Investigation into the Security Practices of Irish Hospitals for Wireless Networks

Sinéad Walsh

A dissertation submitted to the University of Dublin, in partial fulfilment of the requirements for the degree of Master of Science in Health Informatics

2006

Declaration

I declare that this the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university

Signed: _____

Sinéad Walsh

28th September 2006

Permission to lend and / or copy

I agree that the Trinity College Library may lend or copy this dissertation upon request.

Signed: _____

Sinead Walsh

28th September 2006

Acknowledgments

I am deeply indebted to my supervisor Declan O'Sullivan whose help, suggestions and encouragement helped me complete this work.

Mr. Sherif Sultan, who allowed me the opportunity to pursue this work.

Professor Kevin Conlon, who provided me valuable opinions for the research.

My colleagues in the ICT department in AMNCH, a very big thanks!

To Mum, Dad, Colm, Fiona and Orfhlaith who have kept me going through it all.

Table of Contents

List of Figures

List of Tables

Summary

Healthcare is a natural environment for wireless LAN solutions. With a large mobile population of doctors, nurses, physician's assistants and other caregivers, wireless LANs bring the ability to access the latest patient charts, medical records and clinical decision support data at all times, anywhere in the healthcare organisation. As caregivers travel among different facilities, wireless allows for easy connectivity at each site. Early adopters in healthcare recognised these benefits and deployed the first wireless LAN solutions in the late 1990s.

However, with wireless LANs comes a new security risk. Unlike wired networks where physical access is required, wireless LANs transmit signals into the air space, and can extend beyond the physical perimeter of rooms and buildings. The standards which wireless LANs are based on, IEEE 802.11, does not mandate over-the-air security and authentication of users. Unless specifically configured for security, most wireless LAN equipment is an 'open' network, or able to be attached to by any wireless LAN client. This could lead to serious security risks if unauthorised personnel were to gain access to the healthcare network.

This study investigates the current situation relating to wireless security in Irish hospitals and was undertaken to see if Users and Management were in agreement about what the best way forward is.

The IT management completed an audit which documented the technical framework of their particular site. This audit also sought to identify the level to which user's needs were considered.

From this a questionnaire was designed and distributed to clinical users of mobile devices on wireless networks to gain an understanding of the level of awareness that is prevalent among clinicians in relation to wireless security.

The findings of this study revealed that wireless security in Irish hospitals is in quite good shape, but the users are not as informed as they could be. As, a result it is felt that a well implemented wireless security policy is now essential to the integrity and confidence of the Hospital.

Chapter 1 – Introduction

This chapter introduces the concept of wireless technologies in the Healthcare domain. Whilst medication errors is being used to illustrate the strong argument of the benefits of using Wireless Local Area Networks (WLAN), many other arguments exist, however this is not the main focus of this dissertation. The chapter then discusses the rationale and objectives used, and then details the research process for this dissertation.

1.1 The case for mobile devices and wireless networks

According to the Institute of Medicine in a study undertaken in 2000 by the National Academy of sciences, in the US, medication error kills as many as 44,000 and by some estimate 98,000 Americans per year with the costs of drug-related morbidity and mortality at nearly $77 billion per year [1].

The Institute of Safe Medication Practices (2000), estimates that there are 17,000 pharmaceutical brands currently sold in the U.S. and pharmacists make 150 million calls to physicians regarding non-formulary medications, potential drug interactions, incorrect dosages, and illegible handwriting. Several studies have demonstrated that the lack of access to information during decision-making and ineffective communication among patient care team members are proximal causes of medical errors and other adverse events in-patient care [2, 3, 4]

As mobile professionals, healthcare providers are often required to make immediate, life-critical decisions away from a stationery information resource. Providers need

only adopt wireless and Internet technologies, and handheld computers to make important, current patient information immediately available as they dispense care, decreasing substantially the number of medical errors [5]. The clinicians who partook in this research have shown a keen interest in embracing wireless technologies as a progressive benefit to their daily routine. These clinicians who took part in this study use mobile devices as a method of capturing information on diagnosis, surgical/medical procedures and clinical decisions.

Medical establishment studies show that some of the main causes of medication errors to be largely based on carelessness, neglect, and poor communications and information flow. While many of these issues can be addressed with non-technical solutions, it is felt that a system of tablet computers connected via a WLAN could provide tremendous benefits [9]. These benefits come in the form of improved information flow, up to date information, and a series of checks and balances. The mobility, economics, and security of the wireless system make it a better solution than placing workstations in every hospital room [6].

A range of technological solutions are considered and used to overcome the prevailing problems of loss of patient information and to improve medical practices and the overall outcome of service quality. Despite the financial constraint faced by the healthcare industry, in the US, millions of dollars are invested to acquire relevant solutions that meet the desired requirement. The US based 'Healthcare Information and Management Systems Society (HIMSS)' 2004 survey has shown that the driving forces for IT spending by the healthcare industry are reducing medical errors, improving patient safety, and developing electronic health records [7]. The HIMSS

report further identifies the key barriers to technology deployment as lack of financial support, the vendors' inability to deliver solutions, and lack of a quantifiable return on investment. Reluctance to embrace new technology and a requirement to comply with government regulations are other factors in the healthcare industry that are relevant to adopting wireless technology [1]. As expenditures in technology grow organizations increasingly look for empirical measures of benefits.

1.2 The need for wireless security in hospitals

By far the principal concern related to the deployment of WLANs in hospitals is the need for protecting patient information. There is no definitive security model for wireless security in the Irish context, although some Irish hospitals and healthcare organisations have implemented their own internal policies on security. For statutory guidance we must look to the United States who have 'The Health Insurance Portability and Accountability Act', 1996 (HIPAA) [8]. This Act is often used as a guide to the possible standards that could be implemented in countries who, like Ireland, do not have national healthcare information security policies. HIPAA requires that all electronic patient records meet stringent security measures. In order to comply with HIPAA, US hospitals must apply other security mechanisms in addition to Wired Equivalent Privacy (WEP) which is a security protocol for wireless local area networks. For example, the use of Wi-Fi Protected Access (WPA) is encouraged because of effective encryption/authentication and cross vendor support. In addition to the technical safeguards, HIPAA have also documented the need for policies and procedures for networks. The requirement for acceptable use policies encompasses both the wired and wireless networks. The purpose is to implement reasonable and

appropriate policies and procedures to comply with the standards, implementation specifications and other requirements of the HIPAA Security Rule [10].

1.3 Rationale

Through the authors personal experience of working with users of mobile devices it appeared that users were not very aware of the issues surrounding wireless security. Many seemed unconcerned and unaware of the security risks associated with the use of mobile devices. From this observation it was decided to investigate the users' actual awareness of wireless security issues.

The focus of this research centres around 2 major teaching hospitals in Ireland. The identities of both sites have been kept anonymous in order to get a true reflection of the wireless security practices being observed at these locations. Site A is based in the west of Ireland and Site B is located in the East. For the purpose of this research, the general surgical departments have been identified as the key users of mobile devices in daily practice, and as such provide the ideal focus group to ascertain attitudes towards wireless security. In addition to investigating the physical wireless security mechanisms, it was felt that the existence of other measures that make-up a good wireless security framework should be explored, such as the provision of policies pertaining specifically to wireless security.

1.4 Objectives

The objective of this research was to examine the wireless security practices in Irish hospitals and gather data on the awareness of security issues associated with wireless technologies.

1.5 Methodology

The aim was to conduct research in the form of an audit for IT management and from there develop a questionnaire for users. The audit was conducted initially to get an idea of the current practices of wireless security in a typical IT department in an Irish hospital. Also, it was hoped to identify the potential areas of concern for users in the implementation of WLANs within the hospital. From the responses gathered here the next step was to present a questionnaire to users of mobile devices on wireless networks, to examine their knowledge of the security risks associated with mobile devices.

The questionnaire was then distributed to clinical users of wireless networks at 2 teaching hospitals in Ireland. The identity of the research sites was protected, so as to encourage participants to document their opinions and concerns honestly. The sites have been identified as Site A and Site B. Both sites have completed the audit and the questionnaire.

1.6 Overview of the Chapters

Chapter Two provides a detailed overview of wireless local area networks and the wireless 802.11 standard.

Chapter Three introduces the topic of wireless security and the available standards for wireless security in healthcare. In addition the user's attitudes towards wireless security are examined.

Chapter Four presents the design of the audit and questionnaire and displays the results arising form them.

Chapter Five analyses the findings from the audit and questionnaire and compares them with findings from the current literature in the area. The reader is presented with an impression of wireless security practices currently observed in Irish hospitals.

Chapter Six presents the conclusion and recommendations of this dissertation.

Chapter 2 - Wireless Local Area Networks

This chapter provides a detailed overview of 802.11 Wireless Local Area Network (WLAN) technologies. It includes an introduction to 802.11 and details some of the more important wireless technologies. Also, the threats to wireless networks are examined to highlight the issues of concern for IT management.

2.1 Wireless LAN Overview

In the 1990s, wireless LAN technology [11, 12] emerged as a feasible alternative to wired LANs. With high-speed and reliable data communication, it has become a good solution to provide mobility in addition to traditional wired network functions.

Currently, most wireless networks are based on the IEEE 802.11b, 802.11a or 802.11g standards. These standards define how to wirelessly connect computers or devices to a network. Wireless enabled devices send and receive data indoors and out, anywhere within the range of a wireless access point.

The choice of standard depends on your requirements, including data communications speed and range, the level of security, noise and interference concerns, compatibility issues and cost.

2.2 Wireless LAN Technologies

2.2.1 802.11b

Probably the most widely implemented and used wireless LAN technology today, IEEE 802.11b specifies 5.5-Mbps and 11-Mbps data rates (in addition to the already specified 1 and 2 Mbps), but operates in the original 2.4-GHz band also using DSSS modulation [13].

It operates in the 2.4GHz spectrum and can transmit data at speeds up to 11-Mbps within a 100-foot range. Their balances of economy, bandwidth, and particularly range have made it the dominant standard for business.802.11b was the first 802.11 standard to be released and have commercial products available. Also called Wireless Fidelity, or Wi-Fi, it has a range suitable for use in big spaces such as hospital wards. Wi-Fi is currently the most popular and least expensive wireless LAN specification.

2.2.2 802.11g

The IEEE's 802.11g standard is designed as a higher-bandwidth - 54M bit/sec - successor to the popular 802.11b, or Wi-Fi standard, which tops out at 11M bit/sec. An 802.11g access point will support 802.11b and 802.11g clients. This makes 802.11g the obvious choice not only for anyone building a new network, but also for those interested in adding onto or gradually upgrading a pre-existing 802.11 network.

2.3 IEEE 802.11 Architecture

2.3.1 Architecture Components

An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells. Each cell (called Basic Service Set, or BSS) is controlled by a Base Station (called Access Point or, in short, AP) [14].

Although a wireless LAN may be formed by a single cell, with a single Access Point, (and as will be described later, it can also work without an Access Point), most installations will be formed by several cells, where the Access Points are connected through some kind of backbone (called Distribution System or DS). This backbone is typically Ethernet and, in some cases, is wireless itself.

The whole interconnected Wireless LAN, including the different cells, their respective Access Points and the Distribution System, is seen as a single 802 network to the upper layers of the OSI model and is known in the Standard as Extended Service Set (ESS) [16].

2.4 IEEE 802.11 Layers

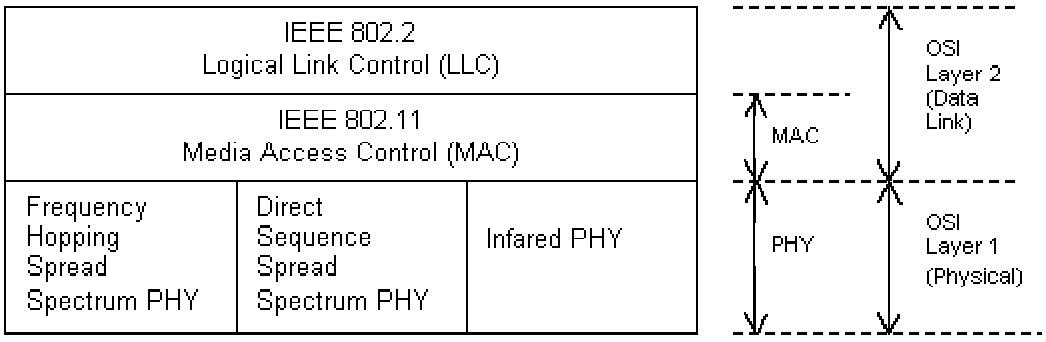

Figure 1 - IEEE 802.11 standards mapped to the OSI reference model

The IEEE 802.11 standard defines the parameters for both the physical (PHY) and medium access control (MAC) layers of the network (as any 802.x protocol) as shown in Figure 1 [17]. The standard currently defines a single MAC protocol, which interacts with three PHYs (all of them running at 1 and 2 Mbit/s) as follows:

- Frequency Hopping Spread Spectrum (FHSS) in the 2.4 GHz Band
- Direct Sequence Spread Spectrum (DSSS) in the 2.4 GHz Band, and
- Infrared (IR)

2.4.1 802.11 Physical Layer (PHY)

The physical layer (PHY), which handles the transmission of data between nodes, can use either direct sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), or infrared pulse position modulation. The 802.11 physical layer (PHY) is the interface between the MAC and the wireless media where frames are transmitted and received.

The PHY provides three functions.

1. The PHY provides an interface to exchange frames with the upper MAC layer for transmission and reception of data.
2. The PHY uses signal carrier and spread spectrum modulation to transmit data frames over the media.
3. The PHY provides a carrier sense indication back to the MAC to verify activity on the media.

2.4.2 802.11 Medium Access Control (MAC)

The 802.11 MAC layer provides functionality to allow reliable data delivery for the upper layers over the wireless PHY media. The data delivery itself is based on an asynchronous, best-effort, connectionless delivery of MAC layer data. There is no guarantee that the frames will be delivered successfully.

The 802.11 MAC provides a controlled access method to the shared wireless media called *Carrier-Sense Multiple Access with Collision Avoidance* (CSMA/CA). CSMA/CA is similar to the collision detection access method deployed by 802.3 Ethernet LANs.

Another function of the 802.11 MAC is to protect the data being delivered by providing security and privacy services. Security is provided by the authentication services and by *Wireless Equivalent Privacy* (WEP), which is an encryption service for data delivered on the Wireless LAN.

2.5 MAC Layer Functions

The following summarises primary 802.11 MAC functions, especially as they relate to infrastructure wireless LANs [5]:

- **Scanning**: The 802.11 standard defines both passive and active scanning; whereby, a radio NIC searches for access points. Passive scanning is mandatory where each NIC scans individual channels to find the best access point signal. The radio NIC can use information gathered along with the signal strength to compare access points and decide upon which one to use.

- **Authentication**: Authentication is the process of proving identity, and the 802.11 standard specifies two forms: Open system authentication and shared key authentication. Open system authentication is mandatory, and it's a two step process. A radio NIC first initiates the process by sending an authentication request frame to the access point. The access point replies with an authentication response frame containing approval or disapproval of authentication indicated in the Status Code field in the frame body.

- **Association**: Once authenticated, the radio NIC must associate with the access point before sending data frames. Association is necessary to synchronize the radio NIC and access point with important information, such as supported data rates. The radio NIC initiates the association by sending an association request frame containing elements such as SSID and supported data rates. The access point responds by sending an association response frame containing an association ID along with other information regarding the access point. Once the radio NIC and access point complete the association process, they can send data frames to each other.

- **WEP**: With the optional WEP enabled, the wireless NIC will encrypt the body (not header) of each frame before transmission using a common key, and the receiving station will decrypt the frame upon receipt using the common key. The 802.11 standard specifies a 40-bit key and no key distribution method, which makes 802.11 wireless LANs vulnerable to eavesdroppers. The 802.11i committee, however, is improving 802.11 security by incorporating **802.1X** and stronger encryption into the standard.

2.6 Threats associated with wireless networks

Wireless LANs have created a new level of productivity and freedom both within and outside the organisation [16]. By design, wireless signals propagate beyond the physical boundaries of the organisation, invalidating the traditional view that the inside of the organisation is secure. Signals from unsecured Wireless LANs that extend outside the corporate network can be found and used by unauthorized personnel-or even malicious hackers. Table 1, as defined by Microsoft [18] describes the most common threats to wireless LANs.

Table 1 - Main Security Threats for Wireless LANs

Threat	Threat Description
Eavesdropping (disclosure of data)	Eavesdropping on network transmissions can result in disclosure of confidential data, disclosure of unprotected user credentials, and the potential for identity theft. It also allows sophisticated intruders to collect information about your IT environment, which can be used to mount an attack on other systems or data that might not otherwise be vulnerable.
Interception and modification of transmitted data.	If an attacker can gain access to the network, he or she can insert a rogue computer to intercept and modify network data communicated between two legitimate parties.
Spoofing	Ready access to an internal network allows an intruder to forge apparently legitimate data in ways that would not

Threat	Threat Description
	be possible from outside the network, for example, a spoofed e–mail message. People, including system administrators, tend to trust items that originate internally far more than something that originates outside the corporate network.
Denial of service (DoS)	A determined assailant may trigger a DoS attack in a variety of ways. For example, radio–level signal disruption can be triggered using something as low–tech as a microwave oven. There are more sophisticated attacks that target the low–level wireless protocols themselves, and less sophisticated attacks that target networks by simply flooding the WLAN with random traffic.
Free–loading (or resource theft)	An intruder may want nothing more sinister than to use your network as free point of access to the Internet. Though not as damaging as some of the other threats, this will, at the very least, not only lower the available level of service for your legitimate users but may also introduce viruses and other threats.
Accidental threats	Some features of WLANs make unintentional threats more real. For example, a legitimate visitor may start up a portable computer with no intention of connecting to your

Threat	Threat Description
	network but then is automatically connected to your WLAN. The visitor's portable computer is now a potential entry point for viruses onto your network. This kind of threat is only a problem in unsecured WLANs.
Rogue Wireless LANs	If your company officially has no Wireless LAN you may still be at threat from unmanaged Wireless LANs springing up on your network. Low priced WLAN hardware bought by enthusiastic employees can open unintended vulnerabilities in your network.

Equipped with the knowledge of risks and threats posed to wireless networks, it is easier to address the security issues of wireless networks. The next chapter will discuss the various facets of wireless security.

Chapter 3 - Wireless Security

This chapter introduces the area of wireless security. A Wireless Local Area Network (WLAN) is the perfect way to improve data connectivity in an existing building without the expense of installing a structured cabling scheme to every desk. Besides the freedom that wireless computing affords users, ease of connection is a further benefit. Problems with the physical aspects of wired Local Area Network (LAN) connections (locating live data outlets, loose patch cords, broken connectors, etc.) generate a significant volume of helpdesk calls. With a wireless network, the incidence of these problems is reduced [19].

However, when choosing to deploy a wireless local area network the single most concern is for its security. Especially in a healthcare setting, where security of medical data is paramount.

The area of wireless security is introduced and explored in section 3.1. This section presents an overview of the current security methods for wireless security. The area of authentication will be discussed.

Section 3.2 provides us with an overall view of the Health Insurance Portability and Accountability Act, 1996 (HIPAA). We are given the background and the reasons behind its origin. The guidelines for wireless security as documented in the 'Final Rule' by HIPAA are then discussed.

Following this, section 3.3 examines the attitudes of users in relation to the adoption of wireless security measures.

3.1 Wireless Local Area Network Security

The 802.11 standard first appeared in the 1990's and was developed by the Institute of Electrical and Electronics Engineers. It has now emerged and expanded to be one of the leading technologies in the wireless world.

3.1.1 Security Overview

802.11 provides for security via two methods:

1. Authentication
2. Encryption.

Firstly *Authentication* is the means by which one station is verified to have authorization to communicate with a second station in a given coverage area. In the infrastructure mode, authentication is established between an AP and each station.

The two main types of authentication are properly known as:

1. **Open System:** The open system requires that the requesting station send its identification to the authenticating station, which either accepts or rejects the connection based on whether or not the identity is recognized.
2. **Shared Key:** The shared key system requires that a secret key is known by both the authenticating station and the requesting station. When a connection is attempted, the secret key is sent from the requesting station and is either accepted or rejected by the authentication station [20].

In an Open System, any Station (STA) may request authentication, as shown in Figure 1 [23]. The STA receiving the request may grant authentication to any request, or only those from stations on a user-defined list. In a Shared Key system, only stations which possess a secret encrypted key can be authenticated. Shared Key authentication is available only to systems having the optional encryption capability.

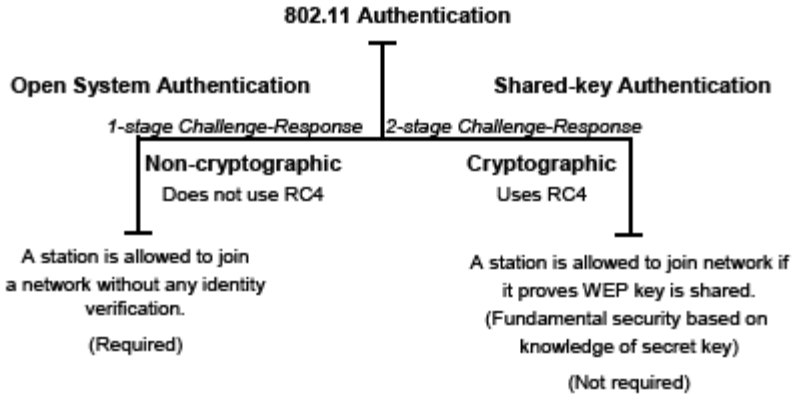

Figure 2 - 802.11 Authentication Technique

Secondly *Encryption* is intended to provide a level of security comparable to that of a wired LAN. The 802.11 standard includes a security technique known as "wired equivalent privacy" (WEP), which is based on the use of an authentication procedure and 64-bit keys with RC4 encryption algorithm. The use of spread-spectrum radio transmission techniques also increases the security in the 802.11 transmission medium [21].

The WEP algorithm was selected to meet the following criteria:

- Reasonably strong
- Self-synchronizing
- Computationally efficient
- Exportable
- Optional

Figure 2 below shows the wireless security of 802.11 in a typical network.

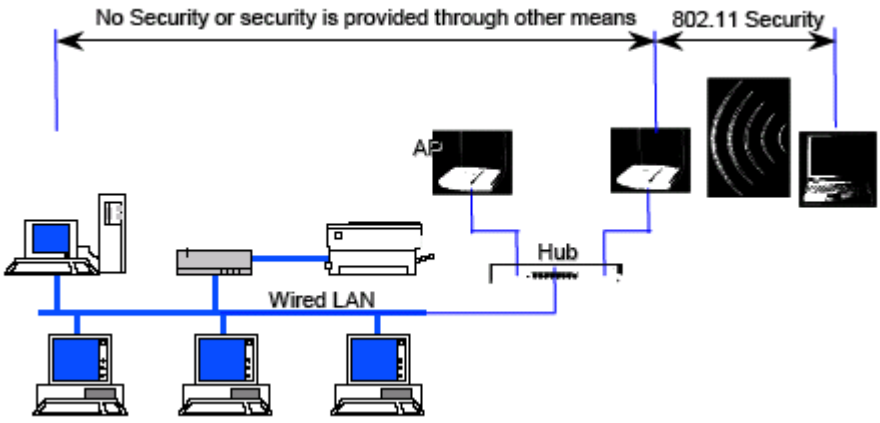

Figure 3 - Wireless Security of 802.11 in a typical network

3.1.2 Authentication

User authentication is a basic theme in both wired and wireless security and covers establishing who the user is (identification), verifying this identity (verification or authentication), and providing proper access to the resource that the user is allowed to use (authorization). User authentication became important when multi-user computers and operating systems were introduced [21].

Even though the traditional login by typing username and password has developed technically over the years it has not changed since the 60s seen from a usability point of view [22]. This tendency is also reflected in the research done around user authentication where most work has been done within the fields of computer communication and computer security, and very little has been done from a usability point of view. The impact on user's opinions of multiple passwords will be discussed later.

3.1.3 The Authentication Process

Preventing access to network resources is achieved through the use of an authentication mechanism where a station needs to prove knowledge of a shared secret. In IEEE 802.11 networks, this process takes place before that a wireless client is associated with an Access Point (AP).

By default, IEEE 802.11 devices operate in an Open System, where essentially any wireless client can associate with an AP without the checking of credentials. True authentication is done with the use of the 802.11 option known as Wired Equivalent Privacy (WEP), where a Shared Key is configured into the AP and its wireless clients. Only those devices with a valid Shared Key will be allowed to be associated to the AP.

This is very similar to Wired LAN privacy, in the sense that an intruder needs to enter the premises (by using a physical key) in order to connect their workstation to the wired LAN.

The authentication process is done once the mobile station has located an Access Point and decided to join its Basic Service Set (BSS). A BSS consists of two or more wireless nodes, or STAs, which have recognized each other and have established communications.

The authentication consists of an interchange of information between the AP and the station, where each side proves the knowledge of a given password.
Once the station is authenticated, it then starts the real association process, which is the exchange of information about the stations and BSS capabilities, and which allows the Extended Service Set (ESS), (the set of APs), to know about the current position of the station. This information is needed by the distributed system so it knows which AP to access when delivering messages to a given station.

Each station can only be associated with a single AP, but APs can be associated with multiple stations. A station is capable of transmitting and receiving data frames only after the association process is completed [24].

Every action tied to an authentication or authorization event can be logged and reported [25]. This is in keeping with the Health Insurance Portability and Accountability Act (HIPAA) guidelines for security of wireless networks. The next section gives an overview of HIPAA and describes the suggested measures for best practice relating to wireless networks.

3.2 The Health Insurance Portability and Accountability Act, 1996 (HIPAA)

In the Irish or even European context there are no standards published relating to security of WLANs in hospitals or in healthcare generally. It has been identified, in the National Health Information Strategy [26], in Ireland that "The adoption of standards is an essential requirement for improving the quality and usefulness of information for all stakeholder groups, and is of crucial importance in the use of the electronic healthcare record". It is however, not stated how this should be achieved.

Although in Ireland we are not obliged to adhere to standards as yet, HIPAA appears to be a reasonable yard stick from which to base security standards on.

The following section introduces HIPAA and discusses the security implications of embracing such a standard.

3.2.1 Background to HIPAA

In 1996, the U.S. Congress signed into law the Health Insurance Portability and Accountability Act to initiate the process of healthcare reform. Economic and social factors were major influences in what eventually became the law known as HIPAA. Driven by a demand to improve quality while maintaining safety and cost effectiveness, multiple challenges to business, government, and healthcare industries were offered to improve and change a healthcare system largely perceived as arbitrary and idiosyncratic [27].

HIPAA emerged from broad-based and wide-ranging efforts to reform health care [28, 29, 30, 31]. The version eventually passed into law, known as the Final Rule, addresses information privacy, the availability and portability of health insurance, and the electronic transfer of information.

HIPAA reflects and represents a regulatory attempt to institute ‘‘good practice’’ in data security among American healthcare institutions. For healthcare organisations to institute good information security practices, they must cultivate leadership support for information security, conduct a comprehensive information security risk assessment and adopt technical and organisational controls that protect health information [32].

HIPPA allows us to have a glimpse at how we would all like our healthcare systems to work. The Act is very beneficial to the patient and the healthcare provider but for the IT specialist all it brings is headaches. Patients will be able to access their medical records no matter what hospital or health service provider they are visiting. Healthcare professionals will be able to transfer the medical information which will enable them to treat the patient. The system will also help the healthcare provider reduce their administration costs. However for the IT specialist, HIPAA is a huge task to implement.

Firstly, every patient, doctor, healthcare professional and hospital will require a unique ID which will identify them and allow them access to their own personal records. Secondly, medical information must be kept secure at all times during transmission and storage. Also you must allow the patient to access their own records

and ensure the integrity of the records. HIPAA is not easy to implement and it is quite expensive. It is difficult to implement the security side of the Act with the current transfer protocols that are in place, especially over long distances. Doctor/patient privacy is nothing new and we cannot allow the Internet to compromise this relationship.

The benefits for patients and users of the healthcare service will be immense. Even though there is a lot of negativity that surrounds the implementation of the Act the bottom line is that all medical systems are now being designed with the patient placed firmly at the centre of the design.

3.2.2 HIPAA and Wireless Security

Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of computers to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions.

The security rules as stipulated by HIPAA require covered entities such as pharmacies, hospitals, health care providers, clearing houses and health plans to conduct an assessment of potential risks and vulnerabilities and to implement - and revisit from time to time - security measures sufficient to reduce such risks and vulnerabilities [33].

Information that has been deemed "secure and/or private" is known as Protected Health Information (PHI) and includes almost all identifiable health records and data that can be transmitted or maintained in any format. Identifiable refers not only to data that is explicitly linked to a particular individual (that's identified information). It also includes health information with data items which reasonably could be expected to allow individual identification.

The core objective of the HIPAA Security Rule is for all covered entities to support the Confidentiality, Integrity and Availability (CIA) of all Electronic Protected Health Information (ePHI). Below graphically summarizes information about the Privacy Rule and Security Rule Safeguard requirements [34].

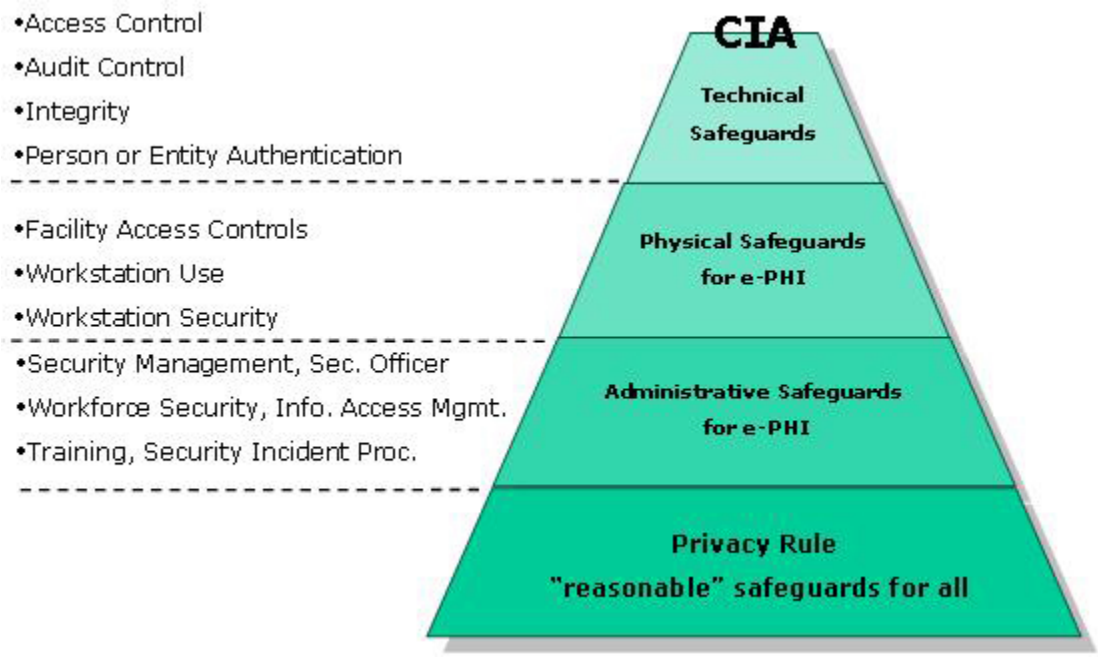

Figure 4 - Privacy Rule and Security Rule Safeguard Requirements

The key sections of HIPAA that focus on security over protected health information are as follows:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organisational Requirements
- Policies, Procedures and Documentation Requirements

3.2.3 Administrative Safeguards

This section documents the majority of the security standards and implementation specifications. The nine standards in this category outline the process infrastructure that needs to be in place for effective security of electronic PHI. The standards address security management, assigned security responsibility, workforce security, information access, security awareness and training, security incidents, contingency plans (for emergencies and disasters), evaluation of security effectiveness, and business associate contracts (or other arrangements) with hospital business partners [35].

3.2.4 Physical Safeguards

Regulations surrounding the protection of computers, equipment, and physical records from hazards and natural disasters are documented in this section of the security rule. Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion [34].

.

3.2.5 Technical Security Services

This section governs the protection, control, and management of information access and the enforcement of administrative policy and procedures. Technical security measures should include user authentication and restriction gateways to maintain security over protected health information. Minimum authentication and access policies require a user ID and password; a more sophisticated policy may include tokens, proximity sensing devices, or digital certificates, among others. IT managers must always consider how information will be accessed and develop a system that will not restrict caregivers from pertinent patient data during an emergency. IT managers should consider implementing audit trail reporting that records data access details and monitors information transmission [36].

3.2.6 Technical Security Mechanisms

These are measures that document procedures to protect patient data from unauthorized users over a public communications network, such as a WLAN or WAN, remote access, intranet, and extranet. It is recommended that IT managers deploy network controls and safeguards like virus protection, encryption, virtual private networks (VPNs), and Internet monitoring controls. Also, healthcare organisations should consider replacing dial-up access with a VPN to prevent unauthorized network entry and data retrieval.

3.2.7 Organisational Requirements

Developing policies, procedures and mechanisms for security management is only one part of a comprehensive programme for protecting health information. Another integral part is ensuring that there are appropriate mechanisms in place for protecting the confidentiality of such data [37].

Organisational requirements of HIPAA require that all covered entities implement and maintain written policies, procedures and documentation required to comply with the security rule.

As a result of these guidelines it is clear that IT managers have quite a large task to undertake. It is felt that while technically securing the network is of paramount

importance, the implications for users should be addressed. The next section addresses some of the attitudes of users in relation to wireless security.

3.3 User attitudes towards wireless security

Due to the nature of wireless communications and the risks therein, it is critical for an organisation to have a security policy explicitly dealing with wireless devices. The final HIPAA Security Rule §164.316 specifies that all covered entities must develop security policies to meet the new regulations [46]. It has been noted by the author that instances occur within a hospital where an employee has gained access to the hospital network via an unsecured "test" access point. However, because the organisation did not have a security policy covering wireless devices, the employee simply claimed, "I didn't know I shouldn't have my own access point." While there may have been no malicious intent on behalf of the employee, he violated the security posture of the hospital. However, the hospital had no recourse for the employee because there was no explicit policy [38].

"A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities", [39].

Unprotected wireless client devices such as notebooks and handheld devices can be exploited as peers or access points to break into corporate WLANs where they can remain undetected indefinitely. So far, there has been little evidence of attacks

targeting such devices. But with 85% of laptops and 60% of handhelds [40] expected to be wireless-enabled by the end of 2006, users should expect to see attacks crafted against those devices in the not-too-distant future. Yet, less than 10% of hospitals are likely to have formal wireless security policies.

The security problems inherent in WLANs are a side effect of the ease with which they can be set up and it's vital to develop a policy from the beginning. "Adding security afterwards means getting new equipment and redeploying the network." Although this may be a little alarmist in relation to both sites in this study, it is clear that before any further deployment occurs, an evaluation of the user practices may be of benefit when thinking of new security measures for the organisation [41]. Even with a plan, there are those in the wireless industry who maintain cautionary stances when it comes to wireless security. One industry executive recently observed that companies were using wireless technology at various levels of standard 802.11b-g. 802.11 uses WEP (wireless equivalency protocol), which has tried to address security shortcomings in the 802.11 standard, and newly evolving standards like WPA (Wi-Fi Protected Access) and WPA2 are even more promising and will probably replace WEP.

Nevertheless, there is still wariness when it comes to implementing wireless networks. Standards continue to evolve, and encryption and authorization algorithms can be implemented incorrectly in both software and hardware [42].

3.3.1 Awareness is the key

Users are often cited as the weakest link in any security chain but an effective training and awareness programme, can significantly reduce the sources, and levels, of risk associated with human behaviour [43]. The inherent insecure nature of the wireless network medium makes it essential that users adhere to effective security practices. These may include, but are not limited to, the use of application level authentication and encryption technologies such as Secure Socket Layer (SSL) and Secure Shell (SSH) [44].

It has become very apparent that in view of the users that no consideration has been given to a wireless security. During the analysis it appeared that a high standard of vigilance prevailed within the system and network security side. The IT personnel appeared not to have given great thought or consideration to the users practice. Although, the high specification security measures that were in place made it virtually impossible to penetrate the network.

In conclusion, it would appear to make organisational sense to define specific policies relating to wireless security. Some experts believe that HIPAA will result in a strategic transformation of the healthcare industry [45]. This would place Irish hospitals in a leading position in Europe for the control and security of health information.

The next chapter presents the IT management audit and the user questionnaire used to investigate the current situation relating to wireless security practices in Irish hospitals.

Chapter 4 - Wireless Security Audit and Questionnaire

This chapter describes the methodology used for this research and the reasons for choosing such.

Much of the background information and methods chosen for the questions were inspired by HIPAA standards. Sections 164.308 and 164.312 of the HIPAA Act provided a frame of reference for designing both the audit and questionnaire.

The results of the research will be revealed and presented in figures throughout.

4.1 Motivation

Through the authors personal observation it was evident that users were not very security savvy. Many users seemed unconcerned and unaware of the security risks associated with the use of mobile devices. From this observation it was decided to investigate exactly how aware of any security issues the users actually were.

Upon investigation it emerged that there were no documented policies or guidelines for users of mobile devices on wireless networks, and so, this provided an opportunity to investigate the practices of IT management and clinical users in the healthcare domain.

Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure it remains secure [47]. The aim of the audit was to provide an insight to the current practices relating to

wireless security in Irish hospitals. The audit design and results are described in section 4.3.

Cognisant of the results of the audit, a questionnaire was designed to see if users were aware of the security considerations that pertain to wireless networks and also if their needs concurred with the findings of the IT management audit. The questionnaire design and results are described in section 4.4.

4.2 Target Groups

The chosen sites were 2 major teaching hospitals in Ireland. The checklist audit was completed by the IT operations managers at both sites. Clinical doctors working in busy surgical departments completed the questionnaires, as they were the principal everyday users of wireless devices. The identities of both sites have been kept anonymous in order to get a true reflection of the security practices being observed at these locations. Site A is based in the West of Ireland and Site B is located in the East. For the purpose of this research, the general surgical departments have been identified as the key users of mobile devices in daily practice.

Site A is at the pilot stage of wireless deployment and has uninterrupted wireless coverage over 2 surgical recovery wards. Wireless access points have also been deployed at other locations, where patient information is gathered throughout the hospital. The locations are as follows:

- Theatre
- Diagnostic Laboratory

Site B has wireless coverage over 2 general surgical wards. The application that is in use at this site only demands information capture and retrieval at the patient bedside. Site B has implemented a session logout time of 10 minutes. This gives the clinicians more than adequate time to get to the neighbouring wards before the connection drops.

4.3 Audit

Initially, it was decided to conduct a survey or audit of IT management practice in order to identify the vulnerabilities in the wireless network. From the information gathered at this stage, the aim was to generate a questionnaire for users, to ascertain their attitudes towards any security issues in wireless networks.

4.3.1 Audit Design

The checklist audit method was chosen as it emerged that this was the most commonly used and effective method of gathering the type of information pertaining to the state of security in a wireless network.

The SANS (SysAdmin, Audit, Network, Security) Institute which purports to be the largest source for information security training and certification in the world has provided some of the guidelines for the audit. The SANS Institute, make reference to what they claim to be essential security considerations for design and deployment of an Enterprise WLAN [48].

An informative list has also been compiled by the US based, National Institute of Standards and Technology (NIST) as part of their documentation on Wireless Security [49]. The questions for the audit were based on the major areas of concern according to both institutes recommendations.

The "Wireless Networking Basic Security Checklist" as suggested by netstumbler [50], is also a useful tool which suggested many similar questions that were deemed essential to identifying security risks on a wireless network. This was also taken into consideration for the design of the audit.

The audit, as outlined in Table 1 was divided into 4 sections:

1. **Physical Security**

   This section poses questions that pertain to the physical security of the devices in the sites.

2. **Network security**

   This section endeavours to identify the vulnerabilities that may be apparent in the hospital wide network.

3. **Wireless security**

   This section questions the issues relating specifically to wireless security.

4. **User Security**

   In this section, it is hoped to highlight the outstanding security issues, if any, concerning users of the wireless network.

4.3.2 Audit Overview

The checklist audit was completed by the IT operations managers at both sites. A number of information gathering approaches were examined, such as interviews, questionnaires and audits. Initially the IT operations managers in both sites were approached and asked if they would be willing to participate in an interview for the purpose of identifying the status of wireless security at this site. Due to the time constraints of the IT management duties, it was suggested that perhaps a questionnaire or audit should be prepared so that they could complete it in their own time. On this recommendation it was decided to design an audit as it appeared to be the most feasible for the purpose of this research.

4.3.3 Audit Results

This section documents the results from the audit conducted in the IT Management departments. The sections highlighted are the only conflicting responses returned by both sites.

Wireless Network Security Audit for IT Management

	Site A		Site B	
Physical Security	**Yes**	**No**	**Yes**	**No**
1. Are the parallel/serial/infrared/USB/SCSI ports secured or removed?		√		√
2. Are the wireless devices physically locked down to the system?		√		√
3. Do you have an inventory of all access points?	√		√	
4. Are there any physical boundary safeguards in place?		√		√
	Site A		**Site B**	
Network Security	**Yes**	**No**	**Yes**	**No**
5. Do only authorised personnel have physical access to the wireless Network?	√		√	
6. Have you checked all the vendors for security patches, and do you regularly receive security updates about patches/vulnerabilities to the software you use in a wireless environment?	√		√	
7. Do you effectively limit your users` abilities to make sensitive information about the system available over the network?	√		√	
8. Do user accounts that are accessible over the network regularly have their passwords changed?	√			√
9. Do you encrypt sensitive data that is transferred	√		√	

over the network?				
10. Is there a session timeout applied to all applications?		√	√	
	Site A		**Site B**	
Wireless Security	**Yes**	**No**	**Yes**	**No**
11. Do you have some form of logging enabled?	√		√	
12. Do you log and audit guest user activity?		√		√
13. Have you performed a site survey to find out exactly where the signal starts and ends?		√	√	
14. Do you test your configuration of the software thoroughly; i.e. Try to break it, try to hack into it, and see if others can do the same?		√		√
15. Have you checked for the latest releases of any available patches?	√		√	
16. If a program accesses sensitive data, do you make sure that it can only be executed by authorized users?	√		√	
	Site A		**Site B**	
User security	**Yes**	**No**	**Yes**	**No**
17. Do you have a standard method for creating and maintaining user accounts?	√		√	
18. Do you have clear and concise acceptable use policies for your users?	√		√	

19. Do you have a policy specific to wireless users?		√		√
20. Are users made aware of the risks associated with wireless technology and security?		√		√
21. Do you set limits on the amount of resources a user can consume, from number of logins to amount of disk space?		√		√
22. Do you keep accurate logs of user activity? i.e., connection time, connection duration and the place where they logged in/connected from.	√		√	

Table 2 - Audit Results from both Sites

The responses from both sites were very similar; the notable differences however presented themselves in the area of network and wireless security. These areas have been highlighted in Table 1 and are presented below:

- Site A declared that users were forced to change their passwords on a regular basis whereas Site B users did not ever have to change their password for any application.

- Site A do not have a session time out applied to their wireless network, whereas site B have a 10 minute timeout.

- Site B have conducted a site survey identifying where the wireless signal starts and ends, and have taken the appropriate measures to manage this. Site A,

however has not, as yet conducted this survey, but have said that one is planned in the near future.

- While both sites have said that they have a general acceptable use policy, neither appears to have any reference to the issues associated with wireless security.

- Also, neither site has indicated that users have been made aware of any security associated with use of mobile devices on the wireless network.

The next chapter, on the analysis of the audit, will present a discussion of the results.

4.4 Questionnaire

The questionnaire was divided into 4 sections as follows:

1. ***Level of Knowledge*** - deals with ascertaining the users level of knowledge in relation to the concept of wireless technology.
2. ***Passwords*** - details the password behaviour of users.
3. ***Logon*** - ascertain that session log out practices adhered to by the participating sites and the attitudes of users to the conditions implemented by the IT departments.
4. ***Security Issues*** - section aims to identify the level of knowledge that users have in relation to any issues associated with wireless security.

4.4.1 Questionnaire Design

Based on the answers to the questions posed in the audit, a questionnaire was designed for the users of mobile devices on the wireless network at both locations.

Upon investigation into the most appropriate method, it was agreed that a questionnaire was the most effective technique in acquiring user's attitudes towards wireless security. Questionnaires offer an objective means of collecting information about people's knowledge, beliefs, attitudes, and behaviour [51] [52].

The irregular schedule of the target group of clinicians meant that an interview technique would be time consuming and very difficult complete due to interruptions such as being bleeped during the interview thus distracting the focus of the survey. As such, a paper questionnaire could be distributed and completed in the participants own time. In an attempt to achieve a satisfactory response rate, a meeting was held with the participating consultants in the hope that they would encourage their respective teams to participate.

This Questionnaire design reflected previous studies that have been carried out in the area of wireless security such as the 2004 IT toolbox Wireless Security Survey [53].

4.4.2 Questionnaire Overview

A questionnaire comprising of 19 questions was circulated to 30 participants in 2 sites. 15 questionnaires were distributed to clinical users in each site. The participants were guaranteed anonymity in order to try and get a true and accurate reflection of the current state of wireless security in Irish hospitals.

A total of 19 surveys were returned. This indicated that an overall response rate of 63% was achieved.

The response rate was broken down as follows:

	No. of Questionnaires returned	**Response Rate**
Site A	9	60%
Site B	10	66%

Table 3 - Response Rate from Both Sites

4.4.3 Questionnaire Results

4.4.3.1 Level of Knowledge

Section 1 deals with ascertaining the users level of knowledge in relation to the concept of wireless technology. In the context of the study importance was placed on gaining an understanding of how familiar the users were in relation to the exposure they have to their practice

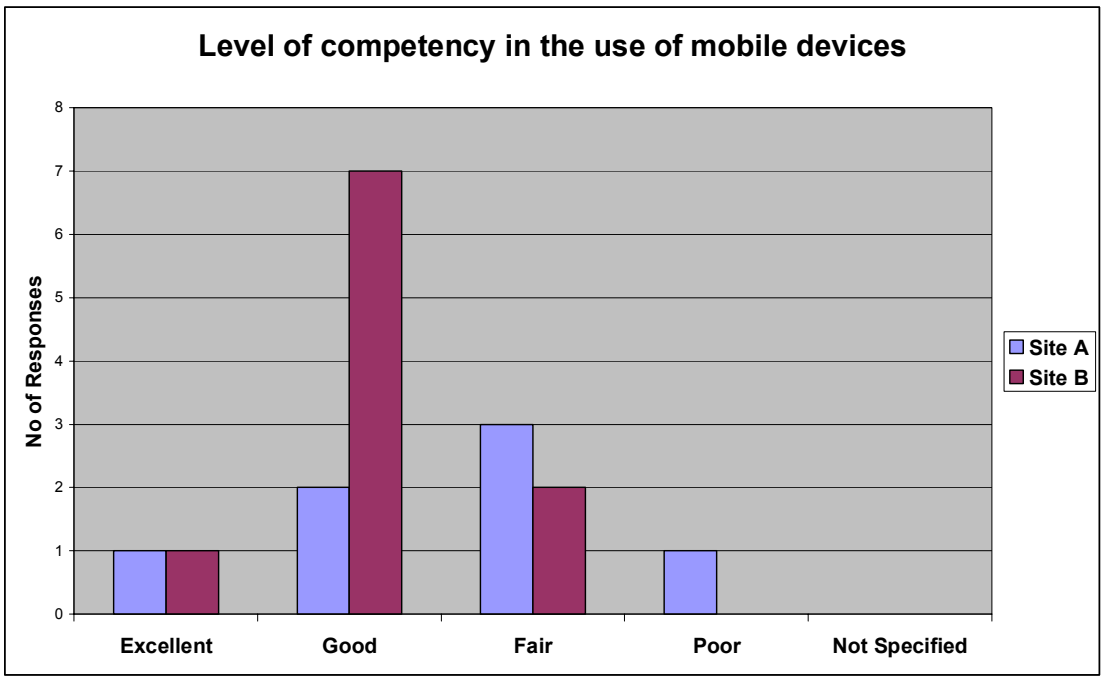

Figure 5 Level of competency in the use of mobile devices

The question was rated with 4 = Excellent, 3 = Good, 2 = Fair and 1 = Poor 0=Not specified

From this it is gathered in Figure 5 that 73% (n=9) users consider themselves to be quite competent (good) in the use of mobile devices.

Users were then asked about the frequency with which they enter patient data on mobile devices and the following in Figure 6 represents a graphical representation of the trend.

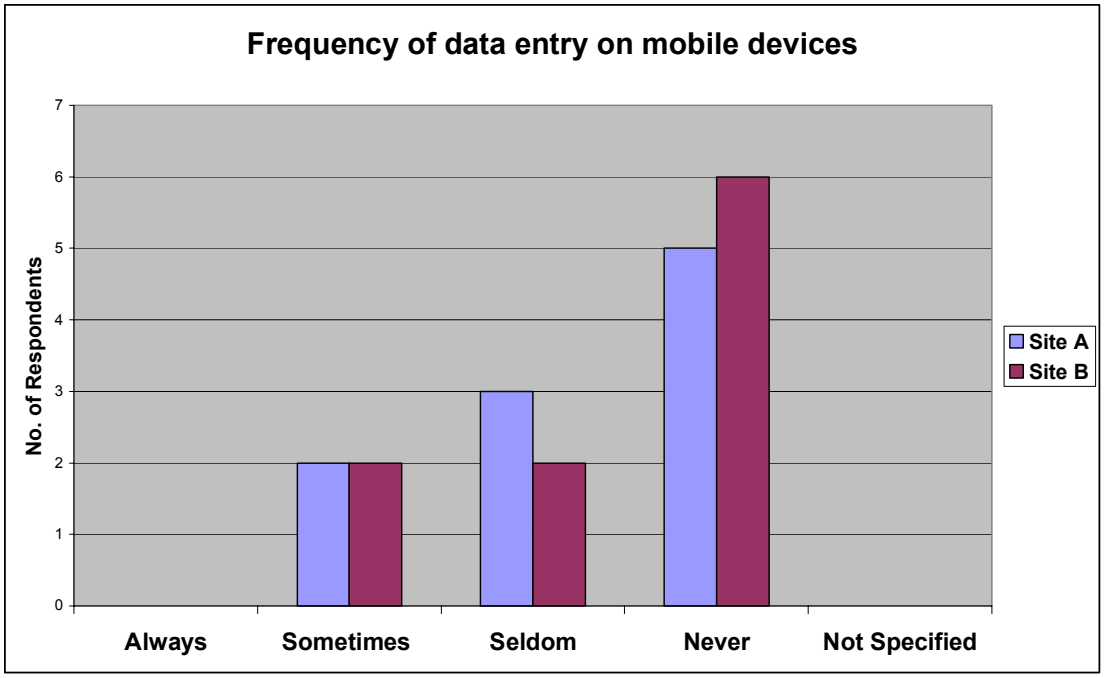

Figure 6 – Frequency of data entry on mobile devices

In relation to training users were asked if they felt that they had adequate training on the applications they used and whether they had received any training specific to wireless security. The following charts (Figure 7 – 8) display the attitudes towards the level of training received in the respective workplaces.

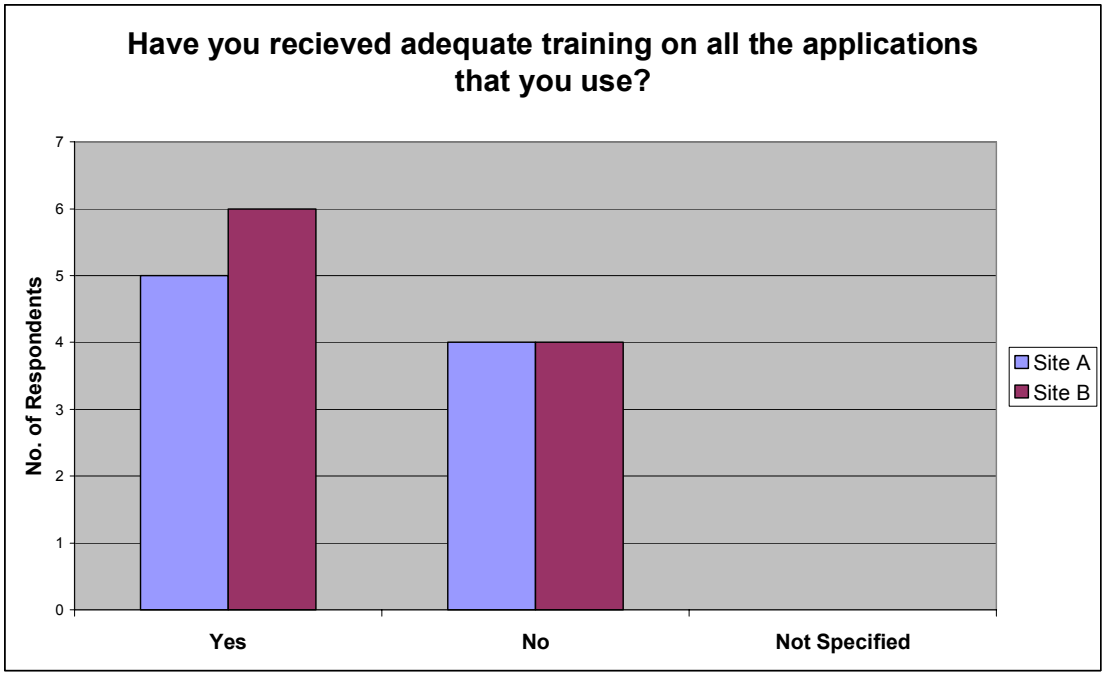

Figure 7– Have you received adequate training on all the applications you use?

According to users in Figure 7, 58% (n=11) felt they had received adequate training on all the applications they used. However 42% (n=8) in contrast felt they could benefit from more comprehensive training. This would indicate that the issues of adequate training would need to be addressed; suggestions will be presented in the next chapter.

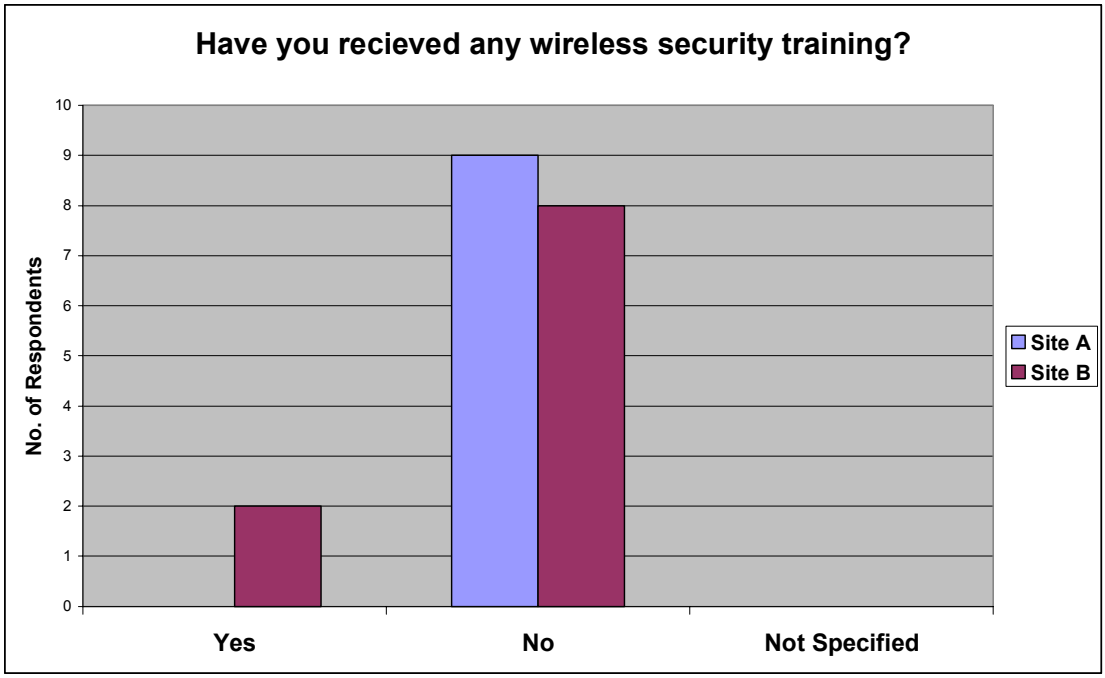

Figure 8– Have you received any wireless security training?

When asked if any users have received any training specific to wireless security and practices, an overwhelming 89% (n=17) in Figure 8 declared that no training or information relating to wireless security had been provided. This concurred with the findings in the IT Management audit whereby both sites indicated that no training had been provided and that no policy for wireless communication existed within the hospital sites.

4.4.3.2 Passwords

This section details the password behaviour of users. Rigby et al [54], make the point that it is difficult to ensure appropriate levels of confidentiality in electronic information systems to the point that the highly exacting requirements being demanded by professional bodies are difficult to satisfy without jeopardising the

functioning of core services. To this end, an investigation of the habits of users and their passwords is detailed in this section.

In Figure 9, 89% (n=17) of users declared that all applications on mobile devices in their work setting were password protected.

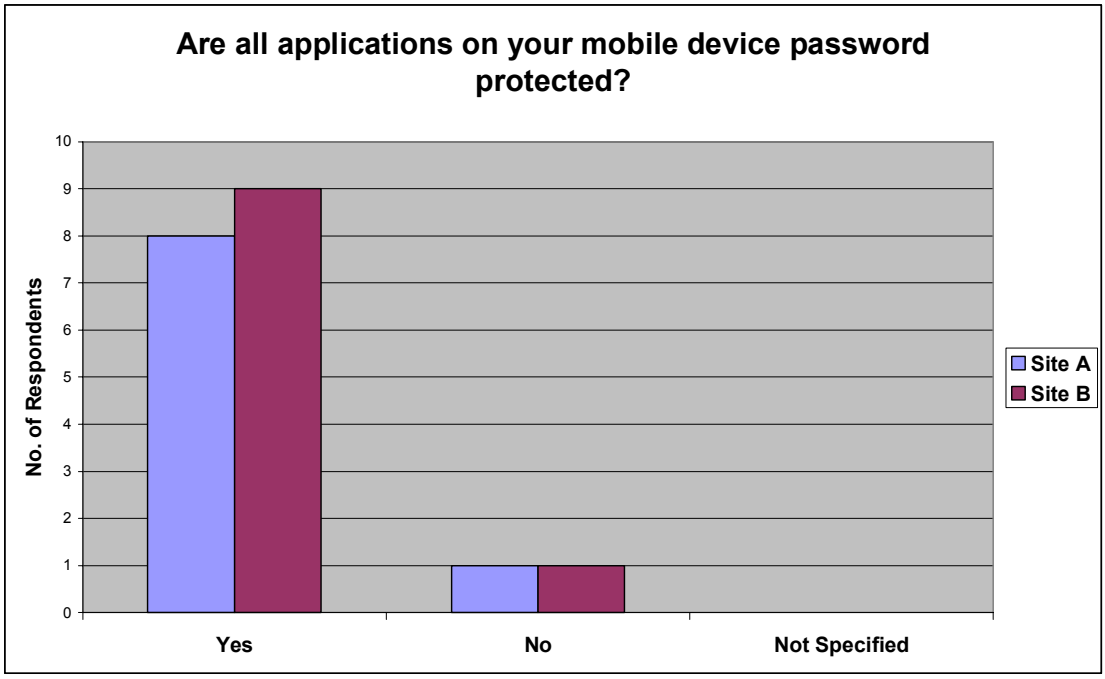

Figure 9– Are all applications on your mobile device password protected?

Users were then asked if they use the same password for all applications. Figure 10 demonstrates that 68% (n=13) of users have the same password for all applications. Also according to the results in Figure 11, 89% (n=9) in site B said that they that they never have to change their password whereas 100% (n=9) of Site A responded that they have to change their passwords on a regular basis.

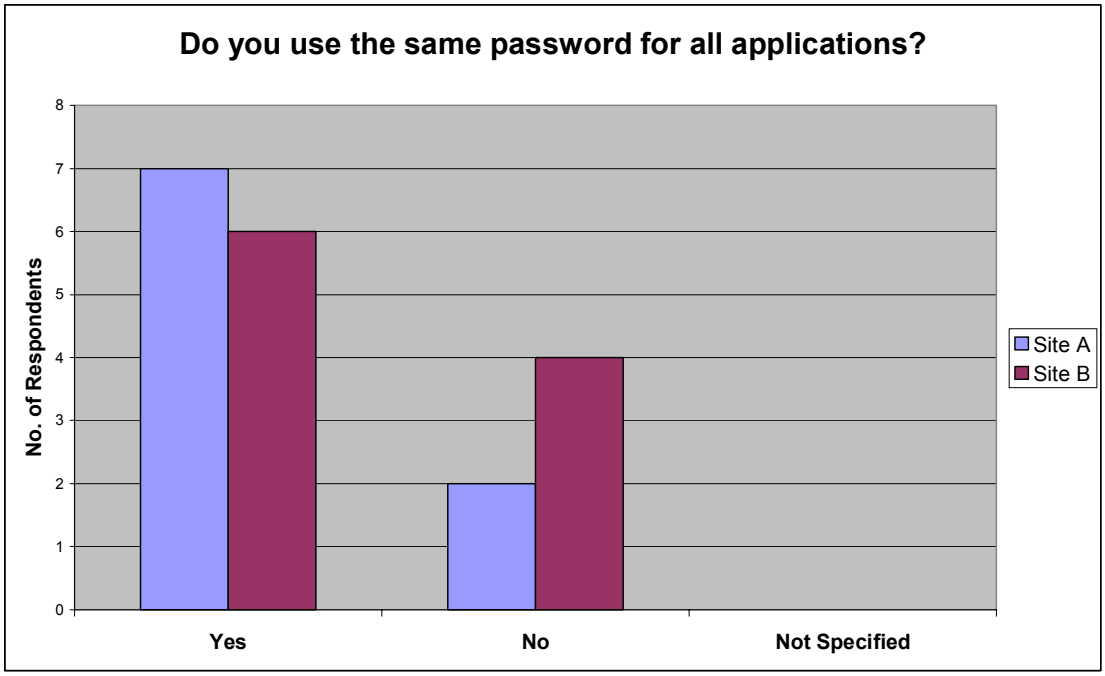

Figure 10– Do you use the same password for all applications?

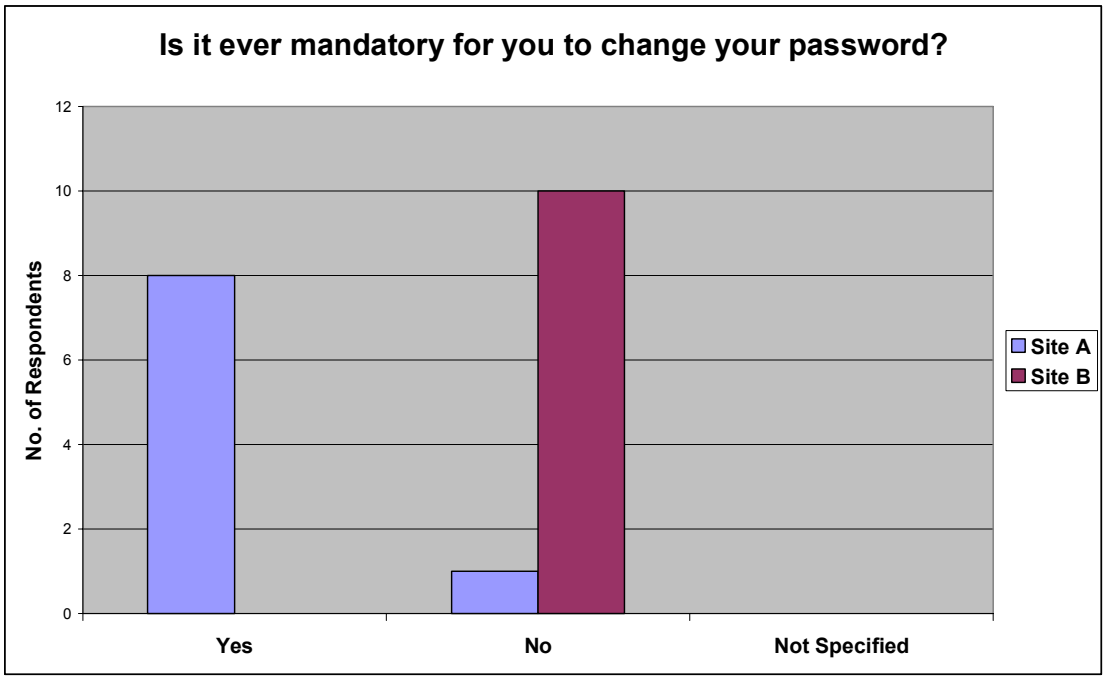

Figure 11– Is it ever mandatory for you to change your password?

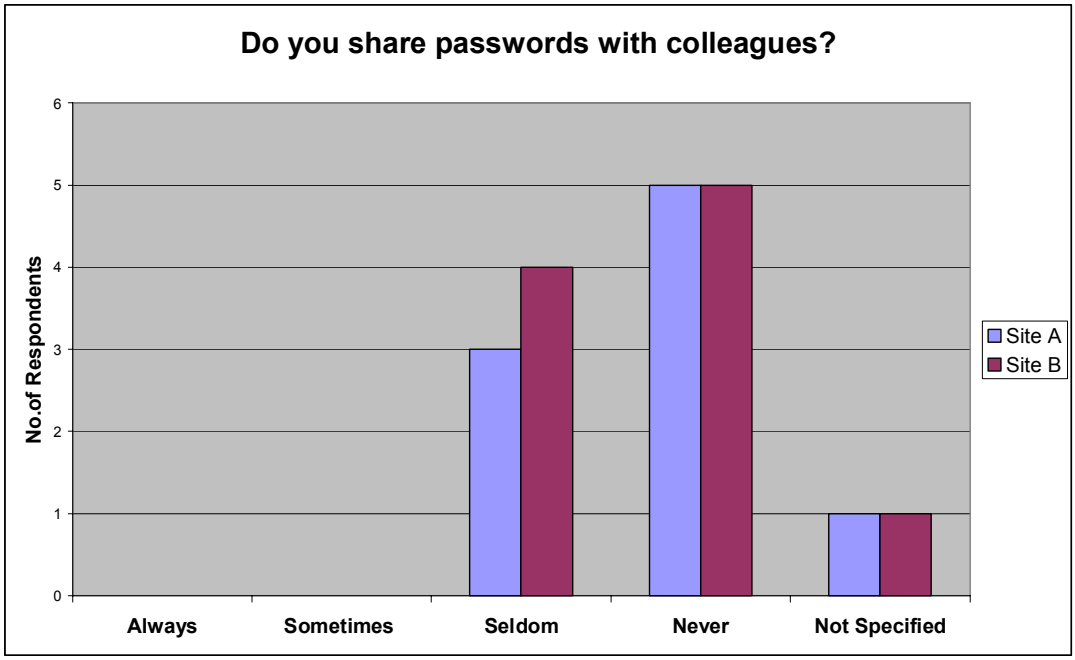

Figure 12– Do you share passwords with colleagues?

While 52% (n=10) say they never share passwords and 37% (n=7) say they seldom share passwords with colleagues it emerged that when asked if they are aware of other colleague's passwords 68% (n=13) in Figure 12 claimed that they were. Therefore, inferring that, in fact 68% are shared.

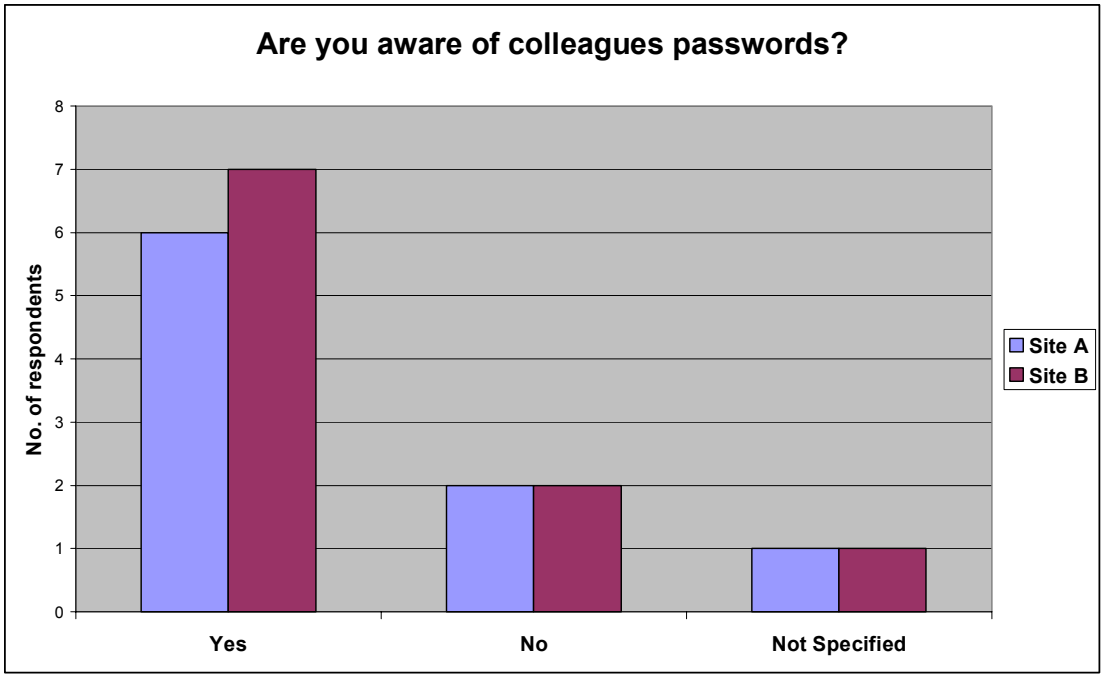

Figure 13– Are you aware of colleague's passwords?

4.4.3.3 Log On

This section was included to ascertain that session log out practices adhered to by the participating sites and the attitudes of users to the conditions implemented by the IT departments.

Respondents were asked if their device had a session log out time. 50% of participants from Site A confirmed that, yes, indeed their devices had a log out time which conflicted with the management audit which claimed that no log out restriction was in place to date. Conversely in Site B, 50% of participants claimed that they had no session log out time. This contradicted findings from the management audit, which expressed a definite session log out time of 10 minutes. The session logout time of 10 minutes has been agreed as a reasonable security measure in Site B. This may be an indication of the lack of experience of the participants at this location.

When asked if users have to re-logon, when moving from ward to ward the large majority, 78%, as seen in Figure 14, have said that they do not experience a connection drop when moving around the hospital. This is probably due to the fact that the 10-minute session logout time allows users to get to the next ward without losing the connection.

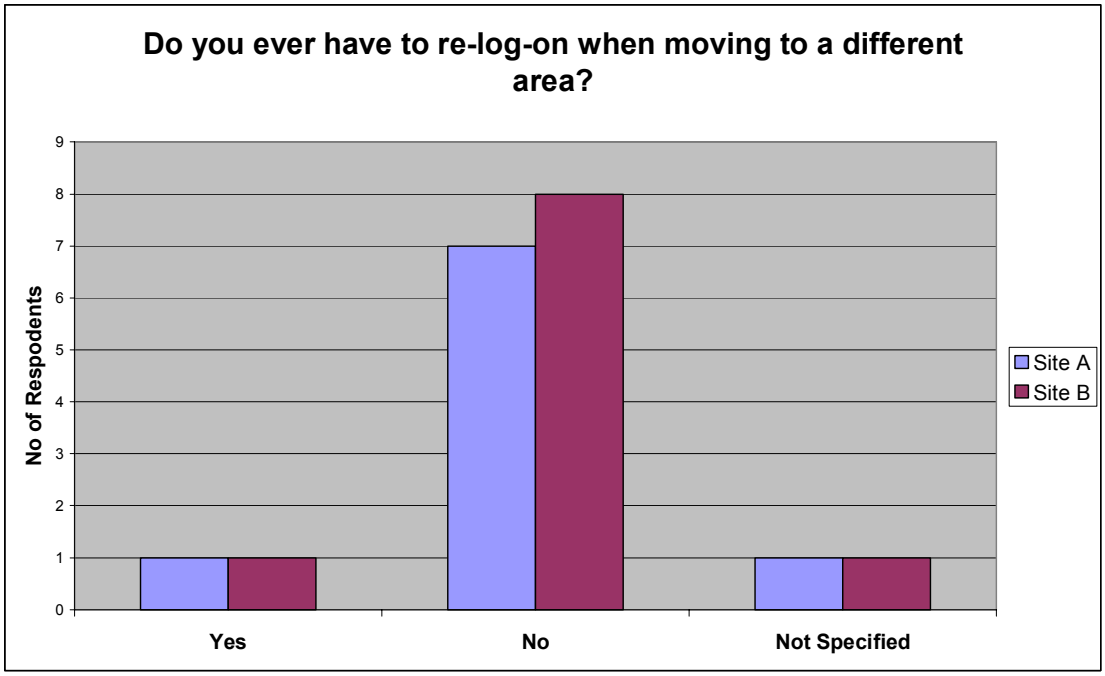

Figure 14– Do you ever have to re-logon when moving to a different area?

Participants were then asked if they ever allowed their colleagues to enter data on the mobile devices while they were personally logged on. Figure 15 displays the responses.

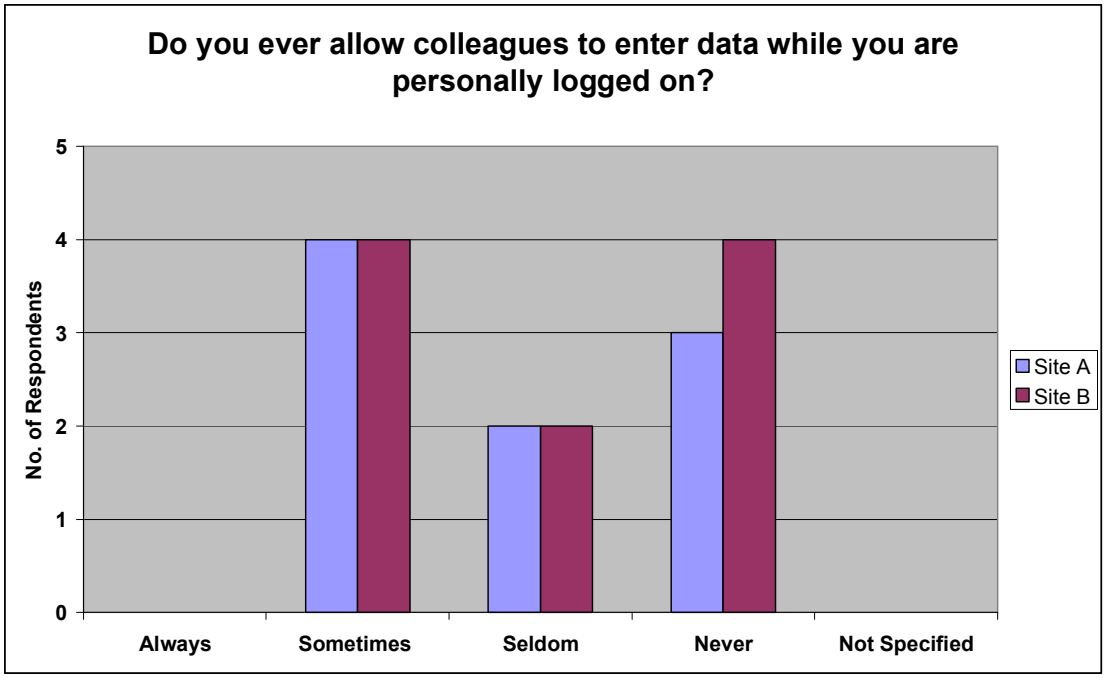

Figure 15– Do you ever allow colleagues to enter data while you are personally logged on?

When you take into account both the "Sometimes" and "Seldom" responses they amount to 63% of respondents who said they participate in letting colleagues enter data on their behalf, while personally logged on. This is quite a worrying trend, as the clinicians do not appear to consider the repercussions of being personally responsible for any patient data entered. This is possibly where training in the form of a wireless policy document, from the IT department could educate users. This training would hopefully lead to a reduction or even near elimination of this bad practice.

4.4.3.4 Security Issues

This Security Issues section aims to identify the level of knowledge that users have in relation to any issues associated with wireless security.

Included, were a number of areas where the users could express their comments or concerns. The uptake on this opportunity was very poor with only a few people expressing any view at all.

When asked if they were aware of any security issues at all, 89% of respondents claimed no knowledge, at all, of any security issues as shown in Figure 16. Again, it is felt that a clear policy document relating to wireless security would address this issue to some extent.

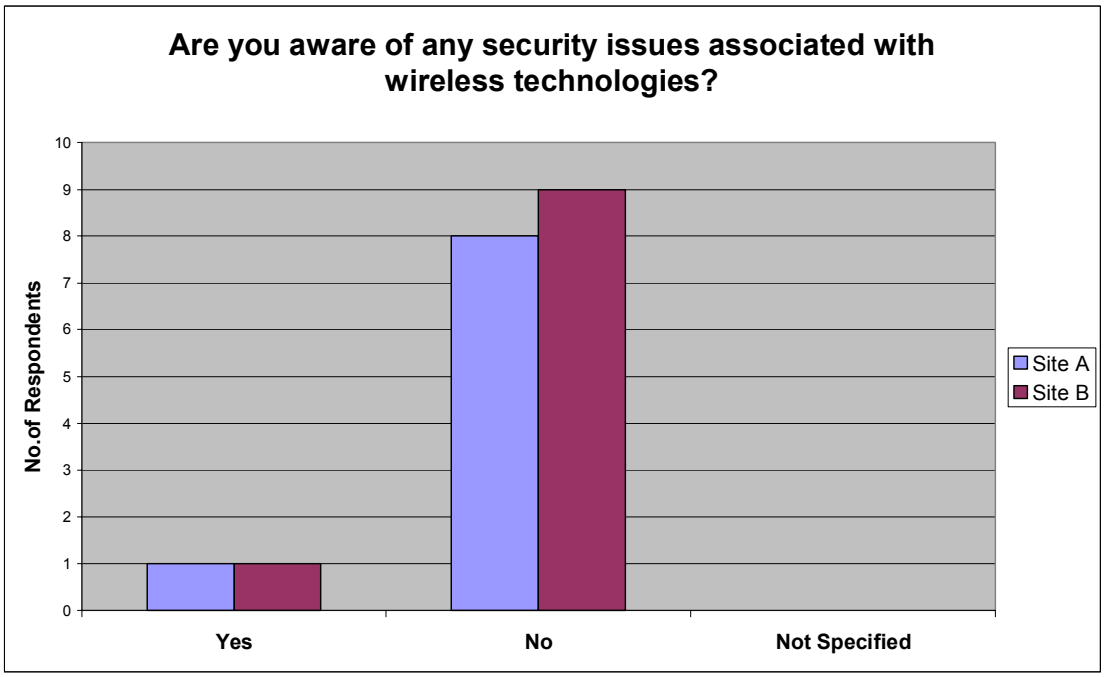

Figure 16– Are you aware of any security issues associated with wireless technologies?

Some of the comments that were received included the following:

- Ease of hacking compared to regular networks
- Viruses, hacking, but not sure how this happens
- System crashes – higher risk of hacking from external sources.

The question was posed without detailing any of the issues to get a feel for any awareness the user knows about without being prompted by a list.

From these responses it appears that users are not very aware at all of the issues associated with wireless technologies.

Following this participants were asked if they had any security concerns using their wireless mobile device. Figure 17 demonstrates that 89% appear to have no concerns about security issues and their device, at all.

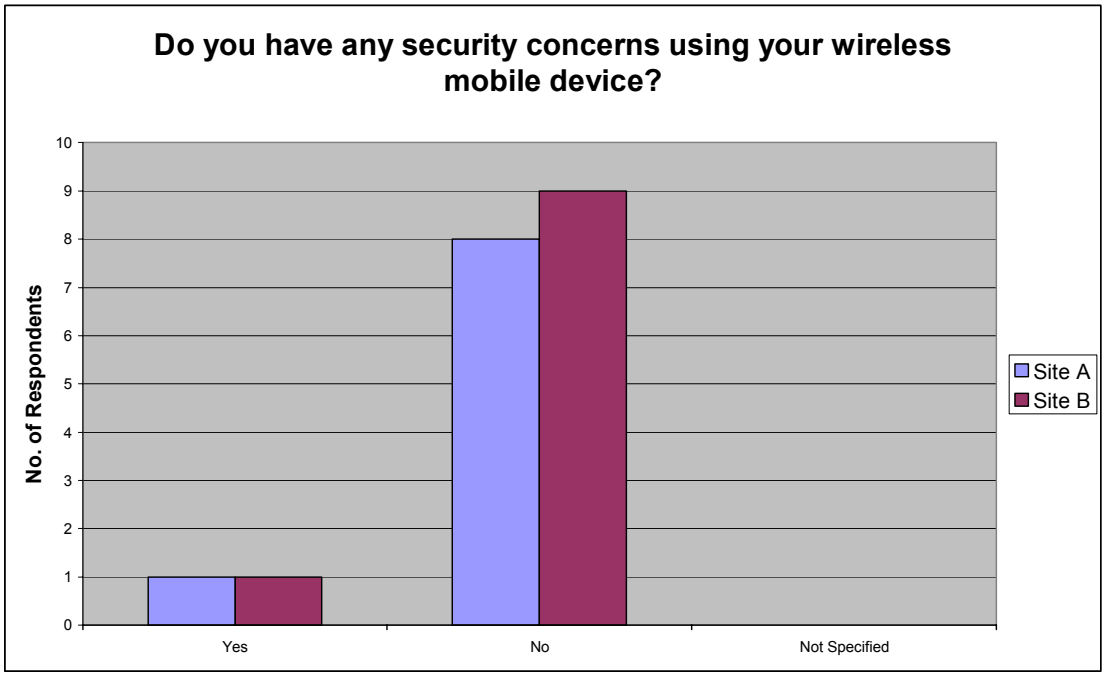

Figure 17– Do you have any security concerns using your mobile device?

Of the 11% that expressed some concern, the following comments were made:

- "I think they can be lost – placed down and left in wards – have seen that happen"

- "No internal policy on use – Often have to tend to patient as well as take notes – feel that just 1 person should take notes to minimize risk of loss or damage to device when left next to patient bed

Concerns with patient confidentiality were addressed by asking users if they thought that confidentiality is compromised by the use of wireless technologies. Figure 18 illustrates the level of confidence that users in both sites have with using wireless technologies as a means to collect and document patient information

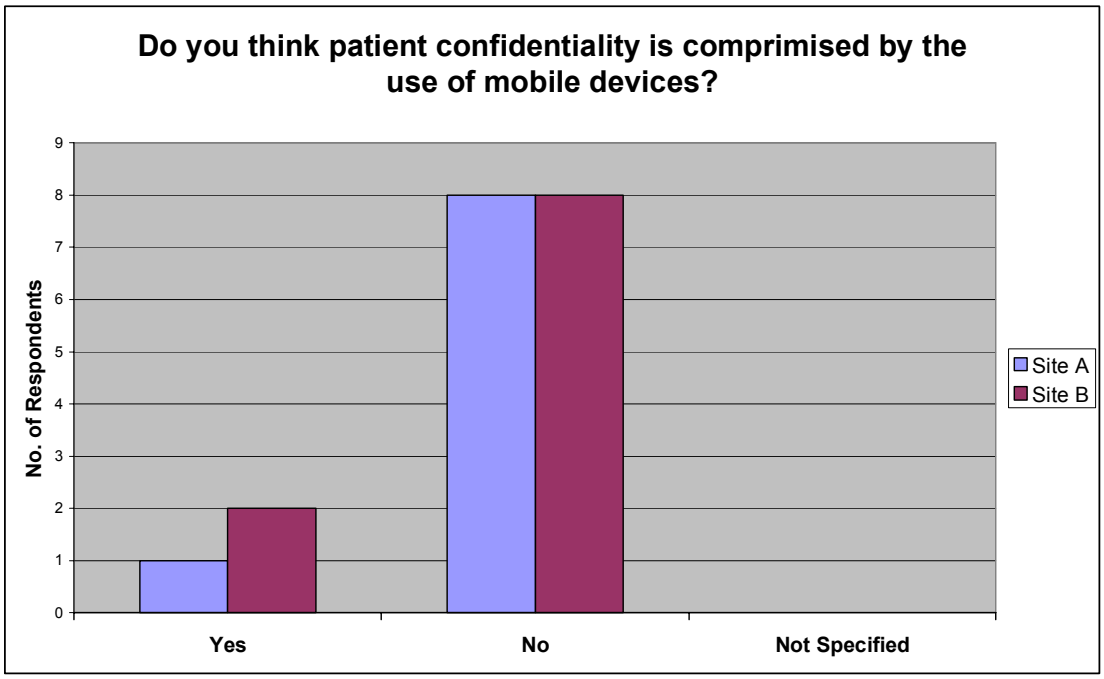

Figure 18– Do you think patient confidentiality is compromised by the use of mobile devices?

Following this, participants were given the opportunity to express any concerns they had in relation to patient confidentiality and mobile devices. Below are the responses that were documented.

- Often unsure if it is saved properly

- Due to the lack of training, IT staff are often called in to assist, and patient data is often exposed to them and others in sorting out issues.
- Lose connection all the time – Very annoying!
- Sometimes
- Don't know!

4.4.3.5 Further Comments

Users were asked "Overall how would you rate the level of wireless security at this location?" The documented responses were as follows:

- Not really sure
- Feel better training is necessary for both users on wireless technologies to ensure proper security of patient data
- No user training – or very little. Lots of sharing of passwords and device system crashes
- IT don't seem to assist when presented with problems and medical staff don't have enough technical knowledge to ensure patient confidentiality

The results that have been gathered through the audit and questionnaire have vividly shown us the current position in which Irish hospitals find themselves in relation to wireless security. It presents IT management with an opportunity to identify and address the concerns that users have, or indeed the assumptions that IT management may have made in relation to the behaviour of users. The next chapter analyses the results and documents the findings.

Chapter 5 – Analysis and Findings

This chapter presents discussion of the results of the audit and questionnaire as completed by the IT managers and users of wireless devices respectively. The impact of issues arising from the audit, together with the users awareness of issues of wireless security issues, are examined in an effort to improve the integrity of wireless networks in Irish hospitals.

5.1 Audit findings

In this section the results of the audit are examined. The audit was carried out in an attempt to find out if there were any vulnerability's in the WLAN. As mentioned previously the responses from both sites, for the most part, concurred. However, the notable exceptions lay in the areas of network and wireless security.

5.1.1 Conflicting points

Both sites had conflicting policies on mandatory password changing. Site A maintain that they have a policy of changing passwords every 90 days whereas Site B do not enforce password changes at any stage. Edward Hurley, News writer with Search Security maintains that changing passwords is another way to combat brute force attacks. Someone hell bent on cracking your password may need a few months to try all the combinations. Changing passwords every 60 or 90 days could foil such attempts. However, changing passwords too often isn't advisable as user confusion could tax IT resources as they constantly forget their passwords [55]. However in

saying this, according to Fred Cohen, who wrote a discussion on managing network security, unless there is a special circumstance, changing passwords even once in a while seems like a poor idea [56]. From this it is gathered that there are 2 schools of though on the practice of changing passwords with equally reasonable motives for the policy adopted.

When asked if there is a session timeout applied to all applications Site B assured that they did apply a session timeout of 10 minutes to all applications both on the wired and wireless network. Site A claimed that not all their applications had a session timeout applied, but that was being addressed as they were in the pilot stage of application roll-out when they completed the audit.

Cisco, worldwide leader in networking for the Internet, supports session timeout, which disconnects a user after a specified time of inactivity. After a session timeout, another person cannot use the connection [57]. This would appear to be a sensible security measure, as it limits the potential time that an intruder can access the data on the unattended mobile device. 10 minutes is the generally accepted industry standard for session timeout duration without being over disruptive to the user.

Another difference in response presented itself when asked if either location had performed a site survey. Site B responded that they had a site survey completed prior to wireless rollout whereas Site A had not. Again, Site A stated that they had a site survey planned before full wireless rollout.

The goal of a wireless site survey is to gather enough information and data to determine the number and placement of access points that will provide the coverage required. Coverage required usually means the support of a minimum data rate in a given area. A wireless network site survey also detects the presence of radio interference coming from other sources that could degrade the performance of your hospital WLAN [58].

It is evident from this that Site A should undertake a site survey as soon as possible because a new set of problems may manifest themselves post implementation of the wireless network in the designated area.

According to the datasheet published by Astro Communications Ltd, a technology advisory company based in the UK [59], whilst the importance of a site survey extends from pre-planning through to the install, is also very important to readjust the survey results at the commissioning stage as this is usually some time after the survey and the site would have invariably changed. Any change in the surrounding area could have an effect on the wireless network. The more accurate the information at survey and commissioning stages, the less time spent in problem determination during operation.

This suggests that completing a site survey early on in the wireless network deployment, identifies issues that could be addressed immediately and that subsequent issues can be dealt with on an individual basis as they arise.

5.1.2 Physical Security

Both sites declared that they did not secure or remove their USB/Serial ports on their mobile devices.

A recent survey conducted by Pointsec [60], a leading worldwide mobile security solutions company, shows that two thirds of IT professionals who use removable media at work admit they do not protect them with encryption. As the use of portable storage devices continues to infiltrate the boundaries of all organisations including healthcare, it should be imperative that all reasonable measures are taken to secure against theft of information.

According to Pointsec USB memory sticks/memory cards (76%) were the most popular mobile device to be used to download data in the healthcare sector followed by laptop/tablet PC (69%), PDA/Blackberry (51%), Smartphone (9%) and mobile phone (2%). This presents quite a worrying scenario for both sites as the findings from the questionnaire indicates that users are not aware of the security risks. It would be evident from these findings that a solution to secure USB ports on mobile devices be implemented post-haste.

HIPAA has suggested that special attention should be paid to the danger inherent in the theft of a wireless device that may provide a thief unauthorised access to protected health information [70].

Both sites signified that there were no physical safeguards in place for securing mobile devices. This seemed to be acceptable since they both use thin client

technology. Site B are currently using a Panasonic tough book which acts as a dumb terminal on the network.

5.1.3 Network Security

This section was included to get an idea of the current status of the wireless network. It applies to the general state of the network at both sites. In this section there were 2 opposing responses which have been discussed above. Both Site A and B agree that only authorised personnel have access to the wireless network. Information sharing over the network is limited as only the application that is required is made available. Also, information can only be saved on the server, not in local directories which would compromise security of information should the device be misplaced or stolen.

All information at both sites, transferred over the network, is encrypted using WEP 128 bit with an access list using MAC address authentication. Site A has plans to use Ciscos Secure ACS 4.0 (Cisco's radius server software) which will provide an even more secure environment for the transfer of confidential patient information. As an important component of the Cisco Identity-Based Networking Services (IBNS) architecture, Cisco Secure ACS extends access security by combining authentication, user or administrator access, and policy control from a centralized identity networking framework. This allows wireless networks to have greater flexibility and mobility, increased security, and user productivity gains [61].

5.1.4 Wireless Security

Risks in wireless networks are equal to the sum of the risk of operating a wired network (as in operating a network in general) plus the new risks introduced by weaknesses in wireless protocols [62].

The responses from the audit indicate that reasonable measures have been taken to secure the wireless network. Both sites ensure that their users have to authenticate themselves by logging on to the network via usernames and passwords. Both have said that any available patches are run as soon as they are released. This is reassuring, because the latest threats to the network can be avoided thus restoring confidence in the network.

Site B claimed they have performed a site survey to detect weakness in the wireless network and have taken appropriate measures to manage any risks identified. Site A have yet to complete a site survey, but have indicated that one has been organised and is soon to be performed. This is a crucial element of a wireless network as a proper site survey provides detailed information that addresses coverage, interference sources, equipment placement, power considerations and wiring requirements. The site survey documentation serves as a guide for network design and for the installation and verification of the Wireless communication infrastructure [63].

5.1.5 User Security

The aim of this section was to determine the importance placed on the user participation in the process of implementing a wireless network. The responses gathered indicate that efforts are mainly spent on the technical side of deploying the wireless network. Commentary with the IT management at both sites indicated that primary concerns were for the physical network and not the users. It was felt that once they were satisfied that the wireless network was secure; users were inherently protected as a result.

When questioned about the provision of security policies, it was found that both sites had a general 'acceptable use' security policy for their departments but no policy specific to wireless networks. Further commentary with management at Site B revealed that they felt it was an un-necessary waste of resources to provide a wireless security policy or training session.

From the findings of the questionnaire, it is evident that the behaviour of users, compromises the security of the wireless network every day. Therefore it is felt that it may not be an un-necessary waste of resources, but a shrewd decision to protect the integrity of the wireless network.

5.2 Questionnaire Findings

This section analyses the results of the questionnaire. The questionnaire was designed to ascertain the user's degree of knowledge about wireless security and the impact of

adhering to issues arising from the IT Management audit. The responses to the questionnaire have given a general insight to the current practices being observed by clinicians in Irish hospitals.

The questionnaire was divided into 4 sections, each of which gives us an insight into the knowledge and behaviour of clinical users of wireless networks.

1. ***Level of Knowledge*** - deals with ascertaining the users level of knowledge in relation to the concept of wireless technology
2. ***Passwords*** - details the password behaviour of users
3. ***Logon*** - ascertain that session log out practices adhered to by the participating sites and the attitudes of users to the conditions implemented by the IT departments.
4. ***Security Issues*** - section aims to identify the level of knowledge that users have in relation to any issues associated with wireless security.

5.2.1 Level of Knowledge

This section details the level of familiarity with mobile devices and wireless networking. When participants were asked to rate their level of competency in the use of mobile devices 43% of users considers themselves to be quite competent-excellent. It was noted that Site B had a much higher level of confidence in their ability as compared to Site A. This would appear to be as a result of the fact that they have been using a wireless network for a number of years and that Site A have just rolled out

their wireless network in the department that was being surveyed. Although, when asked about the frequency of data entry on their mobile device 58% of users said that they never enter data on mobile devices. On investigation into the apparent disparate nature of this response, I was informed by the consultant that the team had just changed over in the pervious week, and that they had not had the opportunity yet to enter data on mobile devices, but that soon, every doctor on the team would record the patient data on the mobile devices.

Users were asked if they felt they had received adequate training in the areas of

1. Applications that are being used every day, and
2. Wireless security

With a response rate 42% feeling that they have not received adequate training on the applications and 89% expressing that they had not received any training or information relating to wireless security it is apparent that not enough attention has been devoted to fully training users on the device they are expected to use every day.

The technology acceptance model (TAM) devised by Davis is seen to be the most influential theoretical approach in studying the determinants of IT utilisation [64]. According to TAM, perceived ease of use and usefulness are assumed to be strong determinants of the actual and successful utilization of technology [65]. It would seem that if users were better informed and trained sufficiently in the use of the device they may have a more positive attitude towards adopting any security protocols that have to be adhered to.

5.2.2 Passwords

In relation to passwords, this section aimed to identify the behaviour of users with their passwords.

89% of users said that their mobile device was password protected it is assumed that the 11% who responded negatively had not used department mobile devices and perhaps did not understand the question since it is known to be true that mobile devices for both sites are password protected.

A contrasting point that presented itself was the behaviour of changing passwords. Site A has a policy of mandatory changing of passwords at regular intervals whereas Site B does not implement such a policy. As such, 89% of users in Site B claim that they never change their passwords.

It would appear that a policy of changing passwords is good security practice, though not absolutely essential. Since there are no definitive national guidelines on security of health information in Ireland, the HIPAA security guidelines were looked at to see if there was a policy on password usage. It seems that passwords are not actually required by HIPAA, but it is generally accepted that a policy to change passwords at agreed intervals, is a good security policy decision [66].

Participants were then asked if they share passwords with other colleagues. 37% of users claim that they do indeed share their password from time to time. This is a very worrying statistic considering the sensitive nature of the data they are dealing with. After that users were asked if they were aware of other colleague's passwords. It emerged that a phenomenal 68% of users knew at least one or several of their

colleague's passwords. Frequently doctors share passwords for electronic patient records and hospital computer systems, as it is difficult and often time consuming to attain their own passwords, especially when very short-term locums are being undertaken. This should be avoided at all costs as it compromises data security [67]. This would indicate that passwords are being shared amongst doctors more than they would like to admit.

The results from both sites were similar, with 60% from Site A and 70% from Site B being aware of other colleague's passwords. The lower level of password knowledge, though still concerning, in Site A, may be attributed to the fact that they do have a policy of changing passwords periodically.

A recent survey by the organizers of the Infosecurity Europe conference found that 90% of office workers would reveal their passwords to a researcher at Waterloo Station in London. Last year, 65% of those surveyed gave up their passwords [68]. It seems that the practice of sharing passwords, across a spectrum of industries, is a major problem that needs to be addressed as a fundamental security measure.

5.2.3 Log On

According to the Audit conducted it emerged that at that time only one site (Site B) had implemented a session logout for the application being used on the wireless network. Site A are to implement a similar session timeout of 10 minutes in the near future, once they have fully rolled out their application wirelessly. It is seen as a basic

security measure; especially in wireless networks where the devices are mobile and can be left down or misplaced easily. The 10 minute session logout time allows users to go between wards, where there is no access point along the way, without losing connection to the application being used. This amount of time appears entirely adequate, as 78% of users reported that they never experience a connection drop on their daily rounds.

Users were also asked if they ever allowed other colleagues to enter data on their behalf while personally logged on. While 37% of total participants said that they never let anyone enter data on their behalf, a considerable 63% declared that they have at one time or another let their colleagues enter data on their behalf. This casual attitude would appear to be as a direct result of the evident lack of training and information on wireless security. The users don't seem to realise the consequences of their actions. For example; one doctor is logged on and has to attend to a patient. He then hands over the mobile device to the next doctor and asks them to enter patient data on his behalf while currently logged on. The second doctor carelessly enters incorrect information. This incorrect information is then recorded against the first doctor's account. Should a legal issue arise as a consequence of this incorrect information, the onus lies with the first doctor, as he is personally responsible for the information recorded against his logon account. It seems that if users were educated in the risks and consequences of their actions that such practice would be considerably reduced.

5.2.4 Security Issues

Following on, an attempt was made to see if any of the users were aware of any issues relating to wireless security. A substantial 89% of users claimed no knowledge of security issues. This implies that adequate consideration is not given to educating and training the users. This is a problem, for all the other areas that have been examined in the study.

It has emerged that users have no concept of what they are dealing with and they don't appear to be sufficiently concerned. 89% have no security concerns using mobile devices and a further 84% don't think that patient confidentiality is compromised by the use of mobile devices.

These figures should not prove to be a problem for users but more a concern for the IT management. The responsibility lies with IT to ensure that users don't have to be overly concerned with the confidentiality issues of using mobile devices as a means of recording patient information. They should take the appropriate measures to ensure that mobile device usage is as secure as possible without infringing on the users ability to perform their duties. As far as this issue is concerned, both sites have adopted thin client technology. This is a prudent security measure as the clients only act as a dumb terminal, which means that all data is saved and backed up on the server. The thin client has little processing ability. Once the mobile device leaves the wireless network coverage area, i.e. outside the door of the hospital, the client is useless, as it has no information stored locally.

According to Fredrik Björck, who completed his Ph.D on "Interpreting the Practice of Managing Information Security in Organisations" there appears to be a discrepancy between what people say and what they do. The mere fact that employees, through an information security education and training programme, arrive at a measurable raised awareness of the information security regulations does not signify that they actually follow these rules or values – at least not all of them. Further, when trying to measure the impact of information security education and training, there is a possibility that some employees *do not* want to state the truth about their own level of awareness. They might be anxious concerning what the employer's reaction would be if they admitted that they did not know of the rules they were supposed to adhere to. Therefore, from an organisational perspective, the focus should not be on what an employee knows about information security, but rather what she does with this knowledge. [69]

Chapter 6 - Discussion

6.1 Conclusions

In an ongoing attempt to improve patient care, mobile devices have been adopted to provide real-time access to patient data. Clinicians are also able to record updates to a patient's medical record at the bedside. This has facilitated the clinician's ability to make immediate, life critical decisions away from a stationary information terminal. Wireless local area networks (WLANs) have proven indispensable to the hospitals primary objective of delivering outstanding patient care. The WLAN solution lets healthcare professionals spend less time on administrative tasks such as retrieving records, freeing up more time to spend with patients [71].

Whilst the tremendous benefits of having mobile devices on wireless networks seem to entice many clinicians to embrace this technology, the issues of security for the devices and the wireless networks appears to be quite a minefield.

According to the United States Government Accountability Office [73], who wrote a report in May 2005 on Information Security Controls such as policies, practices, and tools, can help to mitigate wireless network security challenges that federal agencies face. These controls include

- Developing comprehensive policies that govern the implementation and use of wireless networks,
- Defining configuration requirements that provide guidance on the deployment of available security tools,

- Establishing comprehensive monitoring programs that help to ensure that wireless networks are operating securely, and
- Training employees and contractors effectively in an agency's wireless policies.

From a security perspective, wireless systems inherently increase potential security weak points. It is unlikely that most organisations will adopt a purely wireless infrastructure (at least for the foreseeable future) since corporations already have considerable investment, expertise and processes tied up in the existing wired infrastructure. Consequently, most organisations will operate both wireless and wired systems and so increase the potential channels and points for security breaches [72].

This opinion is reflected in the findings from the IT management audit whereby both sites had a general 'acceptable use' security policy for their wired network that, at the time, was seen to be sufficient for the wireless network also.

In light of technological advances, such as lighter mobile devices, it would appear that most departments will be requesting access to the wireless network in the near future. It is widely agreed in the literature, that evolving technologies such wireless network technologies now demand definitive, exclusive policies for wireless security As such, it is felt that it would be a prudent move to document a specific wireless security policy, and educate the users about the risks associated with wireless technologies. After presenting the findings of the research to the IT managers, they both agreed that the creation of such documentation would be a progressive benefit for the organisations. Site A has already undertaken the task of documenting such a policy,

whilst Site B has agreed that it will be documented and implemented in the very near future.

One of the objectives of the research was to ascertain the level of awareness of users to security issues associated with wireless mobile devices. According to the questionnaire an overall 89% of users at both sites declared that they had not received any training or information relating to wireless security.

The lack of knowledge demonstrated by the users, in relation to the security issues associated with the devices they use every day, highlighted an urgent need for training in this area.

It is felt that it would be beneficial for IT management to communicate more with users to gain a more comprehensive view of the status of their wireless network. Though establishing policies to govern wireless networks would appear to be a basic requirement, institutions often fail to take this step or to inform employees of the risks associated with not using a wireless network in accordance with the policies. Once policies are implemented, it's critical to communicate them to increase users' awareness and understanding [74]. Through the actual process of compiling a comprehensive specific wireless security policy, the IT management would be forced to address the issues that concern user practices. This may reduce the very high incidence of password and logon session sharing among clinicians that is evident from the findings of the study.

It has also been noted that both sites from a technical IT management point of view appear to be very conscientious about applying the best standards of

wireless security available currently. Also 'Site Surveys', to determine any vulnerability in the wireless network appear to be common practice. This will place both sites in a good position to document and adopt a wireless security policy.

6.2 Recommended future work

It is recommended that the lack of documentation be addressed through the introduction of a policy specific to wireless networks, paying particular attention to 'acceptable use' for users.

After a specified time, of perhaps a year, another questionnaire could be completed by users to see if the policy guidelines have had any impact on user's behaviour. This would give us a good indication of the benefits of developing such policies. In saying that, however, it is felt that the IT management would need to take a proactive approach to the implementation of such a policy to reap the full potential benefits of the project. It is important to keep systems administrators informed of technical advances and protocols, but it's equally important for users to understand the reasons for the protocols. An educated user will more likely be a compliant one, without much protest [74].

6.3 Final Remarks

As hospitals adopt wireless technologies the issues surrounding the security of these networks becomes an ever increasing challenge. Through the process of choosing this topic for research and arriving at this point it is felt that wireless security issues can be

more easily identified and managed if specific policies exist. The users need to be empowered through a proactive approach of delivering information and awareness in the form of a wireless security policy.

With all the exciting potential benefits that mobile devices on wireless networks can offer, one can only assume that wireless is here to stay. As such, it seems that this is the perfect time to implement all reasonable security measures, such as wireless policies, to provide a secure environment for workers and most of all “The Patient”.

References

[1] Measures of satisfaction in wireless technology use: The case of Baylor Health Care System.
http://www.txcdk.org/docs/BHCSwireless.v5.pdf (Accessed 28th September 2006)

[2] L.L. Leape, Error in medicine. J. Am. Med. Assoc. 272 (1994), pp. 1851–1857.

[3] J.T. Reason, Human Error, Cambridge University Press, Cambridge, 1990.

[4] L.L. Leape, D.W. Bates, D.J. Cullen, J. Cooper, H.J. Demonaco, T. Gallivan, R. Hallisey, J. Ives, N. Laird, G. Laffel et al., Systems analysis of adverse drug events, ADE Prevention Study Group. J. Am. Med. Assoc. 274 (1995), pp. 35–43.

[5] David Rullo, M.D., Why Work Wireless? (2000). How to reduce medical errors, from the palm of your hand.
http://www.healthmgttech.com/archives/h0900wireless.htm (Accessed 28th September 2006)

[6] Rick Kwon, Guilin Lu , Ray Pabilonia, David Wein, Reducing Medication Errors Through the Use of Wireless LANs and Handheld Computers;
http://www.cyberfab.net/Documents/eHealth/Barcodes/medicationerrors.pdf
(Accessed 28th September 2006)

[7]. Schwartz, J. (2004). Patient safety drives IT spending. VARBusiness, 20(7), p22.

[8] HIPAA Advisory,
http://www.hipaadvisory.com/REGS/HIPAAprimer.htm (Accessed 28th September 2006)

[9] Dr. Bill Crounse, M.D. Mobile devices usher in new era in healthcare delivery
http://www.microsoft.com/industry/healthcare/providers/businessvalue/housecalls/housecalls_mobility.mspx (Accessed 28th September 2006)

[10] Components of HIPAA Security Policy Template.
http://www.hipaaacademy.net/HIPAASecurityPolicies/hipaaSecurityPolicyTemplatesComponents.html (Accessed 28th September 2006)

[11] IEEE Standard for Wireless LAN Medium Access Control
(MAC) and Physical Layer (PHY) Specification, P802.11, 1999.

[12] D.P. Agrawal, Q.-A. Zeng, Introduction to Wireless and Mobile Systems, Brooks/Cole Publishing, 2003, ISBN 0534-40851-6, 436 p.

[13]Edgar Danielyan, IEEE 802.11, “Articles of Interest" vol. 1 no. 1.
http://www.isoc.org/pubs/int/cisco-1-1.html (Accessed 28th September 2006)

[14] Pablo Brenner, IEEE 802.11The New wireless LAN Standard.

http://www.itconnection.ru/support/pdf_repository/technical_tutorial_on_802_11_standard.pdf (Accessed 28th September 2006)

[15] IEEE 802.11: Wireless LAN Security Performance Using Multiple Clients. http://www.medialab.co.nz/assets/downloads/IEEE%20802.11%20Wireless%20LAN%20Security%20Performance.pdf (Accessed 28th September 2006)

[16] Cisco Unified Wireless Network, Five Steps to Securing Your Wireless LAN and Preventing Wireless Threats http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_white_paper0900aecd8042e23b.shtml (Accessed 28th September 2006)

[17] Introduction to IEEE 802.11. http://www.intelligraphics.com/articles/80211_article.html (Accessed 28th September 2006)

[18] Securing Wireless LANs with PEAP and Passwords, Introduction: Choosing a Strategy for Wireless LAN Security, http://www.microsoft.com/technet/security/topics/cryptographyetc/peap_int.mspx (Accessed 28th September 2006)

[19] Eric Janszen, Understanding Basic WLAN Security Issues. http://www.wi-fiplanet.com/tutorials/article.php/953561 (Accessed 28th September 2006)

[20] Seth Fogie, Windows XP Wireless Security. http://www.informit.com/articles/article.asp?p=28694&seqNum=2&rl=1 (Accessed 28th September 2006)

[21] Jim Zyren , Al Petrick IEEE 802.11 Tutorial. http://www.packetnexus.com/docs/IEEE_80211_Primer.pdf (Accessed 28th September 2006)

[22] Jakob E. Bardram, Centre for Pervasive Computing, Department of Computer Science, University of Aarhus, Aabogade 34, 8200 °Arhus N, Denmark. The Trouble with Login – User Authentication and Medical Cooperation. http://www.daimi.au.dk/~cfpc/publications/files/trouble_login.pdf (Accessed 28th September 2006)

[23] Tom Karygiannis, Les Owens, Wireless Network Security 802.11, Bluetooth and Handheld Devices. http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf (Accessed 28th September 2006)

[24] Lor´ and Jakab, Albert Cabellos-Aparicio, Ren´ e Serral-Graci` a, Jordi Domingo-Pascual, Software Tool for Time Duration Measurements of Handovers in IPv6 Wireless Networks, May 24, 2004. http://people.ac.upc.edu/ljakab/homtool.pdf (Accessed 28th September 2006)

[25] SafeWord and HIPAA.

http://www.securecomputing.com/index.cfm?skey=672 (Accessed 28th September 2006)

[26] National Health Information Strategy(2004)
http://www.dohc.ie/publications/pdf/nhis.pdf?direct=1 (Accessed 28th September 2006)

[27] Artnak, K. E. and M. Benson (2005). "Evaluating HIPAA compliance: A guide for researchers, privacy boards, and IRBs." Nursing Outlook 53(2): 79-87.

[28] G.J. Annas, HIPAA regulations - a new era of medical-record privacy. *New England J Med* 348 (2003). pp. 1486–1490.
[29] K.L. Montgomery, HIPAA the health insurance portability and accountability act legislation, *Policy, Politics Nurse Practice* 2 (2001), pp. 29–32.

[30]HHS News (1998). HHS proposes security standards for electronic health data. http://aspe.os.dhhs.gov/admnsimp/nprm/press3.htm. (Accessed 28th September 2006)

[31] K.E. Hanna, No end in sight for final rules on medical privacy, *Hastings Center Report* 31 (2001), p. 8.

[32] Collmann, J., D. Lambert, et al. (2004). "Beyond good practice: why HIPAA only addresses part of the data security problem." International Congress Series 1268: 113-118.

[33] HIPAA & WiFi: Regulatory Tangles for Wireless Health Care Networks Analyzed
http://www.hipaadvisory.com/tech/wireless.htm (Accessed 28th September 2006)

[34] HIPAA Security Rule Overview, Physical Safeguards (164.310).
http://www.hipaaacademy.net/consulting/hipaaSecurityRuleOverview.html (Accessed 28th September 2006)

[35] AHA Regulatory Advisory. The Final HIPAA Security Rule: Making Progress in Implementation.
http://www.aha.org/aha/key_issues/hipaa/content/hipaaadvisory082203.doc
(Accessed 28th September 2006)

[36] Wireless Networking in Hospitals.
http://www.hp.com/rnd/itmgrnews/wireless_hospital.htm (Accessed 28th September 2006)

[37] Professor Merida L Johns Privacy and Security Regulations for Health Information.
http://www.wma.net/e/publications/pdf/2001/johns.pdf (Accessed 28th September 2006)

[38] Kindberg, T., A. Sellen, et al. (2004). Security and Trust in Mobile Interactions: A Study of Users Perceptions and Reasoning.

[39] The SANS Security Policy Project
http://www.sans.org/resources/policies/ (Accessed 28th September 2006)

[40] Jaikumar Vijayan, Gartner sees growing need for wireless security policies, Companies need to think about more than securing WLAN access points
http://www.computerworld.com/securitytopics/security/holes/story/0,10801,93785,00.html?from=story_kc (Accessed 28th September 2006)

[41] David Watson, Expert lapse shows wireless security policy needed.
http://computerworld.co.nz/news.nsf/NL/FA93A71354DD95E3CC256E4300065BB4 (Accessed 28th September 2006)

[42] Mary E. Shacklett, Securing the Airways By: September 1, 2005 URL: http://www.computeruser.com/articles/2409,1,2,1,0901,05.html (Accessed 28th September 2006)

[43] Siemens; Wireless Network Security
http://www.insight.co.uk/files/datasheets/Wireless%20Network%20Security%20(Datasheet).pdf (Accessed 28th September 2006)

[44] Georgetown University, Wireless Networking Guidelines.
http://uis.georgetown.edu/policies/technology/wirelessguide.html (Accessed 28th September 2006)

[45] The hidden benefits of HIPAA.
http://www.sun.com/br/healthcare_609/feature_hipaa.html (Accessed 28th September 2006)

[46] HIPAA Security Policy Templates.
http://www.hipaaacademy.net/HIPAASecurityPolicies/hipaaSecurityPolicyTemplates.html (Accessed 28th September 2006)

[47] Tom Karygiannis, Les Owens Wireless Network Security 802.11, Bluetooth and Handheld Devices
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf (Accessed 28th September 2006)

[48] http://www.sans.org/score/checklists/EnterpriseWirelessNetworkAudit.pdf (Accessed 28th September 2006)

[49]Andrew Z. Tabona, An Overview of Wireless Network Security.
http://www.windowsnetworking.com/articles_tutorials/Overview-Wireless-Network-Security.html (Accessed 28th September 2006)

[50] Wireless Networking Basic Security Checklist.
http://www.netstumbler.org/showthread.php?t=6492 (Accessed 28th September 2006)

[51] Oppenheim AN. Questionnaire design, interviewing and attitude measurement. London: Continuum, 1992.

[52] Sapsford R. Survey research. London: Sage, 1999.

[53]http://wireless.ittoolbox.com/documents/research/survey.asp?survey=vernier survey&p=1(Accessed 28th September 2006)

[54] Rigby M, Forsström J, Roberts R, Wyatt J. Verifying quality and safety in health informatics services. *BMJ* 2001; 323: 552-556

[55] "Proper password policy is imperative" Edward Hurley, 08 Jul 2002, SearchSecurity http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci837272,00.html(Accessed 28th September 2006)

[56] Managing network security — Part 10: Change your password • Discussion, Fred Cohen, Network Security, Volume 1997, Issue 9, September 1997, Pages 8-11

[57] http://www.cisco.com/warp/public/614/7.html(Accessed 28th September 2006)

[58]http://www.infologixsys.com/products/Healthcare/Products/Wireless%20Network/Site-Survey/default.asp (Accessed 28th September 2006)

[59]http://www.astro.co.uk/datasheets/wireless/whatiswifi.pdf(Accessed 28th September 2006)

[60] Pointsec survey Removable Media in the Workplace, carried out amongst 248 IT professionals at InfoSecurity, April 2006 in London.

[61]http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_bulletin0900aecd803882de.html (Accessed 28th September 2006)

[62] Tom Karygiannis, Les Owens, Wireless Network Security 802.11, Bluetooth and Handheld Devices http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf. (Accessed 28th September 2006)

[63]http://www.cisco.com/en/US/tech/tk722/tk809/technologies_q_and_a_item09186a00805e9a96.shtml#qa2

[64] Katrin Arninga, and Martina Ziefle, a, Understanding age differences in PDA acceptance and performance Department of Psychology, RWTH Aachen University, Jaegerstrasse 17-19, Aachen 52056, Germany Computers in Human Behavior , Article in Press, Corrected Proof

[65] Davis, 1989 F.D. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Quarterly 13 (1989), pp. 319–340.

[66] Best Practices: Passwords excerpted from Lockdown: Security Compliance Under HIPAA ,Tom Walsh, CHS, CISSP, Decisions in Imaging Economics, November 2004

[67] Ismail A, Ismail M. To opt in or opt out of electronic patient records? Poor training of locums in using hospital computer systems poses risk. BMJ. 2006 Jul 15;333(7559):147

[68] Edward Hurley, News Writer, Study: Employees willing to share passwords with strangers 24 Apr 2003 | SearchSecurity.com
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci895483,00.html(Accessed 28th September 2006)

[69] Security Scandinavian Style, Interpreting the Practice of Managing Information Security in Organisations
http://www.dsv.su.se/~bjorck/files/bjorck-thesis.pdf, (Accessed 28th September 2006)

[70] HIPPA & WiFi: Regulatory Tangles for Wireless Health Care Networks Analysed
http://www.hipaadvisory.com/tech/wireless.htm, (Accessed 28th September 2006)

[71] Overlake Hospital Improves Patient Care, Reduces Errors, Increases Productivity
http://www.cisco.com/en/US/netsol/ns642/networking_solutions_customer_profile0900aecd802fd374.html(Accessed 28th September 2006)

[72]Vasilios Katos and Carl Adams, Modelling corporate wireless security and privacy, The Journal of Strategic Information Systems, Volume 14, Issue 3, The Future is UNWIRED: Organisational and Strategic Perspectives, September 2005, Pages 307-321.

[73] Federal Agencies Need to Improve Controls over Wireless Networks
http://www.gao.gov/new.items/d05383.pdf (Accessed 28th September 2006)

[74] Susan Kennedy, Best Practices for Wireless Network Security
http://www.computerworld.com/printthis/2003/0,4814,86951,00.html(Accessed 28th September 2006)

Appendix A. Abbreviations

Ap	Access Point
b	bit
BSS	Basic Service Set
CA	Collision Avoidance
CIA	Confidentiality, Integrity, Availability
CSMA	Carrier Sense Multiple Access
DoS	Denial of Service
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
ePHI	Electronic Protected Health Information
ESS	Extended Service Set
FHSS	Frequency hopping Spread Spectrum
GHz	Giga Hertz
HIMSS	Healthcare Information and Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information Communications Technology
IEEE	Institute of Electrical and Electronic Engineers
IR	Infra Red
IT	Information Technology
LAN	Local Area Network
MAC	Medium Access
Mbps	Megabytes

NIC	Network Interface Card
NIST	National Institute of Standards and Technology
OSI	Open System Interconnection
PDA	Personal Digital Assistant
PHI	Protected Health Information
PHY	Physical Layer
SCSI	Small Computer System Interface
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
STA	Station
TAM	Technology acceptance Model
USB	Universal Serial Bus
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Appendix B. IT Management Audit

Wireless Network Security Audit for IT Management

Physical Security

1. Are the parallel/serial/infrared/USB/SCSI ports secured or removed?
   Yes ☐ **No** ☐
2. Are the wireless devices physically locked down to the system?
   Yes ☐ **No** ☐
3. Have you an inventory of all access points?
   Yes ☐ **No** ☐
4. Are there any physical boundary safeguards in place?
   Yes ☐ **No** ☐

Comments:_____

_____

_____

_____

Network Security

5. Do only authorised personnel have physical access to the wireless Network?
   Yes ☐ **No** ☐
6. Have you checked all the vendors for security patches, and do you regularly receive security updates about patches/vulnerabilities to the software you use in a wireless environment?
   Yes ☐ **No** ☐
7. Do you effectively limit your users` abilities to make sensitive information about the system available over the network?
   Yes ☐ **No** ☐
8. Do user accounts that are accessible over the network regularly have their passwords changed?
   Yes ☐ **No** ☐
9. Do you encrypt sensitive data that is transferred over the network?

Yes ☐ **No** ☐

10. Is there a session timeout applied to all applications?

Yes ☐ **No** ☐

Comments:_____

_____

_____

_____

Wireless Security

11. Do you have some form of logging enabled?

Yes ☐ **No** ☐

12. Do you log and audit guest user activity?

Yes ☐ **No** ☐

13. Have you performed a site survey to find out exactly where the signal starts and ends?

Yes ☐ **No** ☐

14. Do you test your configuration of the software thoroughly; ie. Try to break it, try to hack into it, and see if others can do the same?

Yes ☐ **No** ☐

15. Have you checked for the latest releases of any available patches?

Yes ☐ **No** ☐

16. If a program accesses sensitive data, do you make sure that it can only be executed by authorized users?

Yes ☐ **No** ☐

Comments:_____

_____

_____

_____

User security

17. Do you have a standard method for creating and maintaining user accounts?

    Yes ☐ **No** ☐

18. Do you have clear and concise acceptable use policies for your users?

    Yes ☐ **No** ☐

19. Do you have a policy specific to wireless users?

    Yes ☐ **No** ☐

20. Are users made aware of the risks associated with wireless technology and security?

    Yes ☐ **No** ☐

21. Do you set limits on the amount of resources a user can consume, from number of logins to amount of disk space?

    Yes ☐ **No** ☐

22. Do you keep accurate logs of user activity? i.e., connection time, connection duration and the place where they logged in/connected from.

    Yes ☐ **No** ☐

Comments:_____

_____

_____

_____

Appendix C. User Questionnaire

	Site ID: _____ **User ID:** _____

Questionnaire to determine user's attitudes towards wireless security

Job Title: _____

Level of Knowledge

1. How would you rate your competency in the use of mobile devices (e.g. Tablets)?

   Excellent ☐ ☐ ☐ ☐ Poor

2. Have you received adequate training on all the applications that you use?

   Yes ☐ No ☐

3. Have you received <u>any</u> wireless security training (Relating to mobile devices?)

   Yes ☐ No ☐

   3.1. If "Yes". Are you satisfied with your level of training?

   Yes ☐ No ☐

4. When entering/updating patient data – How often is this done on your wireless mobile device?

   Always ☐ ☐ ☐ ☐ Never

Passwords

5. Are all applications on your wireless mobile device password protected?

   Yes ☐ No ☐

6. Do you use the same password for all applications?

   Yes ☐ No ☐

7. Is it ever mandatory for you to change your password on the system?

Yes ☐ No ☐

8. Do you share your passwords with other colleagues?

   Always ☐ ☐ ☐ ☐ Never

9. Are you aware of other colleague's passwords?

   Yes ☐ No ☐

Log On

10. Does your device have a session logout time?

    Yes ☐ No ☐

11. If "Yes" – then does this interfere with your work

    Always ☐ ☐ ☐ ☐ Never

Comment:_____
_____
_____
_____

12. Do you ever allow any of your colleagues to enter patient data on the mobile device while you are personally logged on?

    Always ☐ ☐ ☐ ☐ Never

13. During rounds do you have to re-log on when entering a different area/ward?

    Yes ☐ No ☐

Security Issues

14. Are you aware of any security issues associated with wireless technologies?

    Yes ☐ No ☐

If "Yes" then:
Comment:_____
_____

_____
_____

15. Have you any security concerns using your wireless mobile device?

Yes ☐ No ☐

If "Yes" then:
Comment:_____
_____
_____
_____

16. Do you ever think that patient confidentiality is compromised by the use of wireless technology?

Yes ☐ No ☐

If "Yes" then:
Comment:_____
_____
_____
_____

17. Overall, how would you rate the level of wireless security at this location?

Excellent ☐ ☐ ☐ ☐ Poor

Comment:_____
_____
_____
_____

Thank you kindly for your time!

Appendix D. HIPAA Administrative Safeguards Section 164.308

ADMINISTRATIVE SAFEGUARDS

SECTION 164.308

As Contained in the HHS Final HIPAA Security Rules

HHS Security Regulations **Administrative Safeguards - § 164.308**

a. A covered entity must, in accordance with § 164.306:

1.

i. *Standard: Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.

ii. *Implementation specifications*:

A. *Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

B. *Risk management* (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

C. *Sanction policy* (Required). Apply appropriate sanctions against workforce members who fail to comply with the

security policies and procedures of the covered entity.

D. Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

2. *Standard: Assigned security responsibility*. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

3.

<>

i. *Standard: Workforce security*. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

ii. *Implementation specifications*:

A. *Authorization and/or supervision* (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information

or in locations where it might be accessed.

B. *Workforce clearance procedure* (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

C. *Termination procedures* (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

4.

i. *Standard: Information access management*. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

ii. *Implementation specifications*:

A. *Isolating health care clearinghouse functions* (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

B. *Access authorization* (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

C. *Access establishment and modification* (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

5.

i. *Standard: Security awareness and training*. Implement a security awareness and training program for all members of its workforce (including management).

ii. *Implementation specifications*. Implement:

A. *Security reminders* (Addressable). Periodic security updates.

B. *Protection from malicious software* (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

C. *Log-in monitoring* (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

D. *Password management* (Addressable). Procedures for creating, changing, and safeguarding passwords.

6.

i. *Standard: Security incident procedures*. Implement policies and procedures to address security incidents.

ii. *Implementation specification: Response and Reporting* (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

7.

i. *Standard: Contingency plan*. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

ii. *Implementation specifications*:

A. *Data backup plan* (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

B. *Disaster recovery plan* (Required). Establish (and implement as needed) procedures to restore any loss of data.

C. *Emergency mode operation plan* (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

D. *Testing and revision procedures* (Addressable). Implement procedures for periodic testing and revision of contingency plans.

E. *Applications and data criticality analysis* (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

8. *Standard: Evaluation*. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

b.

1. *Standard: Business associate contracts and other arrangements*. A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in

accordance with § 164.314(a) that the business associate will appropriately safeguard the information.

2. This standard does not apply with respect to--

    i. The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.

    ii. The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or

    iii. The transmission of electronic protected health information from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.

3. A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

4. *Implementation specifications: Written contract or other arrangement* (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

Appendix E. HIPAA Physical Safeguards Section 164.310

PHYSICAL SAFEGUARDS

SECTION 164.310

As Contained in the HHS Final HIPAA Security Rules

HHS Security Regulations

Physical Safeguards - § 164.310

A covered entity must, in accordance with § 164.306:

a.

1. *Standard: Facility access controls*. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

2. *Implementation specifications*:

   i. *Contingency operations* (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

   ii. Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

   iii. *Access control and validation procedures* (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor

control, and control of access to software programs for testing and revision.

iv. *Maintenance records* (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

b. *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

c. *Standard: Workstation security*. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

d.

1. *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

2. *Implementation specifications*:

i. *Disposal* (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

ii. *Media re-use* (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

iii. *Accountability* (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

iv. *Data backup and storage* (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Appendix F. HIPAA Technical Safeguards Section 164.312

TECHNICAL SAFEGUARDS

SECTION 164.312

As Contained in the HHS Final HIPAA Security Rules

HHS Security Regulations **Technical Safeguards - § 164.312**

A covered entity must, in accordance with § 164.306:

a.

1. *Standard: Access control*. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

2. *Implementation specifications*:

   i. *Unique user identification* (Required). Assign a unique name and/or number for identifying and tracking user identity.

   ii. *Emergency access procedure* (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

   iii. *Automatic logoff* (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

iv. *Encryption and decryption* (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

b. *Standard: Audit controls*. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

c.

1. *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

2. *Implementation specification: Mechanism to authenticate electronic protected health information* (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

d. *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

e.

1. *Standard: Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

2. *Implementation specifications*:

i. *Integrity controls* (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health

information is not improperly modified without detection until disposed of.

ii. *Encryption* (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Appendix G. HIPAA Organisational Requirements Section 164.314

ORGANIZATIONAL REQUIREMENTS

SECTION 164.314

As Contained in the HHS Final HIPAA Security Rules

HHS Security Regulations

Organizational Requirements - § 164.314

a.

1. *Standard: Business associate contracts or other arrangements*.

    1. The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.

    2. A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful.

        A. Terminated the contract or arrangement, if feasible; or

        B. If termination is not feasible, reported the problem to the Secretary.

2. *Implementation specifications*(Required).

    i. *Business associate contracts*. The contract between a covered entity and a business associate must provide that the business associate will--

        A. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

        B. Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

        C. Report to the covered entity any security incident of which it becomes aware;

        D. Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

    ii. *Other arrangements*.

        A. When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if--

1. It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or

2. Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.

B. If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(i) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained.

C. The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

b.

1. *Standard: Requirements for group health plans*. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

2. *Implementation specifications* (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to--

. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

i. Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

ii. Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

iii. Report to the group health plan any security incident of which it becomes aware.

Appendix H. HIPAA Policies and Procedures and Documentation Requirements Section 164.316

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

SECTION 164.316

As Contained in the HHS Final HIPAA Security Rules

HHS Security Regulations

Policies and Procedures and Documentation Requirements - § 164.316

A covered entity must, in accordance with § 164.306:

a. *Standard: Policies and procedures*. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

b.

1. *Standard: Documentation*.

i. Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

ii. If an action, activity or assessment is required by this subpart to be documented, maintain a

written (which may be electronic) record of the action, activity, or assessment.

2. *Implementation specifications*:

    i. *Time limit* (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

    ii. *Availability* (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

    iii. *Updates* (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.