost of this promising technology.

Application
Presentation
Session
Transport
Network
Data Link
Physical

Figure 1 – OSI Reference Model

In order to determine what controls can be used to mitigate the information security and privacy issues, data is collected in the form of literature on the subjects of LAN and WLAN security as well as HIPAA. Searches are completed using general and specific search engines.

Selected literature is kept to scholarly papers and articles from trade journals and publications for LAN and WLAN Security information published from January 1, 2002 to April 15, 2004. HIPAA information is acquired directly from the government agency responsible for enforcement of the HIPAA security rule, the Centers for Medicare and Medicaid Services and the HIPAA privacy rule, the Office for Civil Rights.

Conceptual content analysis (Palmquist, 2001) is conducted to identify the risks most often associated with use of LAN and WLAN systems. Table 1 (presented in the Analysis of Data chapter of this paper) contains one column that presents the vulnerabilities. Since an identified vulnerability is not a risk without an identified threat, the second column of Table 1 presents the identified threats currently available to exploit the vulnerability. The third column of Table 1 contains the control used to mitigate the risk created by the vulnerability in combination with the threat. The fourth column of Table 1 shows the information security preservation characteristics that the control effectively maintains.

Content analysis is also used to determine controls (tools, systems and protocols as well as the policies and processes) that are used to provide risk mitigation (vulnerabilities with identified threats) with respect to the characteristics of confidentiality, integrity and availability of the data being transmitted. In the second stage of the analysis those terms found in a positive context for the creation of a secure WLAN implementation are identified and noted.

Several outcomes result from this study:

- Table 1 (see the Analysis of Data chapter of this paper) presents risks identified during the conceptual content analysis as being associated with WLAN systems
- Table 2 categorizes the risks identified in Table 1 within a framework of an a priori set of Information Security Preservation

characteristics suggested by ISO-17799 (2000): confidentiality, integrity, and availability.

- Table 3 is a list of controls identified during the content analysis that are also categorized within a framework of an a priori set of Information Security Preservation characteristics suggested by ISO-17799 (2000): confidentiality, integrity, and availability.
- Table 4 is designed to show the relationship the controls have to the HIPAA security and privacy rules and the effectiveness with respect to the characteristics of Information Security Preservation.
- Appendix A is a specialized dictionary that is used to determine what information security characteristic a control will help maintain. It provides a useful reference for information security professionals to use in the future for determining what information security characteristic is being preserved when new controls are reviewed.
- Discussion of specific controls that are identified as effective in information security preservation and keep costs as low as possible as a result of literature review (Leedy & Ormrod, 2001). This information, presented in the Conclusion chapter of the paper, is intended for information security professionals who

are working in the healthcare industry that are designing WLAN systems.

### **Limitations**

The first WLAN standard, 802.11, was published by the IEEE in 1997 (Carney & Soloman, 2002), however, announcement of the first major vulnerability within the 802.11 protocols was August of 2001 (Cox, 2001). This date frames the time limit for collection of information available about the evolution of the WLAN protocol security controls to the period between August 2001 and April 2004. HIPAA was passed into law in 1996, however, the final security rule was not published in the federal register until February 20, 2003, (Grove, 2003) limiting information available until after that date.

The amount of literature focused on the subject of WLAN security is vast, but many of the sources are proprietary intended as sales literature for a specific vendor solution or non-reputable. There is also a large amount of literature that can be uncovered that is not 802.11 based, since wireless LAN (WLAN) is sometimes used to refer to other radio frequency data transmission systems, such as 3GSM, CDMA, GPRS, and others. Literature that is not specifically 802.11 based is not used. The amount of literature that addresses the newest modifications to the IEEE 802.11 protocol family is currently limited, requiring some use of sources that are of reduced quality such as trade publications. Literature produced by WLAN / LAN and security products vendors is not used to prevent the vendor's competitive interests driving the market toward a specific solution.

There are many facets of Information Security that help ensure the confidentiality, integrity, and availability of information that are not covered in this study. These include physical security of the premises where WLAN hardware might be based, the policies that govern the usage of WLAN in an organization, disaster recovery of a WLAN network, and maintaining the security of a WLAN past the point of implementation. This is not to imply that these aspects of information security are not important, the contrary is in fact the case both physical security policy elements must be in place for technical controls to be effective. This study is limited to technical controls that can be used to design a secure WLAN; inadvertent mistakes of human behavior cannot be controlled by administrative policy alone.

For a risk to exist for information security there must be an identified vulnerability, an identified threat, and non-zero likelihood that the vulnerability will be exploited by a threat. For the purposes of this study the existence of vulnerability and threat are considered to be a reasonably anticipatable hazard to information security.

The study focuses on the impact of HIPAA on WLAN security in the context of the security and privacy rules promulgated after HIPAA was enacted into law. The security rule requires that PHI be protected from reasonably anticipated threats (Gainer et al., 2003).

ISO-17799 security definitions were used to frame the data analysis because of its acceptance as an internationally recognized standard for information security management. ISO-17799 makes clear that controls should be selected that (1) reduce risk to an acceptable level and (2) are based on their cost in relation to the reduction of

risks and losses that could be realized if a security breach were to occur. For the purposes of this study, these two factors are what constitute an “effective control”.

### **Problem Area**

There is a need to deploy information technology that enable healthcare firms to be more flexible and efficient, in this case by using wireless systems (Goldberg & Wickramasinghe, 2003). Taking advantage of the convenience of mobile devices and the cost savings of not needing a physical wiring system has pushed more healthcare organizations toward WLAN (Gainer et al., 2003). Although the study focuses primarily on healthcare firms, the information provided will be usable by financial firms, and other firms that require high security of their information systems to protect customer information as well as proprietary trade secrets.

Most healthcare organizations are HIPAA covered entities currently or will be in the future (CMS, 2003b). HIPAA requires that reasonably anticipated threats or hazards to the security or integrity of the information be mitigated (CMS, 2003a). Vulnerabilities that have been identified within the 802.11 wireless protocols (Arbaugh et al., 2002) can now be reasonably anticipated and are ripe of exploitation. Protections are needed now. However, mitigating the complexity and cost of security for WLAN implementations continues to be a concern (Cox, 2003; Phan, 2001; Stehman, 2003).

As part of a study financed by the Blue Cross Blue Shield Association, the consulting group Milliman USA examined health plan administrative costs from 1998 to 2002 to examine the key drivers behind increasing costs (Sacia & Dobson, 2003)

Information Technology expenses increased on average 15% a year during this time. Milliman found that HIPAA costs were a large contributor to this increase.

For information security professionals WLAN implementations add complexity to information security requiring focused attention on the design of a WLAN (Emigh, 2003; Emigh, 2003; Molta, 2004). At the same time the costs associated with WLAN installation and operations can range widely depending on the requirements identified (O'Hara, 2004).

More importantly, however, is that the HIPAA security rule will go into effect starting April 21, 2005 (Gainer et al., 2003). Before the rule goes into effect, healthcare organizations will need to verify that they have appropriate controls in place to ensure they have complied with the HIPAA security rule. There are both civil and criminal penalties in the form of fines and prison sentences associated with the failure to comply with HIPAA regulations, providing a strong incentive for executive management to take these regulations seriously (US Department of Health and Human Services, 2001).

The outcomes in this study provide a simplified method for defining controls that effectively mitigate the risks of WLAN systems. This allows healthcare organizations to take advantage of the new 802.11 protocols used in WLAN systems and remain compliant with HIPAA regulations. This enables information security professionals to provide assurances to executive management that these new systems can be deployed with minimal risk to the business.

## Definitions

**802.1x** – A standard for passing Extensible Authentication Protocol over a Wired or Wireless LAN, allowing a network device to authenticate a device attempting to connect (Snyder, 2002).

**802.11** – The first wireless Ethernet standard adopted and published by the IEEE, using unlicensed 2.4 GHz radio frequency. Maximum transmission rate is 2 Mbps (Carney & Soloman, 2002).

802.11a – A revision to the 802.11 standard that uses unlicensed 5 GHz radio frequency. Maximum transmission rate is 54 Mbps (Carney & Soloman, 2002)

802.11b – A revision to the 802.11 standard that improved transmission speeds to 5.5 and 11 Mbps (Carney & Soloman, 2002)

802.11g – A revision that is backward compatible with 802.11b and increases transmission speed to 54 Mbps (Carney & Soloman, 2002).

802.11i – A specification that can be used to improve the security of 802.11a, b, g protocols (Eaton, 2002)

**CISM** – The Certified Information Security Manager certification is awarded by the Information Systems Audit and Control (ISACA <http://www.isaca.org>) organization. To earn the CISM designation, security professionals are required to successfully complete the CISM examination, adhere to a code of ethics and submit verified evidence of at least five years of information security work experience, with a minimum of three years

of information security management work experience in three or more of the job analysis domains.

**CISSP** – The Certified Information Systems Security Professional is awarded by the International Information Systems Security Certification Consortium ((ISC)<sup>2</sup> <http://www.isc2.org>). To earn the CISSP certification you must subscribe to the (ISC)<sup>2</sup> Code of Ethics, have a minimum 4 years of direct full-time security professional work experience in one or more of the ten domains of the information systems security common body of knowledge or 3 years experience plus a college degree or 2 years experience plus a Bachelor's Degree and a Master's Degree in Information Security from a Center of Excellence (defined on the (ISC)<sup>2</sup> web site).

**Content Analysis** – “Content analysis is a research tool used to determine the presence of certain words or concepts within texts or sets of texts” (Palmquist, 2001)

**Control** – used as mitigation to a known risk, some examples are policies, practices, procedures, organizational structures and software functions (ISO/IEC, 2000).

**Hacker** – “a person who illegally gains access to and sometimes tampers with information in a computer system” (Webster on-line)

**HIPAA** – Health Insurance Portability and Accountability Act (CMS , 2003a).

**Hot spot** – A specific geographic location in which an access point provides public wireless broadband network services to mobile visitors through a WLAN. Hotspots are often located in heavily populated places such as airports, train stations, libraries,

marinas, conventions centers and hotels. Hotspots typically have a short range of access (wi-fiplanet, 2002).

**IEEE** – Institute of Electrical and Electronics Engineers. This organization creates and publishes standards based on member consensus for a variety of areas, including wireless local area network communications systems (IEEE, 2004; IEEE, 2004).

**ISC<sup>2</sup>** – The International Information Systems Security Certification Consortium is an organization devoted to certification of information security professionals who follow a common body of knowledge, a code of ethics, and maintain continued development of skills.

**ISO-17799** – Is an International standard for a code of practice for information security management (ISO/IEC, 2000).

**Literature Review** – Is the review of literature written previously in the area of interest to the researcher (Leedy & Ormrod, 2001).

**Personal Information** – This definition is taken directly from California Civil Code section 1798.80:

(e) For purposes of this section, "**personal information**" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

- (2) Driver's license number or California Identification Card number.
- (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

**Risk** – For Information Security purposes a risk is a vulnerability for which there is a threat in the environment. Additionally there must be a non-zero probability that the exploit will be used against the system for which the risk is being measured (ISO/IEC, 2000).

**Security (*Information Security, Computer Security*)** – Maintaining the confidentiality, integrity and availability of the information stored or transmitted through a device or system. (Howard, 1997; ISO/IEC, 2000; National Communication System Technology and Standards Division, 1996).

**Threat** – Defines an event whose occurrence will have an undesirable impact, e.g. a utility capable of intercepting data, viruses, etc. (Ozier, 2000).

**TKIP** – Temporal Key Integrity Protocol is a encryption protocol that enables the key to change over time making cryptanalysis much harder, hence intercepting information during wireless transmission more difficult (Phifer, 2002).

**VPN** – A Virtual Private Network is a network of virtual circuits for carrying private traffic (Kosiur, 1998).

**Vulnerability** –an absence or weakness of risk reducing controls (Ozier, 2000).

**Warchalking** – “Warchalking is the practice of marking a series of symbols on sidewalks and walls to indicate nearby wireless access” (Swartz, 2004).

**Wardriving** – The process of searching for open wireless local area networks using automated detection software in combination with global positioning satellite systems. Originally developed by Peter Shipley (Shipley, 2003).

**WEP** – Wired Equivalent Privacy is a security protocol that uses encryption to secure wireless communications over 802.11 protocols (Searchsecurity.com, 2002).

**WPA** – Wireless Protected Access is an interim security standard created by the Wi-Fi alliance that uses some of the mechanisms that are provided as part of the 802.11i protocol (enhancement to the 802.11 protocols) (Webopedia, 2002).

**WPA II** – See 802.11i

**WLAN** – WLAN or Wireless Local Area Network is another name for the Wireless Ethernet standards created by the IEEE. These standards consist of the 802.11 family of protocols (Carney & Soloman, 2002).

## **Chapter II: Review of References**

The method used for this study is based on literature review as discussed in Creswell’s Research Design text (2003). This section provides a review of the references that are key to its development. Three areas are discussed within each of the reviews:

1. A brief summary of the content relative to the purpose and/or problem area of this study
2. A description of how the reference was used as support in this study
3. The criteria used to select the reference

**Baker, D.** (2003). *Wireless In(Security) for Health Care*. San Diego, CA: Science Applications International Corporation.

Baker's article is written for the Health Information Management and Management Systems Society (HIMSS), a respected group that provides certification of professionals in healthcare information systems. It discusses WLAN in detail and is based on the apparent acceptance of Wireless in healthcare even though there are widely known security risks associated with it.

This white paper is a rich source of information for the data analysis portion of this study and provides tables that define vulnerabilities and threats to the WLAN environment, as well as potential controls to mitigate those risks. Baker works for SAIC, an organization well known in the healthcare field in supplying leading edge solutions. This source is selected because the author is the CTO for SAIC and cited references that support the assertions made in her paper. The white paper also has the support of SAIC and HIMSS.

**CMS 45 CFR Parts 160, 162, and 164** Health Insurance Reform: Security Standards; Final Rule. Department of Health and Human Services.

The HIPAA final security rule is enforced by the Centers for Medicare & Medicaid Services. This is the document that enforcement is based upon. The HIPAA Security rule was written for to ensure that guidelines existed that would protect private health information. The final rule documentation is selected to frame the topic within the purpose statement by identifying that WLAN communications must remain secure. It frames part of the problem area by discussing what areas must be addressed in securing WLAN communications. This source was chosen because it is the definitive source from the US government on the HIPAA security rule that affects HIPAA covered entities.

**Creswell, J.** (2003). *Research Design Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks, CA : Sage Publications.

Creswell's Research Design text describes the process of Literature review as that process was implemented in this study. This text is selected because it is used as one of the texts for the University of Oregon's Applied Information Management Program in the Research Methods course. Creswell is professor in Quantitative and Qualitative Methods in Education at the University of Nebraska - Lincoln and specializes in Research Methods.

**Gainer, R., Van Eckhardt, M., Williams, R., & Marks, R.** (2003). *No Rest for the Wary* Vol. 8(20) National Bureau of Affairs.

*No Rest for the Wary* is a discussion of WLAN security issues within the framework of the HIPAA security and privacy rules. While discussing the issues around

HIPAA for healthcare organizations, the authors describe the risks of the WLAN protocols as well as the controls that might be used to mitigate the risks.

This report contains information that is used to frame and focus the topic of this study, define the limitation of context, and define the problem area. Parts of the report also contain information used during the content analysis of the literature. The report is selected because it was written recently, is well referenced and covers all of the topic elements of this study.

**Government of Canada.** (2003). 802.11 Wireless LAN Vulnerability Assessment. Ottawa, Ontario, Canada: Government of Canada.

The 802.11 Wireless LAN Vulnerability Assessment done by the Canadian Government was written to identify the vulnerabilities of WLAN systems and convey a comprehensive security solution so that WLAN systems could be deployed safely for the Government of Canada.

The Wireless LAN Vulnerability Assessment contains information about 802.11 vulnerabilities from a number of sources and provides a great deal of information that was used in the data analysis section of this study. This source is selected because it is issued under the authority of the Chief of the Canadian Communications Security Establishment. The document is professionally organized and was written in May 2003 making it timely as well.

**Henry, P., & Luo, H.** (2002). WiFi: What's Next? Vol. 40(12), 66-72. New York, NY: IEEE.

This document was published in the IEEE Communications Magazine and discusses some of the challenges and solutions to deploying 802.11b; one of the WLAN protocols. The authors discuss many of the conveniences and potential uses of WLAN, and include a discussion of WLAN security.

The article provides substantial information for the data analysis portion of this study, discussing both risks and controls to mitigate the risks. This source was selected because it was accepted in an IEEE publication, the credentials of the researchers; Paul Henry has a Ph.D. in physics and is currently the head of the Broadband Wireless systems research division for AT&T Labs, Hui Luo holds a Ph.D. in Electrical Engineering and is a researcher at AT&T Labs in the areas of wireless/mobile networking, network security and signal processing for wireless communications. The work also contained strong supporting references.

**ISO/IEC.** (2000). International Standard 17799: Information technology — Code of practice for information security management. Switzerland: ISO.

ISO 17799 is an international standard for Information Security Management is based on the British Standard 7799. The standard is used broadly by information security professionals as a reference for guiding information security management. The standard was selected to define the a priori set of characteristics used in the Data Analysis section of this paper to code risks and controls. This source was chosen because it is recognized by an internationally accepted standards organization and is authoritative in the area of Information Security Management.

**Karygiannis, T., & Owens, L.** (2002). Wireless Network Security 802.11, BlueTooth and Handheld devices. NIST.

Also known as the National Institute of Standards and Technology (NIST) Special Publication 800-48, this document was written to provide government agencies with guidance to deploying wireless technologies. Government contractors, such as those processing Medicare claims, are also subject to provisions within the NIST Special Publications. This document helped frame the purpose of the study, providing definitions and also provided input to the Analysis of Data section of this paper.

The paper was selected because NIST is a well respected government agency in providing standards for Security of government related systems. Tom Karygiannis holds a MS.c. in Electrical Engineering and a Ph.D. in Computer Science, as well as 12 years experience in IT organizations. Les Owens is a respected cryptographer with several patents in the areas of cryptography and network security. The paper is professionally organized and leads the reader through the subject with clarity.

**Palmquist, M.** (2001) Content Analysis [Web Page]. URL  
<http://writing.colostate.edu/references/research/content/index.cfm>  
[2004, April 14].

This source is presented via a website that is a part of the Writing Center at Colorado State University. It contains information about content analysis and the subtopics of conceptual analysis and relational analysis. Conceptual content analysis is used in this study as a method of data analysis, in particular using the specialized dictionary mentioned in the overview of the conceptual analysis area. This site was

selected because it is professionally organized and focuses specifically on the topic of interest only (in this case content analysis). In addition, Palmquist has been published in a number of journals, and he focuses on the area of research writing and communications technologies.

**Rittinghouse, J., & Ransome, J. (2004).** Wireless Operational Security (first ed.).

Burlington, MA: Elsevier Digital Press.

This book, published in February 2004, is a comprehensive look at Wireless LAN Security and provides in-depth discussion of the topic. Rittinghouse completed his doctoral dissertation on a security model that could be used for Wireless; Wireless Integrated Secure Data Options Model (WISDOM). That security model is presented in the book and covers vulnerabilities, threats, and controls to mitigate them.

Discovered late in this study, this book is used in as a source of data for analysis. The book was selected primarily because of the author's credentials, John Rittinghouse has a PhD and is also a Certified Information Security Manager (CISM) and James Ransome is a Certified Information Systems Security Professional (CISSP) and a CISM. Both the CISSP and CISM require extensive knowledge and experience. In addition the book provides references for assertions and the subject is covered thoroughly.

**Zahur, Y., & Yang, T. (2004).** Wireless LAN Security and Laboratory designs. 19(3), 44-60.

As part of the process to design a course at the University of Houston – Clear Lake on Wireless Computing and Society, the authors conducted a survey of WLAN

standards, features, and vulnerabilities. Additionally they conducted a survey on security mechanisms (controls) that may be adopted to enhance WLAN security.

This information is well suited for inclusion in the data analysis portion of this study since it contains information on vulnerabilities and controls. This article is selected because it is professionally organized, published in the Journal of Computing in Small Colleges and also written very recently. One of the author's credentials were also taken into account; T. Andrew Yang holds a Ph.D. in Computer Science and is an Associate Professor at the University of Houston – Clear Lake.

## **Chapter III: Method**

The method selected for this study is literature review as discussed in the text Research Design (Creswell, 2003). Literature review is used to focus on the results of previous work done in the same area of research. Within the context of this study literature on securing WLANs is gathered and refocused to align with literature that addresses the needs of organizations subject to HIPAA regulation that want to deploy WLAN in a secure and cost effective manner.

### **Collection of Data**

Collection of data is done with key terms that included: 'wireless networking security', 'WLAN security 802.11', Wired Equivalent Privacy ('WEP'), Wireless Protected Access ('WPA'), '802.11i', Temporal Key Integrity Protocol ('TKIP'), Wireless Security and '802.1x'. Initial terms were identified during the preliminary discovery of literature on this topic.

The first repository of information searched is the Association for Computing Machinery's (ACM) digital library and started with the search term of 'WLAN security 802.11'. The date range was restricted to January 2002 to present because during the initial discovery of literature for this topic; this researcher found that literature was extremely limited on this topic prior to January 2002. This is likely due to the announcement of the vulnerability in August of 2001 (Cox, 2001), and the subsequent amount of time for experts to review possible solutions. The ACM digital library uses a relevance rating for the results ranging from very high relevancy to very low relevancy. This search string retrieved 200 results. Many of the articles covered only part of the

Further searching of the site with other key terms resulted in smaller numbers of articles. Many article titles were retrieved multiple times within the searches.

The next search is done on the Inspec database on the University of Oregon library web site. The key term 'WLAN Security' resulted in 14 returned results that were all within the limitation time frame. Not all of the results were specifically relevant to the topic; WLAN and other wireless terms sometime returned results that were focused toward cellular and other wireless (radio frequency) systems. Those articles not specifically addressing the vulnerabilities, threats and controls for 802.11 security are not collected. During examination of these articles, many were found to be duplicates with ACM articles, but an additional two articles are used in this study.

The Teoma Internet search engine is also utilized during the compilation of literature. It is used because of the capability to quickly drill down further into relevant areas that are identified by the search engine itself. Again the same criteria are used as with the other search engines. The results from this Internet search resulted in a lot of initial articles, narrowing down the results was difficult and many articles did not meet the criteria for inclusion. Several articles are included in this study.

For this study the quality of information hinges on factors that are defined as currency of information, where the information is published, and whether any information is biased toward a specific vendors technology (Bell, 2003; Harris, 1997). Because of the ongoing development of newer security controls, such as the 802.11i

protocol enhancements with IEEE, literature developed recently is of significantly more value to the study. Where the literature is published and by whom the literature is written is important in determining whether any particular vendor had too much influence in its development. Additional factors were used such as the authors credentials, and overall professional design of the literature.

### **Data Analysis**

This study is designed to build on selected information available in literature that is applicable to the topic. Conceptual content analysis lends itself to this effort by examining the content of literature in search of the frequency of particular terms, phrases and concepts used (Palmquist, 2001). In this case, the analysis is designed to aid in identification of risks, and controls that are essential to determining the preservation of information security that is also cost effective, when designing a WLAN. The specific goal of this process is to identify the most effective methods for controlling risk associated with WLAN.

The first coding process identifies the vulnerabilities and threats, combined into risk, associated with WLAN systems. In the next step the risks are categorized using the a priori characteristics of Information Security Preservation (Confidentiality, Integrity, Availability) (ISO/IEC, 2000), and in many cases a combination of these characteristics.

The second coding process identifies the controls that can be used to mitigate the risk associated with the vulnerabilities and threats identified in the previous steps. Controls are also categorized by the a priori characteristics of Information Security Preservation. Analysis is then done to determine the controls that are effective across

all of the categories and which of the two HIPAA rules (security and/or privacy) are met by using them. This is done by reviewing how the risks were categorized across the a priori characteristics of information security preservation (ISO/IEC, 2000).

The decision to frame a direct “cause and effect” relationship between a specific control and a specific risk can be subjective. In cases where the control is explicitly discussed in terms of reduction of a particular characteristic of risk, this is easier to code. In cases where the control is not explicitly discussed with respect to the reduction of a particular characteristic of risk, additional research is done to best determine what characteristic is reduced.

A list of relevant terms is included in the Definitions section of this study and also as a separate Appendix (see Appendix A). The definitions can be viewed as a “specialized dictionary” (as described by Palmquist, 2001) and may be used as an additional resource of the study.

The following tools were used to support the collection and analysis of the literature:

- **ProCite:** A bibliographic database that aids with the collection, organization, searching and reference of materials that have been gathered. The tool allows the bibliographic entry to be annotated with notes and keywords that help organize the information for quick retrieval.

- **SurfSaver:** A product that is added to your browser to enable snapshots of the webpage to be stored in a database. It also allows for annotation with keywords and notes that can be used to help organize the information for quick retrieval
- **Microsoft Excel:** This product is a spreadsheet software program that is used to categorize and code the vulnerabilities, threats, and controls that are applicable.

Once the information resulting from the data analysis is categorized and coded, themes and patterns are evident. Controls that are categorized effective across all of the a priori characteristics of Confidentiality, Integrity, and Availability (ISO/IEC, 2000) are considered more effective than those that are only categorized in one or two of the a priori characteristics.

### **Presentation of Data**

The outcomes of Data analysis are presented in four tables and a series of six Appendices:

- Appendix A contains a “specialized dictionary” [as defined on the Palmquist site (2001)] that gives guidance to performing the conceptual content analysis. The specialized dictionary contains definitions of key terms that help determine what types of information security preservation characteristics are applicable according to the ISO/IEC, 2000: Confidentiality, Integrity, or Availability.

- Appendix B provides a listing of all terms identified in the initial conceptual content analysis related to vulnerabilities and threats (combined into risk) associated with WLAN systems.
- Appendix C contains a list of the source documents used for content analysis in bibliographical format and numbered for referencing within the study.
- Appendix D contains the matrix used to code for vulnerabilities and lists the number of sources that the vulnerabilities are found in.
- Appendix E contains the matrix used to code for threats and lists the number of sources that the threats are found in.
- Appendix F contains the matrix used to code for threats and lists the number of sources that the threats are found in.
- Table 1 provides a grouping of WLAN Security vulnerabilities and threats that make up numbered risks. Table 1 is produced by merging the list of vulnerabilities resulting from the first coding process, presented in Appendix D and the list of threats also resulting from the first coding process, presented in Appendix E. A template for Table 1 is presented below. The vulnerability column contains instances discovered in the 802.11 protocols and documented in the literature. The threat column

contains threats to 802.11 WLAN systems identified in the literature.

Risk Number	Vulnerability	Threat

Table 1 – Identified Risks Template

- Table 2 Categorizes the risks identified in Table 1 (combined vulnerability and threat) according to an a priori set of characteristics of Information Security Preservation (confidentiality, integrity, and availability) (ISO/IEC, 2000). The Template for Table 2 is presented below

Risk Number	Confidentiality	Integrity	Availability

Table 2 – Categorized Risks Template

- Table 3 is the result of coding the controls identified as being used to mitigate risks in WLAN systems (see Appendix F). The controls are also categorized by the a priori characteristics of Information Security Preservation (ISO/IEC, 2000). The template for Table 3 is shown below.

Control	Confidentiality	Integrity	Availability

Table 3 – Categorized Controls Template

- A final outcome, Table 4, is used to support a discussion of the specific controls that are both effective in preserving information security (as defined by HIPAA Rule Compliance) and keeping costs as low as possible. This discussion frames the construction of the Conclusions chapter of this study. This discussion is designed to be of greatest use to information security professionals who are working in the healthcare industry, and who are responsible for the design of WLAN systems that are both secure and cost effective. The template for Table 4 is shown below.

Control	HIPAA Rule Compliance	Overall Effectiveness

Table 4 – Control Effectiveness Template

## Chapter IV: Analysis of Data

A total of 16 documents are used during the data analysis step, selected on the basis of timeliness (published during or after January 2002), the credentials of the authors, and where the documents were published. A list of the 16 documents is located in Appendix C.

The first step is to code for the vulnerabilities and threats. All the terms identified are listed in Appendix B. Once the vulnerabilities are coded (see Appendix D), the data is reviewed and items that are only found in one of the sources are eliminated since there is no verification from other sources. One other vulnerability was dropped, Problems in 802.11b Ethernet protocol, because there is not an identified threat associated with it.

The same process is used for the threats identified (see Appendix E); those identified in only one source are eliminated. Access Point (AP) cloning is combined into the Rogue AP entry, since they are used in the same context. Malware and Trojans are excluded as they are a threat to the client OS of a system.

During the coding the vulnerabilities and threats are identified in the context in which they are found, for instance many types of vulnerabilities and threats are discussed in the context of Denial of Service (DoS) attacks. As revealed through a preliminary review of the context of each instance, vulnerabilities that result from shortcomings internal to the systems can be a result of poor design, failure to properly implement a design feature, or some combination of these items. A preliminary review of the context of each instance reveals that some threats are created externally to the

systems either by environmental factors (such as natural radio interference from the sun), or by human design; examples are hacker tools that use cryptanalysis to break an encrypted communication (Government of Canada, 2003).

The contextual data is summarized in a column labeled Type, in both Appendix D: Vulnerabilities and Appendix E: Threats. The identification and inclusion of contextual data is done to enable the researcher to combine vulnerabilities and threats to form a set of Risks. The final results of this process are presented below in Table 5, which shows the set of Vulnerabilities and Threats, aligned as ten Risks.

Risk Name	Vulnerability	Threats
Loss of Confidentiality and Integrity from flawed encryption	Wired Equivalent Privacy (WEP) protocol	<ul style="list-style-type: none"> <li>▪ WEP Protocol Attacks</li> <li>▪ Eavesdropping</li> </ul>
Loss of Confidentiality, Integrity and Availability if SSID is the only authentication (interception of network ID)	Service Set Identifier (SSID)	<ul style="list-style-type: none"> <li>▪ War Driving</li> </ul>
Loss of Availability by assuming control of AP	Simple Network Management Protocol (SNMP)	<ul style="list-style-type: none"> <li>▪ AP Takeover</li> </ul>
Loss of Confidentiality and Integrity from intercepted credentials	Shared Key Authentication	<ul style="list-style-type: none"> <li>▪ Traffic Sniffing</li> </ul>
Loss of Availability due to spoofing	Media Access Control Access Control List (MAC ACL) can be spoofed	<ul style="list-style-type: none"> <li>▪ MAC address switching</li> </ul>
Loss of Confidentiality, Integrity and Availability from uncontrolled emanations	Exposed Access Points	<ul style="list-style-type: none"> <li>▪ War Driving</li> </ul>
Loss of Confidentiality and Integrity due to communications interception	One Way authentication (Weak end-point binding)	<ul style="list-style-type: none"> <li>▪ Man-in-the-Middle attack</li> <li>▪ Session Hijacking</li> <li>▪ Rogue AP</li> </ul>
Loss of availability because of Interference from neighboring WLAN systems	Overlapping spectral footprint between 802.11 systems (RF Interference)	<ul style="list-style-type: none"> <li>▪ RF Interference</li> </ul>
Loss of availability because of Interference from other systems in the 2.4 GHz frequency range or active Jamming	RF Interference (non 802.11 systems, such as Microwaves, Cordless Phones, Jammers)	<ul style="list-style-type: none"> <li>▪ RF Jamming</li> </ul>
Loss of availability due to multiple unauthorized AP associations	DHCP	<ul style="list-style-type: none"> <li>▪ War Driving</li> </ul>

Table 5 – Identified Risks

Next the risks identified in the initial coding are classified by using the a priori characteristics of Information Security Preservation (ISO/IEC, 2000). The method used for classifying the risks is to examine the contextual description in the source document, in order to determine what impacts these risks have to Information Security preservation. The results of this process are shown below in Table 6.

Risk Name	Confidentiality	Integrity	Availability
Loss of Confidentiality and Integrity from flawed encryption	✓	✓	
Loss of Confidentiality, Integrity and Availability if SSID is the only authentication (interception of network ID)	✓	✓	✓
Loss of Availability by assuming control of AP	✓	✓	✓
Loss of Confidentiality and Integrity from intercepted credentials	✓		
Loss of Availability due to spoofing	✓		
Loss of Confidentiality, Integrity and Availability from uncontrolled emanations	✓	✓	✓
Loss of Confidentiality and Integrity due to communications interception	✓	✓	
Loss of availability because of Interference from neighboring WLAN systems			✓
Loss of availability because of Interference from other systems in the 2.4 GHz frequency range or active Jamming			✓
Loss of availability due to multiple unauthorized AP associations			✓

Table 6 – Categorized Risks

The next step was to code for controls that can mitigate the risks identified in the previous steps. Once identified (see Appendix F), controls are also classified by using the a priori characteristics of the Information Security preservation characteristics (ISO/IEC, 2000) as a way to determine how the controls apply to HIPAA Privacy and Security rule compliance. Many of the sources indicated whether a control was related

to confidentiality, integrity, or availability. In cases where they were not easily determined by context or explicit mention, the specialized dictionary in Appendix A was used to determine what characteristic(s) were impacted. The results are presented in Table 7 shown below.

Control	Confidentiality	Integrity	Availability
Limit Range of WLAN coverage	✓	✓	✓
Directional antenna pattern	✓	✓	✓
Wireless security policy	✓	✓	✓
802.1x authentication at AP w/Extensible Authentication Protocol (EAP)	✓	✓	
Wireless Intrusion Detection System (IDS)	✓	✓	✓
Virtual Private Network (VPN)	✓	✓	
Wi-Fi Protected Access (WPA)	✓	✓	
802.11i Security standard	✓	✓	✓
Temporal Key Integrity Protocol (TKIP)	✓		
Message Integrity Check (MIC)		✓	
Advanced Encryption Standard (AES)	✓		
Personal Firewall on Clients	✓	✓	
Turn off Dynamic Host Control Protocol (DHCP)			✓

Table 7 – Categorized Controls

Many of the controls initially identified in the raw data (see Appendix F) are not used in Table 7. Several of the controls are only found in one of the source documents and are not considered as a generally accepted control because of this. Wired Equivalent Privacy (WEP) is considered to have too many flaws to be used for security, and is considered to be a vulnerability in all of the articles used in the content analysis; except for the AusCERT bulletin (2004) (a list of the articles examined is included in Appendix B).

Media Access Control (MAC) Access Control Lists (ACL) are eliminated from consideration because they are identified as a vulnerability in sources 1, 2, 3, 9, 11,13,14,15 (listed in Appendix C). Any SSID controls are eliminated from consideration because they are not considered to be security controls, but network association identifiers (Government of Canada, 2003). RSN is combined with 802.11i, as it is the main part of the IEEE 802.11i draft proposal. Personal Firewalls was discussed in context with protecting the client system from intrusion, not protecting the Wireless network communications, and was eliminated. Turning off Dynamic Host Configuration Protocol (DHCP) services was pointed to as a control to prevent a station from receiving an IP address (in other words, a static IP would be required and you would have to know it) but this is a method for providing configuration information and not a security control for wireless networks and is therefore not used.

A final step in data analysis is done to determine how the individual controls help comply with the HIPAA Privacy and Security rules, and the overall cost effectiveness of the controls. As a result, Table 4 is created to align controls with HIPAA Privacy and Security rules. Table 4 is used to support a discussion of the specific controls that are both effective in preserving information security (as defined by HIPAA Rule Compliance) and in managing costs. This discussion, designed to be of greatest use to information security professionals who are working in the healthcare industry and who are responsible for the design of WLAN systems that are both secure and cost effective, frames the construction of the Conclusions chapter of this study.

## Chapter V: Conclusions

WLAN equipped systems are becoming common place in Healthcare organizations because of potential savings in deployment and the convenience of use for any number of purposes (Gainer, Van Eckhardt, Williams, & Marks, 2003). Unfortunately, the security of information transmitted over these systems can be at risk due to the poor information security controls available within WLAN protocols (Gainer, Van Eckhardt, Williams, & Marks, 2003; Baker, 2003). Regulation of Healthcare information in the form of HIPAA Security and Privacy rules makes the protection of this information a priority for covered entities (CMS , 2003a). Information security professionals are left to determine what controls will be used to mitigate the risks from the gaps in WLAN protocols.

This study has examined the controls most often identified as a means to ensure the preservation of the Information Security characteristics as identified within the ISO 17799 Information Technology – Code of practice for information security management (2000). By identifying the controls most commonly associated with correcting the loss of the Information Security preservation characteristics, recommendations can be made as to which ones can be used to effectively mitigate the risks identified with information transmission on WLAN systems. Information Security professionals should always perform a risk assessment within their organization's environment, however, the recommendations provided here provide mitigation to most of the risks identified.

Thirteen controls are listed in Table 8 that partially or completely mitigate the risks associated with transmitting health care information over WLAN systems. A discussion of these controls and their effectiveness of each follow.

Control	HIPAA Rule Compliance	Overall Effectiveness
Limit range of WLAN coverage	Security	Partial
Directional antenna pattern	Security	Partial
Wireless security policy	Security Privacy	Partial
802.1x authentication at AP w/EAP	Security	Partial
Wireless Intrusion Detection System (IDS)	Security	Partial
Virtual Private Network (VPN)	Privacy Security	Complete
Wi-Fi Protected Access (WPA)	Security Privacy	Partial
802.11i security standard	Security Privacy	Complete
Temporal Key Integrity Protocol (TKIP)	Privacy	Partial
Message Integrity Check (MIC)	Security	Partial
Advanced Encryption Standard (AES)	Privacy	Partial
Personal firewall on clients	Privacy Security	Partial
Turn off DHCP	Security	Partial

Table 8 – Effective Controls

- 1. Limit range of WLAN coverage:** Limiting the range of the WLAN coverage is recommended to prevent inadvertent access from areas outside the intended coverage area (Government of Canada, 2003). Limiting the range reduces the risk that someone will intercept traffic, but it does not protect information traveling within the intended area of coverage (Karygiannis & Owens, 2002). Because it does not protect information transmitted over WLAN, it is only partially effective in providing compliance with the HIPAA security rule and not effective for compliance with the HIPAA privacy rule.

- 2. Directional antenna pattern:** Use of directional antennas instead of omnidirectional has a similar effect as limiting the range of WLAN coverage. It helps keep the signal isolated to the area to which it is intended (Government of Canada, 2003). Using a directional antenna reduces the risk that someone will intercept traffic, but it does not protect information traveling within the intended area of coverage (Karygiannis & Owens, 2002). Because it does not protect information transmitted over WLAN, it is only partially effective in providing compliance with the HIPAA security rule and not effective for compliance with the HIPAA privacy rule.
- 3. Wireless security policy:** A WLAN security policy is foundational to guiding how wireless will be used and how employees will behave when using wireless (Baker, 2003). Wireless security policy is partially effective in complying with HIPAA security and privacy rules as it cannot protect the actual transmission of information, unless the policy is to not use WLAN systems.
- 4. 802.1x authentication at AP w/EAP:** The 802.1x protocol used with the extensible authentication protocol allows wireless clients to be authenticated at the time of association with an Access Point (Karygiannis & Owens, 2002). This method of authentication is partially effective at complying with the HIPAA security since it can prevent unauthorized users from gaining access to the LAN thereby protecting information assets. It cannot protect the privacy of information that is transmitted over WLAN, however.

- 5. Wireless Intrusion Detection System (IDS):** Wireless IDS are designed to detect intrusions by using passive methods such as traffic analysis or watching for wireless MAC addresses (Government of Canada, 2003). Because Wireless IDS are passive detective controls, they cannot protect a network from intrusion and are, therefore, only partially effective at complying with the HIPAA security rule. They are not effective at protecting the privacy of information transmitted.
- 6. Virtual Private Network (VPN):** VPN provides encryption of the information in transit as well as integrity checking of the information transmitted (Housley & Arbaugh, 2003). Depending on the implementation, strong authentication may be used as well. Correctly implemented VPN systems can be completely effective in maintaining compliance with HIPAA security and privacy rules for WLAN systems.
- 7. Wi-Fi Protected Access (WPA):** WPA is an interim improvement to WEP that does provide better protection for data, but it is not a complete solution (Government of Canada, 2003; Karygiannis & Owens, 2002). WPA is considered a partially effective measure for compliance with HIPAA security and privacy rules.
- 8. 802.11i security standard:** The 802.11i security standard is not yet ratified by the assigned IEEE task group, but it includes many of the other controls listed in this study including 802.1x, TKIP, MIC, and AES (Karygiannis & Owens, 2002; Cam-Winget & Housley & Wagner & Walker, 2003). 801.11i

could be completely effective in maintaining compliance with HIPAA security and privacy rules for WLAN systems.

**9. Temporal Key Integrity Protocol (TKIP):** TKIP is a protocol used in both WPA and 802.11i and provides protection for the keys used to encrypt information transmitted on WLAN. It is intended as a replacement to the flawed WEP protocol (Government of Canada, 2003; Karygiannis & Owens, 2002; Cam-Winget & Housley & Wagner & Walker, 2003). Because it does not correct some of the other problems with WLAN, such as authentication, it is partially effective in complying with the HIPAA privacy rule and not effective in complying with the HIPAA security rule.

**10. Message Integrity Check (MIC):** MIC is a protocol used in 802.11i to ensure the integrity of the information transmitted over WLAN (Government of Canada, 2003; Karygiannis & Owens, 2002). MIC is intended to protect information integrity during transmission; it does not encrypt information by itself. For this reason it is partially effective in complying with the HIPAA security rule, and not effective in complying with the HIPAA privacy rule.

**11. Advanced Encryption Standard (AES):** AES is the US government encryption standard verified under FIPS 140-2 (Karygiannis & Owens, 2002). It is expected that it will be used in future releases of 802.11 protocols. AES is considered partially effective in complying with the HIPAA privacy rule because it enables information to be encrypted, however, since it does not

provide authentication it is considered not effective for the HIPAA security rule.

**12. Personal firewall on clients:** Personal firewalls can provide protection to the WLAN client system by preventing certain types of attacks (Government of Canada, 2003; Karygiannis & Owens, 2002). Personal firewalls are considered partially effective in complying with HIPAA security rules, but do not protect the information during transmission so are not effective in maintaining privacy.

**13. Turn off DHCP:** Turning off DHCP will prevent a client system from receiving an IP address thereby requiring the system to have an IP address already configured within the proper subnet (Karygiannis & Owens, 2002). This is considered to be partially effective in complying with HIPAA security, but does not provide any protection to transmitted data so is not effective in preserving privacy.

In reviewing the literature used in this study, this researcher found the use of VPN or 802.11i the most compelling of the two controls. Both controls protect against all of the risks identified, except Loss of availability because of Interference from other systems in the 2.4 GHz frequency range or active Jamming and Loss of availability because of Interference from neighboring WLAN systems. However, because 802.11i is not yet released and will need to be commercialized after it is made a standard, information security professionals will likely find that VPN is the best solution available at this time to comply with HIPAA security and privacy rules. Authors of the literature

reviewed in this study did commonly point out that VPN should be used in combination with other controls in order to provide a complete solution (Baker, 2003; Government of Canada, 2003).

Unfortunately the risk of Loss of availability because of Interference from other systems in the 2.4 GHz frequency range or active Jamming and Loss of availability because of Interference from neighboring WLAN systems did not appear to have effective controls available at this time. Consequently those two risks remain as part of any deployment and should be taken into consideration as deployment is done. If a system must be relied on for control of real time systems or available for critical systems, support of 911 for instance, options other than WLAN need to be considered.

## Appendix A

### Specialized Dictionary: Security Preservation Characteristics

**Man-in-the-Middle** – A scenario that results from weak mutual authentication, enabling a third party to intervene unobtrusively, by fooling the two parties communicating into believing they are talking to each other. This allows the third part to intercept communications from both parties, read them and potentially modify them as well. This represents a threat to both **Confidentiality** (if the third party can read the message) and **Integrity** (if the third party can make modifications to the message) (Baker, 2003).

**Monitoring and Interception** –Types of attacks that usually involve passive information gathering by using a network traffic sniffer or analyzer. Since this is a passive method, **Confidentiality** is at greatest risk (Government of Canada, 2003).

**Port Based Network Access Control** – 802.1x is an IEEE standard designed to provide an authentication mechanism for connecting to a network resource; in the case of a wired network, a port on a network device, or in the case of a wireless network, authentication to an Access Point. The purpose is to prevent connections to a network device unless a user is authorized, preventing some forms of DoS type attacks (Karygiannis & Owens, 2002). DoS attacks affect the **Availability** of network services.

**Wardriving** – The process of searching for open wireless local area networks using automated detection software in combination with global positioning satellite systems. Originally developed by Peter Shipley (Shipley, 2003). Wardriving is used as a method

of Network Discovery. Networks identified with this process can then be used to compromise **Confidentiality, Integrity, or Availability**.

## Appendix B

### Raw Terms identified during coding of Vulnerabilities and Threats

CSMA/CD MAC (Ethernet Protocol methodology)	War Driving
Service Set Identifier (SSID)	Network Discovery
Media Access Control Access Control List (MAC ACL)	Network access via wireless router
Shared Key Authentication	Denial-of-Service
Wired Equivalent Privacy (WEP) protocol	AP Takeover
Configuration Defaults	AP Cloning (Masquerading)
Simple Network Management Protocol (SNMP)	RF Jamming (interference)
Exposed Access Points	WEP Protocol Attacks
One Way authentication (rogue access point problem)	Passive Attack
Overlapping spectral footprint (radio frequency interference)	Active Attack
Traffic Redirection	Decryption table attack
Masquerading AP	Eavesdropping
Weak binding of endpoints	Traffic Sniffing
Lack of flood protection	Man-in-the Middle attack
Client Platform Security Vulnerabilities	Rogue AP
Dynamic Host Configuration Protocol (DHCP)	SSID discovery
Radio frequency interference	Traffic Analysis
Distance interception	Zero Configuration systems
	MAC Address switching
	Trojans, Malware
	Device Theft to obtain MAC
	Session Hi-Jacking

## Appendix C

### Source documents used for content analysis

Number	Source
1	Government of Canada. (2003). 802.11 Wireless LAN Vulnerability Assessment. Ottawa, Ontario, Canada: Government of Canada.
2	Baker, D. (2003). Wireless In(Security) for Health Care. San Diego, CA: Science Applications International Corporation.
3	Zahur, Y., & Yang, T. (2004). Wireless LAN Security and Laboratory designs. 19(3), 44-60.
4	Henry, P., & Luo, H. (2002). WiFi: What's Next? Vol. 40(12), 66-72. New York, NY: IEEE.
5	Gainer, R., Van Eckhardt, M., Williams, R., & Marks, R. (2003). No Rest for the Wary Vol. 8(20)National Bureau of Affairs.
6	Vaughan-Nichols, S. (2004) Beyond WEP [Web Page]. URL <a href="http://www.wi-fiplanet.com/tutorials/article.php/1490451">http://www.wi-fiplanet.com/tutorials/article.php/1490451</a> [2004, May 1].
7	Cohen, A and O'hara B. 802.11i shores up wireless security [Web Page]. 1926 May 3; Accessed 1924 Apr 4. Available at: <a href="http://www.nwfusion.com/news/tech/2003/0526techupdate.html">http://www.nwfusion.com/news/tech/2003/0526techupdate.html</a> .
8	Geier, J. Minimizing WLAN Security Threats [Web Page]. 2002 Sep 5; Accessed 2004 Apr 10. Available at: <a href="http://www.wi-fiplanet.com/tutorials/article.php/1457211">http://www.wi-fiplanet.com/tutorials/article.php/1457211</a> .
9	Stehman, J. What's really new in WLAN Security? [Web Page]. 2003 Jun 30; Accessed 2004 Apr 10. Available at: <a href="http://www.csoonline.com/analyst/report1502.html">http://www.csoonline.com/analyst/report1502.html</a> .
10	Karygiannis, T and Owens, L. Wireless Network Security 802.11, BlueTooth and Handheld devices. NIST; 2002 Nov.
11	Rittinghouse, J and Ransome, J. Wireless Operational Security. first ed. Burlington, MA: Elsevier Digital Press; 2004 Feb 23.
12	Cam-Winget, N; Housley, R; Wagner, D, and Walker J . Security Flaws in 802.11 Data Link Protocols. ACM; 2003 May; 46, (5): 35-39.
13	Housley, R and Arbaugh, W. Security Problems in 802.11-Based Networks. ACM; 2003 May; 46, (5): 31-34.
14	Arbaugh, W; Shankar, N; Wan, J, and Zhang, K. Your 802.11 Wireless Network has no clothes. IEEE Wireless Communications. 2002 Dec; 44-51.
15	Molta, D. WLAN Security on the Rise [Web Page]. 2004 Feb 4; Accessed 2004 Apr 12. Available at: <a href="http://www.nwc.com/1303/1303ws2.html">http://www.nwc.com/1303/1303ws2.html</a> .

**16**

AusCERT. AA-2004.02 -- Denial of Service Vulnerability in IEEE 802.11 Wireless Devices [Web Page]. 2004 May 13; Accessed 2004 May 16. Available at: <http://www.auscert.org.au/render.html?it=4091>.

## Appendix D

### Raw Data – Vulnerabilities

Vulnerability	Occurrences
Wired Equivalent Privacy (WEP) protocol	15
Service Set Identifier (SSID) used as authentication	9
Simple Network Management Protocol (SNMP)	3
Shared Key Authentication	3
Media Access Control Access Control List (MAC ACL) can be spoofed	8
Exposed Access Points	5
One Way authentication (Rogue AP problem)	6
Traffic Redirection	1
Masquerading AP	1
Client Platform Security Vulnerabilities	1
Overlapping spectral footprint between 802.11 systems (RF Interference)	3
RF Interference (non 802.11 systems, such as Microwaves, Cordless Phones, Jammers)	5
Problems in 802.11b Ethernet protocol	4
Dynamic Host Configuration Protocol (DHCP)	3

## Appendix E

### Raw Data - Threats

Threat	Occurrences
War Driving	7
Network access via wireless router	1
AP Takeover	2
AP Cloning (Masquerading)	4
RF Jamming (interference)	3
WEP Protocol Attacks	3
Eavesdropping	4
Traffic Sniffing	5
Man-in-the Middle attack	7
Rogue AP	8
MAC Address switching	4
Trojans, Malware	2
Device Theft to obtain MAC	1
Session Hi-Jacking	2

## Appendix F

### Raw Data - Controls

Control	Occurrences
Smart Cards	1
Public Key Infrastructure (PKI)	1
Biometrics	1
Limit Range of WLAN coverage	3
Do not broadcast SSID	5
Do not use default SSID	4
Directional antenna pattern	3
Wireless security policy	2
Device authentication	1
802.1x authentication at AP w/Extensible Authentication Protocol (EAP)	11
MAC ACL	5
Wireless Intrusion Detection System (IDS)	4
Harden the access point	1
Use Encryption	1
Use WEP	2
Change WEP key frequently	1
VLAN	1
Virtual Private Network (VPN)	10
Wi-Fi Protected Access (WPA)	5
802.11i Security standard	9
Temporal Key Integrity Protocol (TKIP)	9
Message Integrity Check (MIC)	5
Advanced Encryption Standard (AES)	8
Firewall to isolate WLAN	1
Personal Firewall on Clients	2
Cisco LEAP	1
Properly configure SNMP	1
Robust Security Network (RSN)	3
Turn off Dynamic Host Control Protocol (DHCP)	3

## Bibliography

- Arbaugh, W., Shankar, N., Wan, J., & Zhang, K. (2002). Your 802.11 Wireless Network has no clothes. *IEEE Wireless Communications*, 44-51.
- Baker, D. (2003). *Wireless In(Security) for Health Care*. San Diego, CA: Science Applications International Corporation.
- Bell, C. (2003) Critical Evaluation of Information Sources Or, But Is It Credible? [Web Page]. URL <http://libweb.uoregon.edu/guides/findarticles/credibility.html> [2004, April 12].
- Cam-Winget, N; Housley, R; Wagner, D, and Walker J . Security Flaws in 802.11 Data Link Protocols. *ACM*; 2003 May; 46, (5): 35-39.
- Carney, W., & Soloman, Y. (2002) The Future of Wireless LANs will be Multimode [Web Page]. URL [http://focus.ti.com/pdfs/vf/bband/80211\\_wp\\_multimode.pdf](http://focus.ti.com/pdfs/vf/bband/80211_wp_multimode.pdf) [2004, April 3].
- CMS 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule. Department of Health and Human Services.
- CMS. (2003b) Covered entity chart [Web Page]. URL <http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/CoveredEntityFlowcharts.pdf> [2004b, March 31].
- Cox, J. (2001) Serious Security Weaknesses in 802.11b Wireless LANs exposed [Web Page]. URL <http://www.nwfusion.com/news/2001/0806ieee.html> [2004, April 3].
- Cox, J. (2003) WLAN Security: Users Face Complex Challenges [Web Page]. [2004, April 12].
- Creswell, J. (2003). *Research Design Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks, CA : Sage Publications.
- Eaton, D. (Intersil). (2002) Diving into the 802.11ispec: A Tutorial [Web Page]. URL [http://www.commsdesign.com/design\\_corner/OEG20021126S0003](http://www.commsdesign.com/design_corner/OEG20021126S0003) [2004, April 3].
- Emigh, J. (2003) Wireless Gone Wild: Time to Plan your WLAN [Web Page]. URL <http://networking.earthweb.com/netsysm/article.php/3070611> [2004, April 13].
- Gainer, R., Van Eckhardt, M., Williams, R., & Marks, R. (2003). No Rest for the Wary Vol. 8(20)*National Bureau of Affairs*.

- Geier, J. (2003) Denial of Service a Big WLAN Issue [Web Page]. URL <http://www.wi-fiplanet.com/tutorials/article.php/2200071> [2004, April 12].
- Goldberg, S., & Wickramasinghe, N. 36th Hawaii International Conference on System Sciences IEEE .
- Government of Canada. (2003). 802.11 Wireless LAN Vulnerability Assessment. Ottawa, Ontario, Canada: Government of Canada.
- Grove, T. (2003) Summary Analysis: The Final HIPAA Security Rule [Web Page]. URL <http://www.hipaadvisory.com/regs/finalsecurity/summaryanalysis.htm> [2004, April 14].
- Harris, R. (1997) Evaluating Internet Research Sources [Web Page]. URL <http://www.virtualsalt.com/evalu8it.htm> [2004, April 12].
- Housley, R and Arbaugh, W. Security Problems in 802.11-Based Networks. ACM; 2003 May; 46, (5): 31-34.
- Howard, J. (1997). An Analysis Of Security Incidents on the Internet 1989 - 1995. Unpublished doctoral dissertation, Carnegie Mellon, Pittsburgh, PA.
- IEEE. (2004) About the IEEE [Web Page]. URL [http://www.ieee.org/portal/index.jsp?pageID=corp\\_level1&path=about&file=index.xml&xsl=generic.xsl](http://www.ieee.org/portal/index.jsp?pageID=corp_level1&path=about&file=index.xml&xsl=generic.xsl) [2004, April 4].
- ISO/IEC. (2000). International Standard 17799: Information technology — Code of practice for information security management. Switzerland: ISO.
- Karygiannis, T., & Owens, L. (2002). Wireless Network Security 802.11, BlueTooth and Handheld devices. NIST.
- Kosiur, D. (1998). Building and Managing Virtual Private networks. (First ed., p. 19). New York: John Wiley and Sons, Inc.
- Krippendorf, K. (2004). Content Analysis: An Introduction to Its Methodology (2nd ed.). Thousand Oaks, CA: Sage Publications.
- Leedy, P., & Ormrod, J. (2001). Practical Research (7th ed.). Upper Saddle River, New Jersey: Merrill Prentice Hall.
- Messmer, E., & Cox, J. (2002) Making wireless LAN security air tight [Web Page]. URL <http://www.nwfusion.com/news/2002/1202earlywlan.html> [2004, April 6].
- Molta, D. (2004) WLAN Security on the Rise [Web Page]. URL <http://www.nwc.com/1303/1303ws2.html> [2004, April 12].
- National Communication System Technology and Standards Division. (1996). Federal

- Standard 1037C - Telecommunications: Glossary of Telecommunications Terms. Washington, DC: General Services Administration: IT Service.
- O'Hara, B. (2004) Comparing Costs of Wireless LAN Options [Web Page]. URL <http://www.computerworld.com/mobiletopics/mobile/story/0,10801,89105,00.html> [2004, April 12].
- Owen, R. (2000) A History and Overview of HIPAA [Web Page]. URL <http://www.hipaadvisory.com/regs/hipaahistorybyzon.htm> [2004, April 10].
- Ozier, W. (2000). Risk Analysis and Assessment. H. Tipton, & M. Krause Information Security Management Handbook (4th ed., ). CRC Press LLC.
- Palmquist, M. (2001) Content Analysis [Web Page]. URL <http://writing.colostate.edu/references/research/content/index.cfm> [2004, April 14].
- Phan, S. (2001) 802.11b Update: Stepping Up Your WLAN Security [Web Page]. URL <http://www.networkmagazineindia.com/200112/focus3.htm> [2004, April 12].
- Phifer, L. (2002) Better than WEP [Web Page]. URL [http://www.isp-planet.com/fixed\\_wireless/technology/2002/better\\_than\\_wep.html](http://www.isp-planet.com/fixed_wireless/technology/2002/better_than_wep.html) [2004, April 14].
- Sacia, K., & Dobson, R. (2003). Understanding Health Plan Administrative Costs.
- Searchsecurity.com. (2002) Wired Equivalent Privacy [Web Page]. URL [http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci549087,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci549087,00.html) [2004, April 14].
- Shiple, P. (2003) Peter Shipley [Web Page]. URL <http://www.dis.org/shiple/> [2004, April 4].
- Snyder, J. (2002) What is 802.1x [Web Page]. URL <http://www.nwfusion.com/research/2002/0506whatisit.html> [2004, April 14].
- Stallings, W. (2001). Business Data Communications. (4th ed., p. 92). New Jersey: Prentice-Hall.
- Stehman, J. (2003) What's Really New in WLAN Security? [Web Page]. URL <http://www.csoonline.com/analyst/report1502.html> [2004, April 12].
- Swartz, A. (2004) Warchalking [Web Page]. URL <http://www.warchalking.org/> [2004, April 3].
- US Department of Health and Human Services. (2001) Protecting the Privacy of Patient's Health Information [Web Page]. URL <http://aspe.hhs.gov/admsimp/final/pvcfact2.htm> [2004, April 1].

Webopedia. (WPA [Web Page]. URL <http://www.webopedia.com/TERM/W/WPA.html> [2002, April 14].

wi-fiplanet. (2002) hotspot [Web Page]. URL <http://wi-fiplanet.webopedia.com/TERM/H/hotspot.html>.

Zahur, Y., & Yang, T. (2004). Wireless LAN Security and Laboratory designs. 19(3), 44-60.