How will the publics' use of the Internet including their experience of E-banking affect their perception of privacy and confidentiality of Electronic Health Records?

Diane Hanrahan

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

2008

Declaration

I declare that 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: _____

Diane Hanrahan

Date:_____

Permission to lend and/or copy

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

Signed: _____

Diane Hanrahan

Date:_____

Acknowledgements

The author acknowledges and wishes to thank the following people without whom this dissertation would not have been possible:

Lucy Hederman for her excellent supervision, guidance and advice.

Mary Sharp for her keen statistical guidance.

Prajesh Narendra Chhanabhai whose kind words and knowledge helped me to pursue this line of research. I would also like to acknowledge his generosity in the sharing of information.

The participants in the questionnaire, who gave their time enthusiastically.

Directors of Nursing Maura Pidgeon and Geraldine Clerkin for their encouragement over the past two years, which gave me the confidence to pursue this course of study

.

My employer, The Mater Private Hospital Dublin, for facilitating and allowing me the time to complete this study.

My work colleagues, for their help and support.

My dear friend Melissa Lanigan who never lost faith in me, listened to me at length and kept me on track. This dissertation would not have been submitted without her selfless help

And finally my husband Criostoir, my family and friends, for their good humour and patience while the office door was closed.

Abbreviations

CPR	Computerised Patient Record
EHCR	Electronic Health Care Record
EHR	Electronic Healthcare Record
EMR	Electronic Medical Record
EPR	Electronic Patient Record
FNC	Federal Network Council
HIQA	Health Information Quality Authority
HIT	Health Information Technology
ICT	Information and Communications Technology
ICRS	Integrated Care Record Service
IOM	Institute of Medicine
IWS	Internet World Stats
NJIR	National Joint Internet Research
OECD	Organisation for Economic Co-operation and Development
PHIPA	Personal Health Information Protection Act
PHR	Personal Health Record
PIPED	A Personal Information and Electronic Documents Act
TAM	Technology Acceptance Model
TRA	Theory of Reasoned Action

Summary

Healthcare professionals have a duty of care to maintain records in confidence (Department of Health and Children 2008). It is the principle of confidentiality that is the foundation of a trusting healthcare professional - patient relationship. According to the Institute of Medicine up to 98,000 people in the USA die every year from medical errors resulting from inaccurate or incomplete medical records (Kohn et al 1999). Still (2005) suggests that with the introduction of an Electronic Health Record (EHR) system, the number of medical errors could be reduced by up to 90%. However, researchers have reported that the public have great concerns in relation to the security abilities of such technology (Chhanabhai and Holt 2007).

The Internet in its original form was first developed in 1968 and its use has increased rapidly with usage as high as 73.6% in North America (IWS 2008). As a result of the advances made in ICT, and the Internet in particular, E-banking emerged allowing users to conduct their banking transactions online. Indeed this technology has been warmly accepted into Irish society despite the increased publicised incidences of fraudulent internet related activities (Corrigan 2006). Although the effect of fraudulent transaction is inconvenient, it is repairable with changes to account numbers and replacement of new cards solving the problem in many incidences. However, the effect of unauthorised access to personal health information is irreparable as this information is highly personal and lifelong.

The aim of this study was to determine if the publics' experience of the Internet and E-banking would effect their perception of privacy and confidentiality in relation to the EHR. A comparison was drawn from a study carried out in New Zealand in 2006 by Chhanabhai and Holt (2007) which examined the healthcare consumers concerns around the implementation of an EPR. An adapted version of their questionnaire was used on a convenient sample of N=100 people. The results were analysed using Excel and it was established that whilst there was a high level of computer usage among respondents, the use of E-banking had no affect on their perception of privacy and confidentiality in relation to EHR. A small number of respondents who did not use the internet were split evenly as to whether paper records were as secure as electronic records. This differed from the study population of 73% felt that EHR were more secure. There were many similarities between this study and the one conducted by Chhanabhai and Holt (2007). One notable difference though was in response to whether the EHR was more secure than paper records. Chhanabhai and Holt (2007) state that 55% believe that paper records were more secure, while the percentage was only 22% in this study. It is envisaged that this study will be reproduced on a larger scale in the near future with Mr. Prajesh Chhanabhai and Mr. Alec Holt who have expressed an interest in conducting further research together in relation to this topic.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.0 Background

"All that may come to my knowledge in the exercise of my profession or outside my profession or in daily commerce with men, which ought not be spread abroad, I will keep secret and will never reveal"
(Hippocratic Oath, circa 4th century BC)

Privacy and confidentiality go hand in hand when caring for patients' and when documenting this care; all healthcare professionals have a duty to maintain medical records in confidence (Department of Health and Children 2008). Indeed, the Irish Medical Council (2004 pp29) states that confidentiality is a 'time honoured principle of medical ethics....which extends after death and is fundamental to the doctor/patient relationship'. It is this principle that is the foundation of the trusting relationship that healthcare professionals build with their patients. However, if this trust is broken it can have lasting and devastating effects on the public's perception of the care that they have received, which is possibly why healthcare professionals are reluctant to embrace information and communication technology (ICT) (Abdolrasulnia 2008 and Economist 2005).

Davis (2001) recounts the following piece of commentary by Rhona McDonald who is the editorial registrar with British Medical Journal on the issue of privacy and EHR access:

> "Here is my dilemma. I want my notes to be strictly confidential but readily accessible to those who need them. Electronic notes, while potentially solving my second problem, sets alarm bells ringing with regard to the first. I am not a technophobe, but I am wary of giving out personal financial information over the Internet, and the thought of my entire medical history floating somewhere in cyberspace doesn't fill me with confidence. Perhaps I have seen too many films about ingenious hackers."

The question that arises is – if the above commentary was made by someone who

used the Internet and carried out E-transactions including E-Banking on a regular basis would they still have the same reservations?

1.1 Motivation

Health informatics has been defined as the application of ICT in healthcare (Trinity College Dublin 2008), however, in 2005 The National Consumer Health Privacy Survey established that 67% of respondents were "somewhat" or "very concerned" about the privacy of their personal health records should they be electronically stored. If such a high percentage of the general public are voicing concern in relation to the security abilities of this technology then it has to be questioned whether the electronic healthcare record (EHR) will ever be implemented successfully. Indeed, the implementation of an EHR may seem a distant aspiration in today's Irish health service but as is evident in the literature, it has proven to be the way forward (Still 2005).

Throughout the literature the words 'privacy and confidentiality' are used to describe the precautions to protect the patients' details in healthcare. Carter (2000) argues that in order to provide for successful EHR implementation, attention must be paid to the delivery of appropriate information that is useful to both the client and clinician while ensuring privacy protection and accountability. Ultimately, Carter (2000) is referring to the security of such information. Indeed, in the domain of ICT, the word 'security' replaces privacy and confidentiality but fundamentally throughout the literature they mean the same thing. The recording and storage of personal data for use by a third party has evidentially lead to similar concerns with regard to who will have the authority to access data that is pertinent to the client (Peleg et al 2007).

Electronic or E-banking was first implemented in Ireland in the late 1990s and its acceptance worldwide has occurred rapidly (Mori 2002). One of the major banking players reported having over half a million on-line customers in 2006 which was an increase of 88% in the previous four years (Kelly 2006). In fact, there are now banking institutions that only operate on-line services and the general public appear to

be embracing this new technology with little or no fear in relation to security issues. The question arises in relation to whether the public would be happy to accept the same safeguards for their health information as they do for their financial transactions?

Califf and Muhlbaier (2003) argue that the Internet and supporting information systems have revolutionized the non-medical world. They compared the ICT advancements of the banking industry versus that of the healthcare industry and conclude that the majority of banking institutions can provide bank account holders with the facility to withdraw funds or pay bills remotely via computer. They also highlight that making sensitive information about people's finances available is possible because of common language and standards adopted by the finance industry. In contrast, they argue, the medical community has not developed a standard language and is a mixture of paper and computer-based systems that do not allow the multipurpose use of data. This, they contend, leads to fragmentation with healthcare providers completing one set of forms for billing, another for clinical records, and yet a third for research purposes.

The planning and organisation that must take place prior to the implementation of an EHR is a lengthy and time consuming process (Ovretveit et al 2007). Although many countries are on this journey and much has been written on the processes that are underway. Amatayakul (1999) states, that the principle of consumer health informatics is that of 'empowering individuals' to play a greater role in their own healthcare and to be active participants in the decisions that affect their healthcare. This brings the EHR into a new light. It is not only the application of an ICT system that will assist healthcare practitioners but an integrated record that will empower the healthcare consumer/patient in decision making in relation to their own care and treatment. However, according to Hodge (2003) the public's cautiousness is related to misuse or wrongful disclosure of their sensitive health data. It has been suggested by many researchers that this may be due to their lack of expertise in ICT and online transactions (Mathematica 2007). This suggestion led to the motivation to investigate whether this was a valid assumption or not.

1.2 Research Question

The question this study aims to answer is 'How will the publics' use of the Internet including their experience of E-banking affect their perception of privacy and confidentiality of Electronic Health Records?' It is planned to ascertain the public's understanding and opinion of an EHR, to establish how accepting the concept would be and if this acceptance is related to their use of the Internet and of E-banking with a focus on privacy of data and security. It also aims to deduce how the general public perceive on-line security and privacy and establish if their beliefs will influence their acceptance of an EHR implementation.

1.3 Research Overview

A comparison will be drawn from a study carried out in 2006 in New Zealand that examined the healthcare consumer's security concerns around the implementation of an EHR. An adapted version of the questionnaire used in that study served as the research tool for this study. Following a critical review of the literature, the research question was formed and a convenience sample of N=100 people was approached and a structured interview was conducted. The results established that there was a high level of computer usage among the respondents, though there was a lower use of e-commerce and E-banking. Indeed, use of the Internet to purchase goods and E-banking was much higher in respondents under the age of 40. However the survey shows that there is a definite concern surrounding the privacy and confidentiality of healthcare records. This concern is related to perceived potential problems with EHR system security that have already affected other IT systems. It appears from this study that there would be a higher level of acceptance of this form of health record if appropriate safeguards were put in place to adequately protect it. It can be stated as a result of the outputs from this study that there was no definite co-relation between those respondents that use E-banking and the acceptant of the EHR, but with the limited number of respondents that did not use the internet there was less concern regarding privacy and confidentiality of their health records and 50% felt that paper based health records were more secure. This study was carried out at a time when almost daily media reports stated privacy and confidentiality breeches with IT

systems worldwide and it could be suggested that this had some influencing factor.

1.4 Outline of Dissertation

Chapter 2 provided a literature review, carried out from October 2007 to August 2008. The headings used were:

- Electronic Healthcare Records
    - Privacy and confidentiality in relation to EHR
    - Patient perceptions of EHR
    - Security in relation to EHR
    - Electronic Health Record and Consent
    - EHR Acceptance study: Mr. Prajesh Chhanabhai and Mr Alec Holt
- The Internet
    - Internet usage
- E-Banking
    - E-Banking and Security
    - E-Banking and user acceptance

Having completed a review of the literature, a research methodology is outlined and the research process is described in Chapter 3. An adapted questionnaire was used from a study carried out in New Zealand by Chhanabhai and Holt in 2007. The changes made were initially related to the location of the survey with question 3 being removed. Question 7 was added and 3 further questions were adapted following feedback from the pilot study. This questionnaire was carried out during a six week time period in June and July 2008. Participants were sought until 100 questionnaires were completed.

Chapter 4 detailed the results of this quantitative study, which were analysed using an Excel spreadsheet. A comparison was drawn with the study carried out by Chhanabhai and Holt as mentioned above.

Chapter 5 discusses the results from chapter 4 regarding the public's perception of

privacy and confidentiality of an EHR system related to their use of the Internet and E-banking. It outlines Ireland's readiness for EHR system.

Chapter 2
Literature Review

2.0 Literature search

Parahoo (1997) proposes that the purpose of a literature search is to put the current study into context of what is known already and is useful in identifying, refining and formulating the research question. In order to review the literature a search must first be carried out to locate and identify the most current and relevant material. The reviewer must also build on existing theory or research and the researcher should strive to understand what is already known about the topic. A thorough literature review provides a foundation on which to base a new knowledge and generally is conducted well before any data is collected (Polit, Beck and Hungler 2001). Therefore, the literature search began with a search of relevant databases. The Boolean operators AND, OR and NOT were used in association with key words as seen in the table below.

Table 1: Summary of Key Words

E-banking AND security
Electronic Healthcare Record AND Security
Electronic healthcare record AND E-banking
Access Electronic health records
Health Smart card
E-banking AND security OR confidentiality
EHR OR Electronic Health record AND confidentiality
E-banking AND implementation
E-banking OR on-line banking AND adoption of.

A search of publications and journals not available in the library databases was also performed. This literature search was repeated periodically to ensure that the most recent publications were not omitted. Many of research and opinion articles retrieved were not relevant and therefore were omitted from the literature review. Once the

article was deemed relevant it was critically reviewed as suggested by Parahoo (1997) and a total of 103 articles were included in the review and the findings documented under the relevant heading. These headings were developed as a result of the themes which emerged from the reviewed literature. They are:

- Electronic Healthcare Records
    - Privacy and confidentiality in relation to EHR
    - Patient perceptions of EHR
    - Security in relation to EHR
    - Electronic Health Record and Consent
    - EHR Acceptance Study: Mr Prajesh Chhanabhai and Mr Alec Holt
- The Internet
    - Internet usage
- E-Banking
    - E-Banking and Security
    - Security, Technologies and Risks
    - E-Banking and user acceptance

The literature review will begin by defining an EHR and establishing how an EHR has evolved.

2.1 Electronic Healthcare Record

According to the Institute of Medicine up to 98,000 people in the USA die every year from medical errors resulting from inaccurate or incomplete medical records (Kohn et al 1999). Still (2005) suggests that a viable solution is the introduction of a correctly monitored EHR system with more consumer interaction and the number of medical errors could be reduced by up to 90%. There are many definitions in the literature of what this EHR is, some more informative and holistic in respect of patient autonomy than others. Neame (1996) defines the EHR as a confidential record that is maintained by a healthcare professional or an organization, containing the patient's personal and demographic details, a summary of the patient's medical history and documentation of each event, including symptoms, diagnosis, treatment and clinical outcome with relevant documents and correspondence also included. Whilst this definition appears

to include all relevant data that a healthcare professional would seek, it omits the concept of patient ownership. Pyper et al (2004) argues that an EHR is a longitudinal record of the patient's healthcare that the patient, in addition to healthcare professionals, has access too. According to Alvarez (2006) an EHR is a secure and private lifetime record of an individual's health and care history, available electronically to authorized health care providers, which facilitates the sharing of data across the continuum of care, across healthcare delivery organisations and across geographies. The Irish Standards Authority (ISO 2004) defines an EHR as:

> "A repository of information regarding the health of a subject of care, in computer readable form, stored and transmitted securely, and accessible by multiple users. Its primary purpose is the support of continuing, efficient and quality integrated health care and it contains information which is retrospective, concurrent and prospective"

For the purpose of this research, the above definition will be adopted.

Whilst there are many phrases used throughout the literature to describe medical records which are recorded electronically, Wietz et al, (2003) in an effort to distinguish and clarify what is an EHR is, as opposed to a patient record, states that an EHR is information stored electronically about an individual's 'lifetime health care and status'. The authors argue the importance of a clear distinction being established between the EPR and EHR and suggest that an EPR refers to those records that are kept and owned by a medical institution, or a department or speciality within an institution. The EHR, however, refers to a record that is kept outside an institution and would be a central repository for all health data specific to that person.

Hayrinen, Saranto and Nykanen (2007) in an attempt to define what an EHR is used for examined the differing type available. The table below is extracted from their findings.

Table 2: Types of EHR (Adapted from: Hayrinen, Saranto and Nykanen 2007).

Type of EHR (ISO)	Definition
Electronic medical record (EMR)	Generally focused on medical care
Departmental EMR	Contains information entered by a single hospital department
	Picture archiving and communication system (PACS)
	Anaesthesia records
	Intensive care records
	Ambulatory records
	Emergency department systems
	Pathology laboratory system
	Oncology records
	Cardiology records
	Operation theatre records
	Gynaecology records
	Internal medicine records
	Pharmacy systems
	Geriatric centre records
	Diabetes clinic records
	Radiology reporting system
Inter-departmental EMR	Contains information from two or more hospital departments
	Obstetric records for inpatient and outpatient clinics
	Prescribing system
Hospital EMR	Contains all or most of patient's clinical information from a particular hospital
Inter-hospital EMR	Contains patient's medical information from two or more hospitals
Electronic patient record (EPR)	Contains all or most of patient's clinical information from a particular hospital
Computerized patient record (CPR)	Contains all or most of patient's clinical information from a particular hospital
Electronic health care record (EHCR)	Contains all patient health information
Personal health record	Controlled by the patient and contains information at least partly entered by the patient
Computerized medical record	Created by image scanning of a paper-based health record
Digital medical record	A web-based record maintained by a health care provider
Clinical data repository	An operational data store that holds and manages clinical data collected from health service providers
Electronic client record	Scope is defined by health care professionals other than physicians, e.g. physiotherapists
Virtual EHR	No authoritative definition
Population health record	Contains aggregated and usually de-identified data

Following a comprehensive review they described an EHR as a document primarily used for the purposes of setting objectives and planning patient care, documenting the delivery of that care and assessing the outcomes. It includes information regarding patient needs during episodes of care provided by different health care professionals

Some researchers would suggest that paper based healthcare records are fragmented and facilitate clinician recording information that is specific to their needs and not documenting the 'full picture' (Chhanabhai, Holt and Hunter 2006). Flanagan (2006) concurs and argues that although paper records can be easily browsed, and are directly accessible, portable and self-contained, they are also seen as cumbersome, lacking in structure, fragile and degradable, illegible, incomplete, inaccurate and can only be accessed by one person at any given time. A comparison of paper and electronic records is documented in table 2 below which highlights the positive aspects of an EHR; indeed, the literature is abundant with positive studies which support the argument for the implementation of an EHR.

Table 3: Functional Comparison between the Paper-Based Record and the Electronic Version (Adapted from: Chhanabhai, Holt and Hunter 2006).

Function	Paper-Based Record	Electronic Record
Availability	One location	Multiple locations
Cost	Approximately $500 per lifetime	Tiny individual cost
Security	Low	High
Consumer control	Little to none	Can be high
Data	Difficult to extract	Should be easy to extract
Durability	Low	High
Duplication of records	Yes	No
Duplication of tests	Yes	Rare
Audit trail	No	Yes
Practitioner "freedom"	Good	Restricted
Patient interaction	None	Full

The Institute of Medicine (IOM) in 1991 completed an 18 month study based on improving patient records in response to increasing technological advances. A challenge faced by the committee was to provide a thorough yet concise description of what patient records should be. The future patient record envisioned by the IOM committee is not simply a digitalised version of the current paper record; rather, it provides broader functions to practitioners, is used actively by practitioners in the delivery of care, and serves as a resource in the evaluation and management of patient care. The Committee concluded what they refer to as a Computer Patient Record (CPR) is an essential technology for health care for three reasons. Firstly, the uses and demands of patient data are increasing. Secondly, the increasing complexity of treatment, the growing numbers of elderly patients with chronic illnesses, and a continually mobile population are generating more data to be tracked with greater difficulty in tracking them. Thirdly, achieving the goals of improving the quality and managing the costs of health care requires improved information management capabilities. The Institute developed a very specific definition of what a CPR is and the data it should contain. CPRs should contain a problem list, health status and functional level, and clinician rationale for patient care decisions. They should be able to be linked with other clinical records to provide a longitudinal patient record. CPR systems must protect patient confidentiality. They must provide convenient access to authorised users at all times, support direct data entry by practitioners, and allow custom-tailored views of the data. CPR systems should be able to be linked to knowledge, literature and bibliographic databases. They must be flexible and expandable to support evolving needs of users. Such CPRs will assist the process of clinical problem solving and enable practitioners and institutions to evaluate and manage the quality and cost of care (Hyrinen 2007).

The Department of Health and Children published a strategy document on Health Information in 2004. This document was developed to support the principles' set out in the Brennan and Prospectus reports, by ensuring that health information becomes more readily available and appropriately used throughout the health service. The principles of this report are:

- The safeguard, privacy and confidentiality of personal health information
- Ensuring that health information systems are efficient and effective

- Health information should be used to its optimum
- Health information should be of a high quality.

The strategies outlines within this document aspire to:

- Establish a legislative and information governance framework
- Adopt an integrated and national approach
- Establish processes and structures that ensure the fuller use of health information
- Improve access to health information
- Establish health information standards
- Exploit enabling technologies.

This document also details that the establishment of the Health Information and Quality Authority (HIQA) will facilitate the implementation of an EHR ensuring adherence to quality standards. This implementation would be legislatively assisted by the Health Information Bill. The strategy document details the prospective EHR development in Ireland, it is clear that the perceived benefit of this ICT is a focus for HIQA as stated that its primary function is safer, higher quality and more patient centred healthcare across traditional healthcare boundaries. Architectural models for an EHR are still being developed, but it is recognised that a common national approach is required (Health information: A national strategy 2004).

Waegemann (2002) examined a survey carried out by the Medical Records Institute in the USA and it concluded that the benefits of an EHR were better quality of care, more cost effective care, better access to care, the ability to share information, improved workflow, and a reduction in medical errors. Whilst there is plenty of positive literature supporting the implementation of EHRs', the main concern of the general public when surveyed is the aspect of privacy and confidentiality (Anderson 2006).

2.1.1 Privacy and Confidentiality in relation to the EHR

Privacy and confidentiality have been at the cornerstone of the patient - clinician relationship since ancient times, with patients' entrusting their most private and intimate details to their health care professionals (Flanagan 2006). With the emergence of ICT systems, governments and other organisations have implemented guidelines and legislation in an effort to address the issues of privacy and confidentiality in the information age.

Neame (1996) documents that a Code of Practice was developed under the New Zealand Privacy Act covering the sharing of health information to ensure that the sharing of confidential data was supported. For large organisations such as hospitals to function efficiently, they need the flexibility to be able to assign user privileges to selected staff with a unique user identifier to facilitate the audit trail of the individual undertaking each transaction.

The right to privacy within the medical field has traditionally involved the elements of consent and confidentiality. Weitz et al (2003) defines privacy as the right of patients' to decide for themselves the time, circumstances and extent to which their attitudes, beliefs, behaviours or opinions are shared with or withheld from others. Although Wilson (1998) refines this definition when discussing privacy and confidentiality in relation to the EHR;

> "its the right to control the circulation of personal information about oneself, freedom from unreasonable interference in one's private life and the right to the protection of personal data against misuse or unjustified publication."

In Ontario, Canada The Personal Health Information Protection Act, 2004 (PHIPA), governs health care information privacy and they concur with the above definition describing privacy as the client's right to control how his/her personal health information is collected used and disclosed. PHIPA sets consistent rules for the management of personal health information and outlines the client's rights regarding his/her personal health information. This legislation accounts for a client's right to privacy with the needs of the healthcare providers to access and share health information. The sharing of personal health information is allowed among health care

team members to facilitate efficient and effective care. Health care teams include all those providing care to the client, regardless if they are employed by the same organization. PHIPA requires that personal health information be kept confidential and secure.

In 1989 Annas established that patients' are not likely to disclose any intimate details freely unless they are certain that no one else, not directly involved in their care, will learn of them. Indeed, two decades on, the public's concerns in relation to the EHR and security maintenance still exists. According to Chhanabhai, Holt and Hunter (2006) the security of health records primarily encompasses the principles of privacy and confidentiality. The Irish Medical Council (2004 pp16) states that medical records should be stored in such a manner that 'ensures confidentiality, security and ready accessibility for clinical staff when required for patient management.' The Data Protection Agency argues that privacy and confidentiality of patient records forms part of the ancient Hippocratic Oath and are core principles in the treatment of patients in healthcare (Data Protection Agency 2008). Indeed, it is the Data Protection Agency that addresses the issue of security and maintaining privacy and confidentiality of medical records. It also dictates rights of patients and medical staff in relation to personal information and imposes obligations on data controllers. These rights apply to information held both electronically and in a manual form and whilst it is clear that the onus of responsibility is on the holder of this data to keep it 'safe and secure', there are no guidelines or minimal requirements as to how to do so. Some researchers would argue that it is because of this lack of direction from such organizations in relation to the security of medical records that patient's perceptions are so negative in relation to the EHR (Chhanabhai, Holt and Hunter 2006).

Whilst it is clear from the literature that the implementation of the EHR will pose many challenges, particularly in the area of privacy and confidentiality, researchers argue that it is important that the patients' trust is both attained and maintained in order to ensure its success (Flanagan 2006). However, prior to attaining their trust it is necessary to ascertain how they perceive the EHR and the issues surrounding it.

2.1.2 Patients Perceptions of EHR

Mathematica is an American company which conduct research to support decisions in relation to social policy problems. Mathematica (2007) refers to the EHR as a personal health record (PHR) and define it as an electronic record of an individual's health information that the individual owns and manages in a secure environment and would argue that this PHR has the potential to improve health care quality and access to care. Mathematica (2008) even suggest that EHRs' may also empower consumers and help them take a more active role in their health care by allowing them to access and coordinate health information and share it with those who need it. Mathematica has addressed the following questions by conducting focus groups in federally designated medically underserved areas in New Jersey.

- How do members of underserved populations view the concept of PHRs?
- What are the potential barriers to adopting PHRs among underserved populations?
- What factors must be considered in designing PHRs for underserved populations?

In a paper released as a result of the above study Bagchi (2007) established that nearly all participants mistrusted the security of electronic records systems. They recognized that many health care providers already use electronic clinical health records and believed their personal physicians would keep their health information private, but they had less trust in the integrity of electronic health records maintained by other providers or other entities (for example, insurance companies and employers). Most respondents believed that information contained on a personal computer could be easily accessed and compromised. The participants agreed that a "smart card," a personal credit card-type device that would be carried by the health consumer, could provide secure access to essential personal health information in the event of the owner's incapacity. It was assumed that the health information contained on the card could be read only with a scanner available to health personnel. There was a consensus of trust associated with this device. The study showed that participants wanted to be able to limit access to their health records to designated healthcare providers and other relevant interested parties. They also wanted a facility to limit what type of access each provider gained access to.

The issues highlighted from the study are:

- The digital divide in the undeserved remains a formidable barrier to the adoption of electronic PHR systems.
- PHR developers and implementers' need to overcome consumer mistrust with an educational strategy before PHRs will be widely accepted.
- Privacy standards that can allay consumers concerns regarding access to their PHRs.

Li and Poovendran (2005) define a smart card as a credit-card size device with a microprocessor and memory embedded. It can securely store a key that is not extractable from the card, or can be revealed only when a correct personal identification number (PIN) is entered. Favier (2007) concurs with this definition in his examination of the health smart card and his findings suggest that the use of which is growing, driven by the need to provide secure identification and authentication of patients in order to provide the relevant secured services. He further argues that they improve the security and privacy of patients' information, reduce the risk of healthcare fraud and support the concept of portable medical records. An article written in Card Technology today (2004) detailed the launch of the Medicare smart card in Tasmania, Australia which allowed clients to have access to a variety of healthcare information, such as organ donation request and childhood immunisation records. It operated in conjunction with 'Health Connect', an electronic patient record system that gives authorised health professionals access to information about procedures, treatments and tests. The Australian Medical Association strongly opposed this implementation stating fears for the privacy and confidentiality of their patients data due to the under development of the system. Indeed, the Australians are not alone; in 2004 a national consumer health privacy survey carried out by the California Healthcare Foundation published in November 2005 indicated that 67% of participants surveyed were concerned about the privacy and security of their health information stored electronically. This same survey indicated that 13% of consumers admitted that they practiced medical hiding behaviour, a custom that is detrimental to the healthcare plan of the patient (Bishop et al 2005).

Doty (2008) examined the information discussed at the Health Information and Management Systems Society convention which took place in the USA in Feb 2008.

Interoperability was high on the agenda and emerged as not the issue it was anticipated to be, as open platforms between Google and Microsoft seemed to be the choice. Interoperability raises the issue of how these solutions will ensure that healthcare consumer's information remains private and secure.

> "the question remains will consumers trust the major search engine with their personal health information? The healthcare community will ultimately benefit from the integration standards, portability and accessibility of electronic health records"

Holmes and Hanson (2007) examined market research carried out in the USA concerning what motivated the public to share their medical records. 47% of the respondents stated that they would be willing to share their medical information for lower insurance premiums. 27% stated they would be willing to share if it resulted in better coordination across organisation of medical care/treatment. Consumers lack trust in health privacy laws and their general level of trust in their health plan provider was directly associated with their willingness to share their medical health record.

2.1.3 Security in Relation to the EHR

Boehm (2007) highlights privacy and security fears as the top reason for USA health plans members not taking advantage of the EHR. Members were concerned regarding how and by whom their personal health data will be accessed and used. Half of those surveyed by Forrester Research Inc. stated that sharing of sensitive personal health on the web was too risky. One third of non-users felt that the promises of privacy and confidentiality of their health records were not enough. Concerns regarding site security prevented some members accessing their private data.

Care delivery organisations have an ethical and regulatory responsibility to ensure the privacy and security of their patients' health records. This security requires a coherent and comprehensive strategy that is supported by a framework of appropriate policies and standards. This strategy should identify what must be protected and what threats could occur and ensure that privacy, security and compliance policies and technical controls align with perceived threats (Hieb and Runyon 2008).

In a letter written in 2007 to the Senate Committee on Health, Education, Labour and Pensions in the United States of America, Janlori Goldman, Director of the Health Privacy Project states that privacy is one of the most important elements of any health information technology initiative. In order to establish a more trustworthy privacy-protection environment, the establishment of a policy framework for the development and adoption of a nationwide interoperable health information technology infrastructure is essential. Goldman (2007) goes on to state that studies have documented that the public believes that a computer-based medical records system is less secure than a paper-based one. Numerous unauthorised access of digital health records in the USA have added to consumer anxiety about electronic health information. Indeed the Health Information: A National Strategy (2004) concurs with this stating that sharing of health information enforces ethical and legal obligations on the health professional. It is incumbent on the governing bodies that an information governance framework is put in place. It was proposed in 2004 in this strategy document that a Health Information Bill would be enacted to provide safeguards to ensure protection and appropriate use of health information. In June of this year The Minister for the Department of Health and Children announced a public consultation exercise. One of the purposes of the bill is stated as: Facilitating the greater use of information technology for better use of patient services (Department of Health and Children 2008). A discussion paper on the proposed health information bill issued by the Department of Health and Children in June 2008 states that modern technology has for the most part simply brought the issues of privacy, confidentiality and consent of personal health information into sharper focus.

2.1.4 Electronic Healthcare Record and Consent

In a clinical environment, treatment of a patient often involves a team of medical personnel, such as a primary clinician, specialist clinician, nurses and allied health professionals. In such a group environment, it is a challenge to ensure only the valid medical personnel have access to the patient's EHR, so that patient's privacy is guaranteed, while the records have authorised consent to be retrieved to provide best possible treatment for the patient. Consent may be categorised as explicit when it is clearly and unmistakably stated. While this type consent for all healthcare purposes

would resolve doubt about the use of electronic health information it may become difficult to implement due to the weight of bureaucracy involved and the difficulty in reaching the entire population. Consent may also be described as implicit where consent can be validly inferred. Implicit consent covers the sharing of health information among the primary, secondary and tertiary health care teams. It would not cover the distribution of information for teaching or third party research (Department of Health and Children 2008). Mandl (2001) asks should the onus be on the patient to consent to who can access their EHR or should the primary physician have that responsibility? This question has proved troublesome and consensus would indicate that a combination of both would prove the most advantageous (Ray 2006).

The Health Service Executive (2006) details in an article written as a user handbook for staff in Cork University Hospital that to give valid consent there must be adequate intellectual and mental capacity. Consent must be given voluntarily and with all knowledge presented. Though this maybe written with a focus on patient – physician interaction the same should apply for consent to view or add to ones EHR. Indeed Watson and Halamke (2006) argue that most people agree that patient centred care requires comprehensive information to be available wherever and whenever care is provided. There is less agreement, however, on how patients should consent to use of electronic records and how the data can be kept secure (Gostin 1997). The NHS are examining two broad models regarding patient consent to use and sharing of their electronic records. The first is the "opt-out" model, which was championed by Watson in particular. This is where the public are informed of the NHS care records service and are offered the facility to indicate that they do not wish their electronic records to be shared. The second model is for no sharing to occur until people have expressed their wish to share their clinical records within the NHS, i.e. "opting in". In Scotland the "opt-out" approach was adopted and the general public were informed using an extensive publicity campaign in February 2006 there were 3.3 million records with sharing facilities and 22 records opted out (Watson and Halamke 2006).

Following on from this the health service in Alberta, Canada, changed from the 'opt-in' position to an 'opt-out' one in 2003. The decision was made after consultation with patients and clinicians. The opposing side of the model is the "opt-in" option which is the approach that Halamka recommends and this has been implemented in

Massachusetts over a two year period up to 2006. The policy has enabled the education of patients regarding the risks and benefits of data sharing and creates a sound foundation for trust. This trust, Halamka reasons, is a prerequisite to successful implementation of the technology and it is argued that the clinically relevant information has been disclosed with the patient's consent (Watson and Halamke 2006). There were no figures to reflect this how many patients had decided to "opt-in". Whatever a patient chooses to do, whether it is 'opt-out' or 'opt-in', these options would not be possible today without the development of the Internet and its ability to allow us to instantly access and multiply share information.

2.1.5 EHR Acceptance study: Mr. Prajesh Chhanabhai and Mr Alex Holt

Chhanabhai and Holt (2007) reviewed the literature in relation to how privacy has emerged as the main concern that health consumers have with any records system. They detail a speech delivered by Givens (1996) to a conference in San Diego titled 'Towards an Electronic Patient Record' they discussed a Louis Harris Poll from 1995 found that 100% of Americans who were surveyed saw the benefits of having their health records computerized. However, 82% expressed concern about the negative effects of a computer-based system. Their concerns were based on the following points:

- Information gathering concepts;
- Loss of control regarding the use of their personal information;
- Lack of awareness of the controls and protections that are in statute regarding the protection of privacy.
- Fear of inadequate implementation of systems
- Risk of error due to carelessness, and poor judgment by those who may handle their personal information.

In a further more recent study referenced by Chhanabhai and Holt (2007), the public expressed concerns stemming from their previous experiences with computerised systems. Westin (2005) examined the Harris Interactive survey and found that 48% of adults in the USA claimed that the benefits of an EHR would outweigh any risks to

privacy. However almost 70% of these surveyed was concerned regarding the robustness of data security safeguards. Their concerns included:

- Sharing of medical information without the consumer's knowledge;
- An increase in medical errors rather than a decrease with the use of computers;
- Reduction of any existing privacy rules;
- Consumers not revealing all necessary information to their healthcare provider due to the fear of having their details being made available electronically

It was the above literature that formed the basis for the research conducted by Chhanabhai and Holt (2007). They formulated a questionnaire by adapting questions from 3 studies; Westin (2005) who examined the American publics' attitudes towards EHR, the NHS (2003) who also conducted a review of the general public's views on EHR's and Pyper et al (2004) who studied patients' experiences when accessing their on-line electronic patient records in primary care. They placed the questionnaires in GP surgeries in three cities in New Zealand. The results from Chhanabhai and Holts' (2007) research are summarised as follows:

- A total of 300 surveys were completed and returned (a 75% response rate),
- One hundred eighty-eight (62.6%) had not heard of EHRs
- Those who had heard of them indicated that they were a positive innovation in the health sector
- 202 (73.3%) participants were highly concerned about the security and privacy of their health records
- Participants were worried about hackers (79.4%), vendor access (72.7%), and malicious software (68%)
- 80% of participants believed that security systems would make EHR systems more secure
- Those who buy items over the Internet were less apprehensive about security concerns.

The findings showed that for an EHR to be fully embraced in the health service, 2 main issues need to be addressed:

- EHR security systems have to be of the highest level, with constant monitoring and updates.
- The involvement of the 'health consumer' in the ownership and maintenance of their EHR should be a priority. The aim of an EHR in the collection of information from 'cradle to the grave' must involve the subject of the record to ensure that completeness occurs.

Chhanabhai and Holt (2007) conclude that from the results of the study the consumer is ready to accept the transition, as long as one can be assured of the security of the system and involvement in decision making.

2.2 The Internet

Leiner (1999) describes the Internet as a world-wide broadcasting tool, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location.
On October 24, 1995, the Federal Networking Council (FNC) unanimously passed a resolution defining the term Internet. The FNC agrees that the following language reflects the definition of the term 'Internet' and it refers to the global information system that:

Table 4: Internet Definition (Leiner et al 2003)

Internet Definition	
1	Is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons.
2	Is able to support communication using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extension follow-ons and/or other IP compatible protocols.
3	Provides, uses or makes assessable, either publically or privately, high level services layered on the communications and related infrastructure described herein.

The figure below details the brief history and the rapid growth of the Internet, so facilitating the development of on-line communication and transactions.

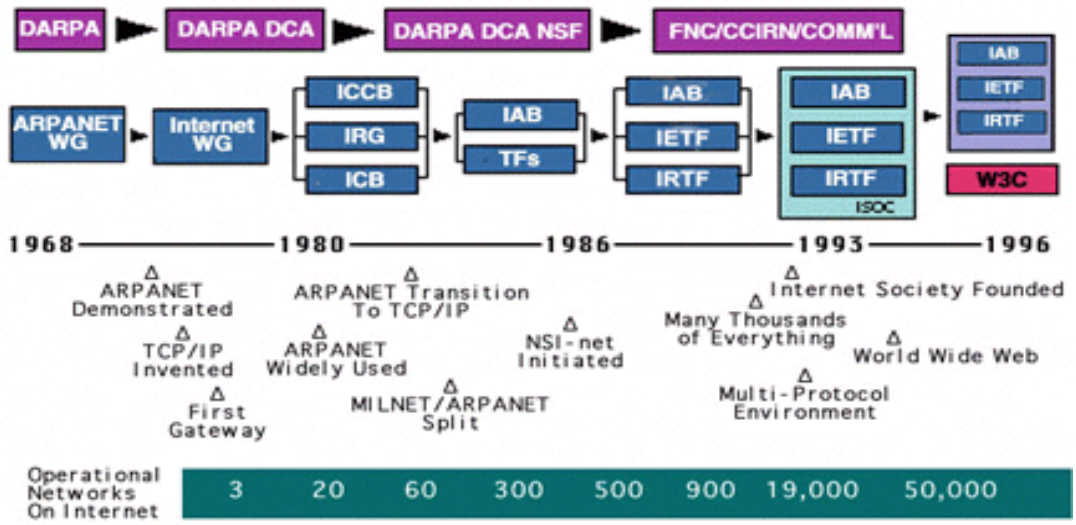

Figure 1: **Internet Timeline** (Slater 2002)

The Internet had been used to augment, or even supplant, product and service delivery processes considered as more traditional (Vainio 2006). Wikipedia describes today's Internet as a global system of interconnecting computer networks that exchange data by packet switching using the standardised Internet protocol. It is also described as a network of networks that contains millions of private and public networks that are linked by fibre-optic wireless and copper wire connections.

2.2.1 Internet Usage

Internet usage in Ireland was examined in a report issued in April 2008 as a result of a statistical analysis carried out by the National Joint Internet Research between July and December of 2007. This report started that 69% of 19-24 year olds, 61% of 25-34 year olds and 56% of 35-44 year olds had connected to the Internet in that time. The gender spilt showed equal amounts of male and female responders and equal male versus female Internet users. Analysis of social class was quite remarkable with a

variation of 65% between the lowest and highest stated social class with the higher social class being the more frequent user. In Ireland, Dublin showed the highest usage percentage, 16% higher than non Leinster counties. All respondents who attended third level education stated they had used the Internet. Interestingly, participants that were born outside Ireland had a 15% higher usage than those born in Ireland. Internet usage worldwide in 2008 according to Internet World Stats (2008) is 21.9%. With 73.6% usage in North America dropping to 5.3% population penetration in the African continent, although this statistic is low, the increase rate since 2000 is over 1000%. Whilst usage of the Internet is growing rapidly, Buddle (2008) issues a note of caution stating that though the Internet is growing at a good rate this rate is not the same throughout the world. He argues that this is due to a deficit of broadband penetration and persistently high connection cost and concludes that until these issues are addressed Internet growth will not increase.

2.3 E- Banking

Banking is not any different from other business areas, as banking in general is an extremely information-intensive industry. As a result the advances made in ICT, and the Internet in particular, have a central role in today's banking and how consumers conduct their financial transactions. Robertson (2004) declares that in the financial industry, the Internet has had a profound impact by providing the most efficient, cost effective method of gaining new customers, servicing existing customers, and also providing increasing financial services. In the USA in 2004, more than 33 million households used online banking, and e-commerce accounted for almost 10% of all credit card purchases.

Hanrahan (1999) defines on-line banking as the ability for customers to avail of banking services through the Internet, including account opening and day to day operation of those accounts, without the need for interaction or intervention of the bank branch. The Federal Financial Institutions Examination Council (FFIEC) (2001) concurs with this definition and suggests that online or E-banking is the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels.

The concept of online banking or more commonly known as E-banking dates back to the early 1980s, when the prototypes were developed (Bainbridge 2006). It took until October 1995 for the Presidential Savings Bank in the USA to announce the facility for regular consumer use. The other major banking institutions quickly followed suit with Chase Manhattan and Security First Network Bank being at the forefront. Today, there are a number of banks operated solely via the Internet and have no 'four-walls' entity at all, for example Rabo Bank in Ireland. The developers of online banking had predicted that it would be only a matter of time before online banking completely replaced the in-branch conventional kind. Bainbridge (2006) argues that this prediction has proved a somewhat over optimistic assessment - many traditional customers still harbour an inherent distrust in the process. Others have opted not to use many of the offered facilities because of either personal or reported experiences with online fraud, others still prefer the face to face banking transactions and for some this reluctance is their lack of computer expertise.

Despite the reservations of some it is estimated that a total of 55 million families in the USA will be active users of online banking by the year 2010 (Bainbridge 2006). There are few banks now that do not offer this facility to customers and the number of E-banking customers has been increasing at an exponential rate. Initially, the main attraction was the 24 hour facility, the ability to instigate immediate transactions and also the elimination of tiresome bureaucratic red tape and paperwork involved in regular banking. The speed with which this process happens online, as well as the other services possible by these means, has translated into a literal boom in the banking industry over the last five years. Nor are there any signs of the boom letting up - in historical terms, online banking has just begun. A study carried out by Daniel (1999) found that 25% of banks in the United Kingdom and Ireland had already implemented an on-line transaction facility offering customers the service in their homes. A further 50% were at that time in the development and testing phase.

In today's international market a study carried out in April of 2008 by ComScore stated that Canada ranked number one in adoption of online banking, with 67.1 of Canadian Internet users banking online. Other English-speaking countries had significantly lower penetration, including the U.K. (49.5 percent), U.S. (44.4 percent),

and Australia (41.7 percent) (Bernie 2008). At the time of this dissertation going to publication, there were no reliable figures available in relation to online or E-banking and its usage solely in Ireland. The world of commerce has become multifaceted with the emphasis on time saving and immediacy. Some customers are reluctant to wait in line at their local bank to carry out transactions that may not be processed until close of business. The emergence of the Internet has revolutionized the way in which business is carried out and nowhere more evident than in modern banking procedures, and online banking being one of the greatest advances.

With E-banking, a customer can perform almost every kind of bank transaction and service via the Internet. This means that complex transactions can occur almost immediately and can be executed by the customer without ever leaving their home or office. E-banking overcomes a number of physical limitations that were previously part of the banking process. For instance, a customer with E-banking privileges can access and transact an account even past normal banking hours. E-banking operates separately from regular banking services and is available 24 hours a day, 7 days a week.

This service is highly personalized offering the customer the ultimate in convenience and security. A bank offering this service must use a secure website that has controls preventing access or misuse without proper authorization. The customer uses a username and password as well as various other customized safety parameters to access and use the account (I-onlinebaking 2008).

Whilst it is recognised that the development of the Internet has been a portal for e-transactions and so E-banking, it is not all positive. There are security issues to be considered and as a result the privacy and confidentiality of users in relation to their finances and the risks surrounding them also need to be discussed.

2.3.1 E-banking and Security

Security refers to the processes and tools that ensure confidentiality of information (Weitz et al 2003). According to Moutaz (2005) there are two main issues affecting security in Internet financial transactions:

- Preserving the confidentiality and integrity of online financial transactions
- Limiting disclosure of personal financial records to third parties.

Financial institutions are constantly searching for more effective identification methods, however, some of the more advanced identification technologies have proved financially unresourcable and not user friendly. According to Aburrous (2008) security has been widely recognized as one of the main obstacles to the adoption of Internet banking and is considered an important aspect in the debate over challenges facing Internet banking. With the expansion of on-line fraud techniques, more protective identification methods must be used. Financial institutions generally employ robust internal security measures but it is the consumer login site that provides the challenge. These institutions at present have no control or autonomy over the degree of protection employed by each user.

Corrigan (2006) states that security issues are stalling the uptake of Internet banking. Indeed, a survey of the Irish market, carried out in 2006 by Behaviour and Attitudes for international IT consultancy CA, found that of the 1.4 million Irish adults who use the Internet, almost 10 per cent (125,000 people) claim that they do not carry out transactions online due to worries over identity theft. To add to these consumers worries, in April of 2008 a media report detailed the theft of four laptops from a major Irish banking organisation containing customers' names and addresses, medical backgrounds, life assurance details and bank account details. The number of customers affected by these thefts initially was estimated at 10,000 this was later revised upwards to over 31,000. The customer's details were stored unencrypted though lesser forms of security were used such as password protection (Kennedy 2008). Also in September 2007 a laptop containing the unencrypted social security number of 800,000 job applicants was stolen in the USA. Goodin (2007) also details in The Register on-line magazine of data breaches that had resulted from criminals who found ways to exploit weaknesses in corporate networks. One on-line broker institution stated that hackers had infiltrated a database containing social security numbers, birth dates and account numbers on an undisclosed number of clients. Computer forensic experts also discovered a Trojan that had stolen more than 1.3 million records from people who were looking for work through a recruitment agency in the USA.

Kornokov (2006) details the growth in theft of personal financial data, this theft is netting thieves large rewards as their technological methods become more sophisticated. In 2005 a major credit card company suffered a data theft due to breeches by a third-party processor, in which cybercriminals extracted 40 million personal records. An estimated 13.9 million credit cards were involved in that incident. However, major advancements in the area of security in ICT have been made, some of which will be discussed below.

2.3.2 Security Technologies and Risks

The technologies that exist to maintain privacy and confidentiality of information will now be discussed as will the ever evolving applications that exist which attempt to override them.

2.3.2.1 Information Encryption

Encryption is a method for communicating securely over insecure communications channels, such as the Internet, by encoding messages so that they can be read only by parties having the proper key or decoder (Raysman and Brown 1998). Technological encryption is practice of data coding in order maintain security. This was historically used in manual form prior to the digital age and was employed by government and military agencies. Most technological encryption systems belong in one of two categories:

- Symmetric Key Encryption which uses an algorithm that uses trivially related, often identical cryptographic keys for both decryption and encryption
- Public Key encryption is when the key used to encrypt a message differs from the key used to decrypt. In public key encryption, a user has a public and a private key. The private key is secret while the public key may be widely distributed.(Wikipedia)

2.3.2.2 Anti-Virus

The installation of antivirus and antispyware programmes go along way to protect the user from malicious software downloads. A study carried out by America Online and The National Cyber Security Alliance (2005) found that 67% of those surveyed had no antivirus protection or had not recently updated their protection. However, even with these protections in place innovative criminals find ways through.

2.3.3.3 User Log on

Authentication is the validation of someone or something. With the rise of on-line fraud as a result of the anonymous nature of the Internet it is essential to provide robust verification and authentication techniques prior to allowing access to system and transactions (Tubin 2005). Username and login identification methods have been the standard. The risk associated with this is the banking institution put the onus on the user not to divulge these identifiers. Tubin (2005) states that divulgence to immediate family member has proved costly as this group have been identified as the most likely perpetrators of account theft crime.

2.3.2.4 Firewall

A Firewall is a system designed to prevent unauthorised access to or from a private network. It can be implemented in both hardware and software. All messages entering or leaving the network pass through the firewall. These messages are examined and those messages that do not meet the specified criteria are blocked. A firewall is considered a first line defence in protecting private information.
A study carried out by AOL and The National Cyber Security Alliance in 2005 stated that 44% of home computers lacked correctly configured firewalls.

2.3.2.5 Malware

The converse side of the protection systems that are detailed above is Malware.
The Linux information project (2006) refined its definition of Malware as any software that is developed for the purpose of doing harm to computers or via computers. Malware can be classified in many ways, on the basis of how it is spread, how it is executed and or what it does. Below is detailed the differing types of malware.

2.3.2.5.1 Phishing

On-line fraud has evolved to now involve the technique of phishing. Typically phishing involves the manipulation of its targets to divulge their access identification. With this information customer accounts are skimmed and identities are abused. On-line fraud has evolved further with user unwittingly downloading malware on to their computers. This computer code is developed to enable the collection of user information for malicious purposes and can be used for identity theft (Rogers 2006).

Freid (2002) defines phishing as the act of sending to a user an e-mail falsely claiming to be an established legitimate enterprise in an attempt to trick the users into surrendering personal or private information. The e-mail typically directs the user to visit a website where the user is asked to update personal information such as passwords, credit card, social security and bank account numbers that the legitimate organisation already has. The website is bogus and set up only to illicit the users information. Rogers (2006) describes phishing attacks as using both social engineering and technical subterfuge to steal consumers' personal identity data and financial account details. Social engineering schemes use false e-mails to lead consumers to spurious websites designed to trick recipients into divulging financial data. By hijacking brand names of banks phishers reassure recipients regarding legitimacy. Technical subterfuge plants crime ware into the recipients PC to steal credentials directly. Software is now available which provides investigative techniques and critical analysis of Internet fraud. Figure 2 graphically shows an increase of 62% in Internet fraud related to phishing between 2003 and 2006.

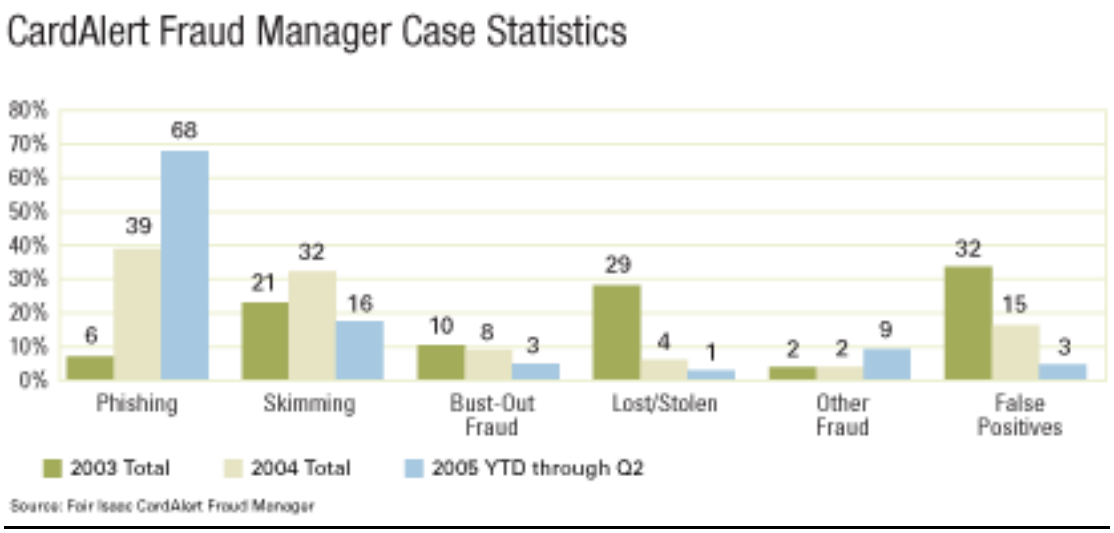

Figure 2: On-line Fraud Statistic from 2003-2005 (Fair Isaac Inc. 2005)

In 2006 a poll was carried out by a security specialist company SophosLabs and it was established that a high frequency of phishing e-mails often purport to come from financial organisations and banks, 20% of business claimed to receive more than five phishing e-mails per day. An example received by the author of this dissertation has been included in Appendix 1. Indeed many organisations that are targeted are now sending out warnings to both their customers and the perpetrators of this phishing that they are aware of incidents as detailed in Appendix 2.

2.3.2.5.2 Other Malware

Tipton and Krause (2004) argue that malware which affects users' abilities to use computers safely is being developed at an alarming rate. They suggest that this malware is becoming more and more effective in dealing with existing security abilities. They discuss some of the common malware that users have reported encountering;

- **E-Mail Attachment:** The client opens an e-mail attachment that may contain various types of malware. When this attachment is opened, the payload is

installed. This malware may also be hidden in a macro in a spreadsheet or document that executes when the file is opened.

- **Pop-Up Downloads**: While users are visiting a web site a pop-up window appears offering a seemingly useful service or offer. Once the user clicks into the window malware is downloaded.
- **Drive-By Downloads**: When the user enters a website clicks on a navigation link or reads a HTML e-mail message malware is automatically downloaded. This attack vector can install malware with no indication that it has occurred.
- **Hacking:** Software specialists that have extensive knowledge of the Internet gain access to systems. The Hacker can take over a computer completely.
- **Trojan Horse:** This type of programme gains entry under disguise. The programme comes disguised as something that the user intends to download
- **Cross-Site Scripting:** A legitimate vulnerable website is targeted, the perpetrators own code is entered which amalgamates with the web sites original content. Consumers login credentials are stolen though legitimate looking forms.

In 2005 a Gartner research study on the effect of phishing and online attacks on Consumer Confidence stated that in the 12 months ending May 2005 that 73 million adults in the USA who use the Internet said they received or think that they received an average of 50 phishing e-mails in the previous year. This is a growth of 28% in one year. The study reports that nearly 2.5 million US adults have reported losing money due to online attacks. Indeed, 25% of those surveyed stated that on-line attacks have influenced their online activities. It may be that as a result of these incidents and experiences by Internet users that privacy and confidentiality concerns exist in this group in relation to the EHR.

2.3.3 E-banking User Acceptance

E-banking has become an everyday activity in many households despite the concerns discussed above (Robertson 2004). The use of E-banking is increasing rapidly (Bainbridge 2006). Moutaz (2005) conducted a study of E-banking security

perceptions and customer satisfaction issues. He surveyed 100 people and established there was a correlation between respondent's attitudes towards E-banking and their comfort level in relation to security with regard to their age level of education and annual salary.

In contrast, Taft (2007) found that user acceptance hinged on four premises:

- Training received
- Programme efficacy
- Perceived ease of use
- Locus of control

Taft went on to determine if age, gender, race and income affected user acceptance and her findings indicated that none of the variables did.

Wang, Wang and Tang (2006) using the technology acceptance model (TAM) (figure 3) as a theoretical framework, introduced "perceived credibility" as a factor that reflects the user's security and privacy concerns in the acceptance of Internet banking. It also examines the effect of computer self-efficacy on the intention to use Internet banking.

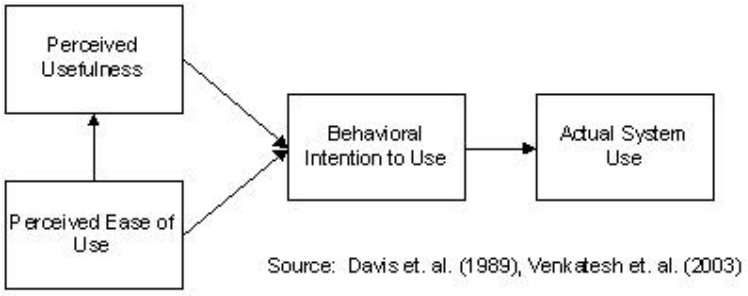

Figure 3: TAM Model

The model is adapted from Theory of Reasoned Action (TRA), which was originally proposed by Fishbein and Ajzen in 1975. TAM is an information system theory, which is used simply to predict and explain the user acceptance of information technology. The model addresses the reasons why users either accept or reject particular piece of information technology. (Vainio 2006)

The table below shows E-banking usage/acceptance in Ireland associated with age during its inception period, this table in direct conflict to the argument made by Taft (2007).

Table 5: Age groups of Internet Banking Customers Source: Hanrahan (1999)

Age Group	Number of Customers
10-18	0%
19-25	17%
26-35	48%
36-45	21%
46-55	9%
56-65	3%
66 +	1%
Unknown	1%

In Singapore, ease of use is high on the agenda when users were asked about their acceptance of E-banking (Sohail and Shanmugham 2003). In addition, Internet accessibility, awareness, trust and security concerns, convenience and attitude towards change were identified as main factors that affect the adoption of Internet bank services in Malaysia (Sohail and Shanmugham, 2003). It appears that worldwide user acceptance is influenced by the how accessible and easy to use the system is and if the users perceive the security to be of a high enough standard to ensure their personal information is protected.

2.4 Conclusion from Literature Review

Parahoo (1997) proposes that the purpose of a literature search is to put the current study into context of what is known already about the subject. It is clear from the literature search and review that EHRs will benefit both the users of the EHR and the recipients of care (Still 2005). However, a potential barrier to the EHRs

implementation is patient fears in relation to the privacy and confidentiality of their health record and the security that an electronic version can provide (Annas 1989 and Giverns 1996). The literature shows that Ireland is at a conceptual stage of EHR development. The Department of Health and Children issued a strategy document in 2004 and is presently at the public consultation stage of the health information bill. They will provide the framework for the eventual EHR development and implementation. The coordination of this is placed in the hands of HIQA who have a budget for 2008 of almost €1 million assigned to health technology.

It is over a decade since Irish banking institutions embraced E-banking and the literature highlights that there are similar issues which exist in relation to security and E-banking despite these issues some 60% of people are conducting some of their banking business online (Corrigan 2006). Unfortunately, leakage of electronic personal information has made headlines in Irish newspapers on a weekly basis lately, despite the advancements made in security technologies. However, these technological advancements are rendered useless if correct procedures are not in place to protect this sensitive information (Aburrous 2008). Regardless of these very public security breeches, the general public are still using this service on a daily basis. It therefore has to be asked if the general publics use of the Internet including their experience of E-banking affect their perception of privacy and confidentiality of EHRs. This question was addressed below using an adapted version of Chhanabhai and Holt's (2007) questionnaire.

Chapter 3
Research

3.0 Introduction

"The Purpose of all research is to solve a problem"

LoBiondo-Wood and Harper (2002)

Parahoo (1997) describes research methodology as a plan that illustrates how, when and where data are to be collected and analysed. It is comprised of the following elements: The approach, data collection method, time, place and source of data and the method of data analysis, all of which will be used as a framework to document the following piece of research. Firstly, as recommended by Cormack (1991) the approach must be decided upon to ensure that the aims of the study are met with the correct research design.

3.1 The Approach

The methodological approach is often determined by a number of philosophical and ideological orientations in addition to the practical issues that need to be considered in relation to research to design (Tarlings and Crofts 2002). In the area of health research -with its strong tradition of biomedical research using quantitative strategies, qualitative research is often criticised for lacking scientific rigour (Cormack 1991). Commonly heard criticisms are, that qualitative research is anecdotal, personal and can be strongly subject to researcher bias; secondly, it is argued that qualitative research lacks reproducibility (May and Pope 1995). Parahoo (1997) describes qualitative research as being subjective due to the researcher's interactive stance in order to get close to what participants think and experience, whereas the objective nature of quantitative research proves an advantage for uniformity and consistency.

Whilst there is criticism for qualitative approaches, there is also some for the quantitative approach with Cormack (1991) suggesting that the detached approach that this method facilitates allows the participants to be treated as though they are objects.

However, McSherry et al (2006) argues that a quantitative research method enables a structured approach to data collection enabling the use of differing size sample groups and thus enhancing the generalisability of the findings. The objectivity of quantitative methods means that the researcher stands outside the phenomenon in order to study it. Data collection and analysis are expected to be free from bias.

The table below details a comparison between quantitative and qualitative research.

Table 6: Qualitative and quantitative research attributes (Gordon and Langmaid 1988)

Qualitative	Quantitative
Open-ended, dynamic, flexible	Statistical and numerical measurement
Depth of understanding	Sub-group sampling, or comparisons
Taps consumer creativity	Survey can be repeated in the future
Penetrates rationalised or superficial responses	Taps individual responses
Richer sources of ideas for marketing and creative teams	Less on research executive skills or orientation

The research method used by Chhanabhai and Holt (2007) in the questionnaire that is to be used in this research in an adapted form, is quantitative, with two questions that provide a facility for comment by the respondents.

3.2 Research Design

In a quantitative study the research design spells out the strategies the researcher plans to adopt and to develop information that is accurate and interpretable. The process of research design is to provide a framework for answering the research questions (LoBiondo-Wood and Harper 2002).

The research documented in this dissertation is an adapted version of a study conducted by Chhanabhai and Holt (2007) in New Zealand. This study used a quantitative, cross-sectional research method and the author conducted the same method for this research. With this in mind the author plans to adopt the same

research process and design. The research process followed is outlined below.

Table 7: The Research Process

Phase	Activity
Step 1	Literature review
Step 2	Research hypotheses - identification of core areas for analysis
Step 3	Selection of general public and individual interviews
Step 4	Collation and analysis of information from interviews
Step 5	Conclusions from research from interviews
Step 6	An assessment of the general publics' current usage of E-banking and perception of security risks associated with it.
Step 7	The Publics understanding of an EHR and perceived risk association
Step 8	Comparison of results from this study with the New Zealand study.

It was at step 1 that Chhanabhai and Holt's (2007) study was found on PubMed's database and it was decided to reproduce the same research in Ireland. Prajesh Channabhai's e-mail address was available on the article and the author was contacted with details of the plan to replicate the study in Ireland. Mr Chhanabhai replied and was very eager for the study to be reproduced with an aim to draw comparisons for future publication (Appendix 3). This study was adapted for the Irish setting as detailed below.

3.3 Research Tool

Chhanabhai and Holt(2007) formulated the questionnaire by adapting questions from 3 studies; Westin (2005) who examined the American publics' attitudes towards EHR, the NHS (2003) who also conducted a review of the general public's views on EHR's and Pyper et al (2004) who studied patients' experiences when accessing their on-line electronic patient records in primary care. As this questionnaire (Appendix 4) was used in New Zealand it needed to be adapted to an Irish setting and as a result the following questions were changed:

- Questions 3 ‘At the time of filling out this questionnaire what part of New Zealand were you in? Auckland, Christchurch, Wellington, Dunedin’ was removed as the original questionnaire was completed remotely and the location was pertinent
- Question 7 was added asking respondents’ to complete 'I use E-banking'
- Question 9 ‘Giving those who treat you access to your medical records to make decisions about your treatment’ was changed from ‘medical records’ to ‘health records’. Resulting from feedback from the pilot study.
- Question 10 ‘Are you concerned about the privacy and confidentiality of your medical record’ was changed from ‘medical records’ to ‘health records’. Resulting from feedback from the pilot study.
- Question 11 was changed from “Do you know about the National Health Index” to “Do you know about the Health Information National Strategy”.

3.4 Ethical Considerations

When humans are used as study participants, care must be exercised to ensure that rights of those humans are protected (Polit, Beck and Hungler 2001). One of the most fundamental ethical principles in research is that of beneficence; to do no harm. The research should benefit the participants or at least put the participant at minimal risk. These researchers define ‘minimal risk’ as no greater than those ordinarily encountered in daily life or during routine physical or psychological tests or procedures. There was no risk to any participant taking part in this study and this study aimed to benefit the general public as it provides information on protection required for information technology systems.

The right to respect was also taken into account which includes the right to self-determination and full disclosure. The right to self-determination refers to the right of all participants to decide to participate or not to participate in the study (Polit and Beck 2004). All participants’ in this study were approached and the author introduced herself, asked for a few minutes of their time and informed of the nature and purpose of the study. The participant then decided whether to participate or not. The principle

for respect for human dignity refers to the full disclosure of all information to the participant and his/her right not to participate and/or to withdraw at any time from the interview. All participants were informed that they could withdraw at anytime during the brief interview. No participants chose to end the interview prematurely.

The principle of Justice refers to the participants' right to fair treatment and the right to privacy (Polit and Beck 2004). Participants were treated fairly at all time during the research process as participants' were selected in a fair and non-discriminatory manner and those who chose not to partake, had their decision respected by the author. According to Polit and Beck (2004 pp149) participants have the right to expect that all data they provide will be kept in the 'strictest confidence'. The questionnaires were marked 1-100, there was no identifiable material such as name, address, or date of birth etc recorded and therefore anonymity was assured. The questionnaires were photocopied and a copy was kept in a locked desk in a locked room in the author's home. The second copy was kept in a locked filing cabinet in a locked office at author's workplace.

The final area of ethics that Polit and Beck (2004 pp151) refer too is consent. They suggest that the following information should be given to all participants

- Participant status – participants should understand that the information they provide will be used for research purposes. All participants were informed of this during the recruitment process.
- Study goals – participants should be informed of the overall goals of the research in a language that they understand. Participants in this study were informed that the aim of this research was to identify if their experience of the Internet and E-banking transactions affected their perception of privacy and confidentiality of EHR's. None of the participants required further clarification.
- Type of data and Procedures – participants should be informed of the type of data to be obtained and how it will be collected. Participants in this study were informed that 100 questionnaires were to be completed and the information gathered would be analysed and documented. This would form part of a dissertation in submitted to the University of Dublin, in partial fulfilment of

the requirements of the degree of Master of Sciences in Health Informatics.

- Nature of the commitment and potential risks – participants should be informed of the time commitment and any foreseeable risks. The participants in this study were informed that this questionnaire would take a maximum of 10-15 minutes and there were no foreseeable risk associated with participating.
- Sponsorship and potential benefits – participants should be informed of funding from third parties and also if the research is part of an academic requirement. All participants were informed as documented above. This was the only way in which the author benefited from this research.
- Confidentiality – participants should be guaranteed confidentiality and anonymity if possible. Participants in this study were guaranteed both as documented above.
- Voluntary Consent – researchers should inform all potential participants that participation is strictly voluntary and failure to do so will not result in any loss of benefit or any penalty for them. This was made clear to all participants at the time of recruitment.
- Right to withdraw and withhold information – participants should be informed that even after consenting to participate they have the right to withdraw and also to withhold any piece of specific information.

Polit and Beck (2004 pp151) suggest that if all of the above has been 'communicated to the participants' then informed consent has been obtained. Whilst informed consent is normally documented (Cormack 1991), in this study, a consent form will not be collected to maintain anonymity. Verbal consent will be obtained and implied consent will be assumed on completion of the questionnaire by the participant.

3.5 Pilot Study

A pilot study is defined as a small sample group that acts as a prelude to a larger scale study. It has similar methods and procedures that yield preliminary data in order to determine the feasibility of the "parent study" (Jaireth, Hogerney and Parsons 2000).

Its purpose is not so much to test the research hypotheses, but rather to test the protocol, data collection instrument and sample recruitment strategy (Polit, Beck and Hungler 2001). A pilot study was conducted with 10 participants; 5 from the authors' work place and 5 friends with the adapted questionnaire. Some confusion was reported by the author's friends when answering question 10 'are you concerned about the privacy and confidentiality of your medical records?' as part of question 9 refers to 'health records'. Whilst the author's colleagues had no issues with the terms, it was felt members of the general public may also be confused and the term 'medical records' was changed to health records for clarity in the main study.

It was noted that there was a reluctance to voice their comments when asked. With this in mind it was decided that the questionnaires would be filled out by the participant but questions would be asked by the surveyor. This proved fruitful as many interesting comments were entered. It was suggested by one participant that the issue of confidentiality be reinforced on approaching subjects to participate. This suggestion was taken on board and all respondents were assured of the anonymity of the survey prior to agreement to participate.

3.6 Sample Selection

Studies involving humans involve two sets of people; those who do the research and those who provide the information. In a quantitative study the people who are being studied are referred to as subjects or study participants (Polit, Beck and Hungler 2001). LoBiondo-Wood and Harper (2003) describe the sample selection as the process of selecting a representative unit of a population for study in a research investigation. When sampling is correctly utilised the researcher can make inferences and generalisations about the designated population without the necessity to examine it in its entirety. For the purpose of this research the author plans to utilise the Non probability sampling process and within that process a convenient sample of the general public will be the objects of the study. The sample selection will involve approaching 100 members of the general public with an adapted version of Chhanabhai and Holt questionnaire. This will differ from the research carried out by Chhanabhai and Holt (2007) who gathered information from the patients or

relatives/friends of patients attending GP's. Chhanabhai and Holt (2007) participants had an average age of 35, this would not be the same in Irish GP surgeries and therefore, difficult to replicate. It also thought that approaching friends or relatives of those attending GP's would be as reliable as approaching members of the general public. It is for these reasons that the author did not specifically approach participants currently receiving, or companions of those receiving GP care.

3.7 Sample Size and Recruitment Procedure

Chhanabhai and Holt (2007) left 400 questionnaires (Appendix 2) in GP's surgeries' with 300 of them being returned completed. The sample size was reduced to 100 as the author approached the participants and completed the questionnaire with them as opposed to leaving the questionnaires to be completed by participants and therefore practical constraints such as time and resources limited sample size. In addition, the author also could not find any documented evidence for such a large sample size.

Recruiting the subjects began by identifying participants and gaining their cooperation once deemed eligible to participate. Polit, Beck and Hungler (2001) suggest that face to face recruitment is more effective than solicitation by telephone, letter or Email. The exclusion criteria for sample selection were that they had to be over 18years of age and have the ability to speak English and be currently residing in Ireland. Prospective participants were approached in a courteous manner as suggested by Polit, Beck and Hungler (2001) and were informed of the purpose of the questionnaire and how confidentiality would be maintained. The author repeated the same dialogue on each encounter which was.

- Introduction by Name
- Request for some of their time
- Consent obtained for their time
- The questionnaire purpose was explained
- The anonymous nature of the questionnaire was stated
- Consent obtained to complete the questionnaire
- Questionnaire completed

- Participant was thanked

The prospective participants were approached in a number of random locations in the north side of Dublin as it was felt that this would be representative of Ireland's population. As stated by Cowan (1997) a non probability convenient sampling technique is simply based on the availability of subjects. Selection is non-random and lacks a systematic approach. It is difficult to generalise the findings with this type of approach but the author felt that in an effort to attempt replication the study carried out in New Zealand this would be the better option. Participants were continually approached until 100 subjects were reached. The analysis and results will be discussed in the next chapter.

Chapter 4
Analysis of Results

4.0 Introduction

The answer to research questions is obtained through an analysis of the collected data (Polit and Beck 2004). These results need to be evaluated and interpreted in order to add to what is known of the existing body of knowledge in relation to the chosen research question (Cormack 1991). The research was carried out over a six week period between June and mid July. 143 people stopped when they were approached in total, 17 did not speak English, 3 were on holiday and were not currently residing in Ireland and 23 could not participate due to time constraints. As stated above this questionnaire was adapted from a questionnaire used by Chhanabhai and Holt in 2007 in a study titled: 'Consumers Are Ready to Accept the Transition to Online and Electronic Records If They Can Be Assured of the Security Measures'.

The questionnaire contained 16 questions of which some had multiple parts. There were 4 sections in the questionnaire:

- About You
- Your Computer Use
- Electronic Health Records
- Security and Your Records

Participants were surveyed on their computer use in relation to the Internet, e-commerce and E-banking transaction use, also knowledge of EHR systems and awareness of security, privacy and confidentiality issues within the information technology sector. The survey also questioned the publics perception of their health record security whether it is stored in a paper or electronic version. The aim of this was to examine the publics' perception of the Internet and on-line transactions with a focus on privacy of data and security and to deduce how their perceptions of on-line security and privacy will influence their acceptance of EHR implementation.

The survey was concluded when 100 questionnaires were completed. The returned data was entered onto a excel spreadsheet. Filters were used and customised to obtain

the required data. The data will be presented in sequence with the questions asked. As the questionnaire was adapted from a previous study carried out by Chhanabhai and Holt in New Zealand in 2007 a comparison will also be drawn.

4.1 Summarised Outputs from Questionnaire

As stated above the questionnaire was divided into 4 sections which will be dealt with separately below.

4.1.1 About You

The 'about you' section had two questions in the adapted survey.

The first question referred to the respondent's age, with 24% (24) of respondents between 30-39 years old which was marginally the highest group. Over 50% were under the age of 40. There were no respondents over the age of 80. The mean age was established at 41 years of age.

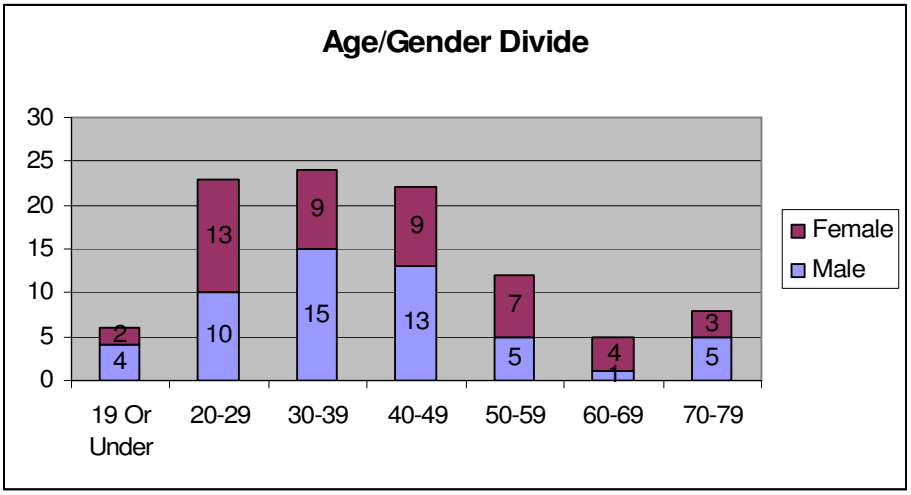

Figure 4: Age/Gender divide

The gender section was divided almost equally and within that divide the age ratio was somewhat differing with twice as many males in the 19 and under age group responding than female, 50% more 20-29 and 30-39 respondents were male. Only 1 60-69 member of the public was male with 4 being female, yet almost double the

amount of male 70-79 were questioned in comparison to female.(Figure 4)

4.1.2 Your Computer Use section

Research carried out by Forrester Research inc. for Microsoft in 2004 detailing the factors that influence usage showed that the average computer usage by the general public between the ages of 20 -64 years was 82.9%. From figure 6 below it is apparent that the percentage has remained unchanged with 83% of the respondents using a computer "regularly" or "fairly regularly". Indeed a colossal 94% of respondents have used a computer at some time in their lives. Internet usage almost reflected the same figure as computer usage as seen in figures 6 and 7 indicating that when respondents use a computer it would involve the use of the Internet.

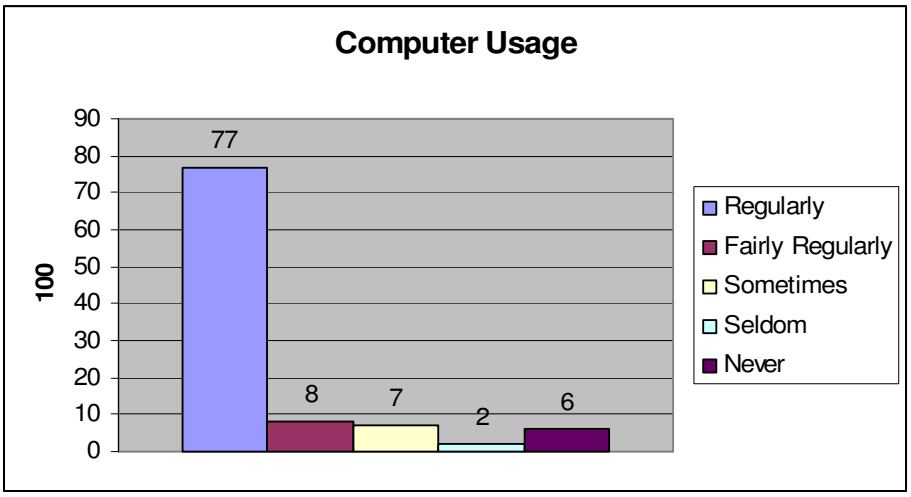

Figure 6: Computer Usage

79% of those asked stated that they used e-mail regularly or fairly regularly 31 were female and 44 were male, with the vast majority (75) of those 79 stating that they used E-banking regularly. Of the public who answered negatively (21) 90% were female and 10% were male. Indeed only two of these had ever used the Internet and this was categorised as "seldom" of which none utilised E-banking.

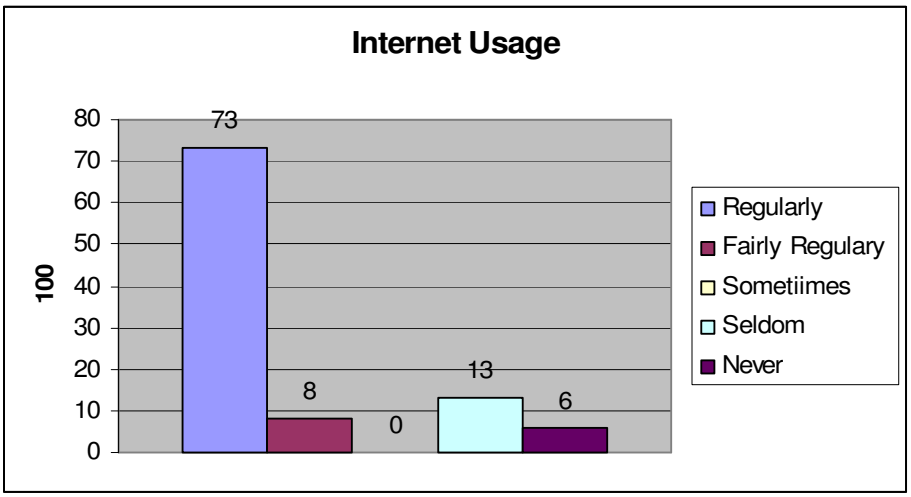

Figure 7: Internet usage

When looking at the usage of the Internet in more detail, it can be seen that 100% of the 40 and under age group questioned used the Internet regularly or fairly regularly as seen in figure 8. Examining the data from the older age groups it shows that only 28% used the Internet regularly or fairly regularly and 19% seldom or never used the Internet.

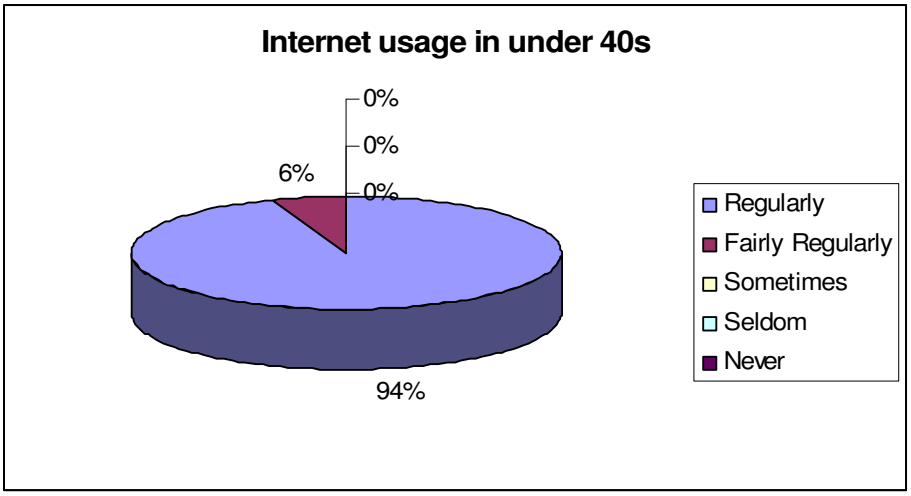

Figure 8: Internet Usage in Under 40s

There appears to be a connection between reluctance to use the Internet to purchase item and the use of E-banking with 23% and 28% either seldom or never using the Internet for these facilities. In contrast there appears to be more acceptance of E-

banking use with 60% using E-banking regularly or fairly regularly and only 53% happy to purchase on the Internet in the same categories. As demonstrated in figures 9 and 10. The highest percentage of 36% who used E-banking were in the 20-29 age group, but the usage in this study has increased in the 30-49 age groups by over 10% when compared to figures from Hanrahan (1999). These results back up the findings by Hanrahan (1999) that age is an affecting factor in contrast to the study carried out by Taft (2007) where age was not found to be an influential factor in E-banking acceptance.

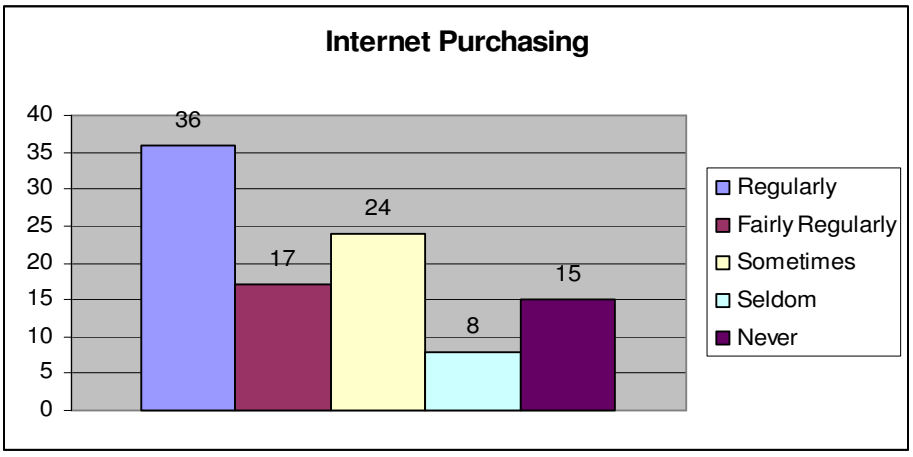

Figure 9: Internet Purchasing

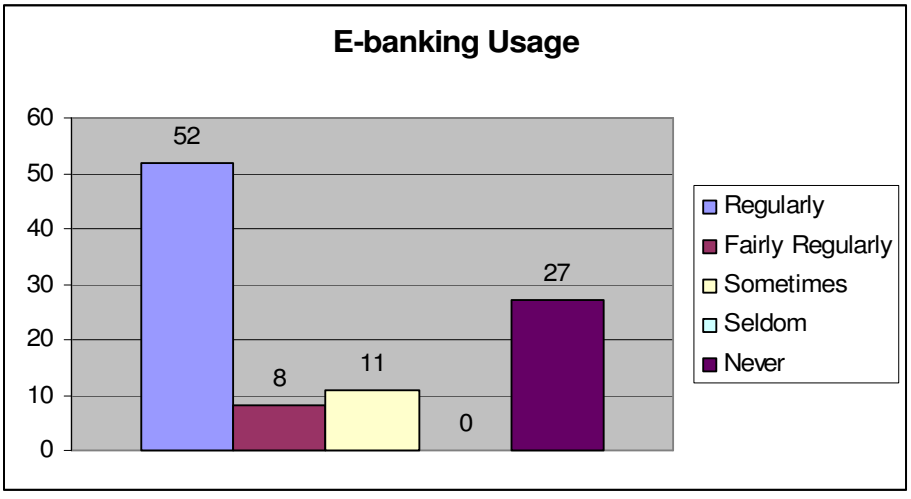

Figure 10: E-banking Usage

4.1.3 Electronic Health Records

Only one third of those surveyed had any knowledge of the concept of an Electronic Health Record as detailed in figure 11. Though when described most had a positive opinion. Question 9 follows on to ask how the respondents would feel regarding specific elements of choice that a proposed EHR would bring. This question elicited strong reactions from some. When asked about the proposed benefit of acquiring access to their record in order to make decisions on their care 87% agreed or strongly agreed that this would be a positive gain from an EHR but of the 8% who disagreed, their personal reactions were strong. One respondent stated "It's not my responsibility to make decisions about my health – that's a Doctors job". A further 8% also did not wish to have the facility to look up medical history. The reaction to this question was more moderate indicating a preference to a "read only" facility where healthcare choices were the responsibility of the physician. This is indicated in the 96% of respondents who felt that 24 hour access to the health record would be positive only 4% remaining neutral, none of these were in the 50 and older age groups.

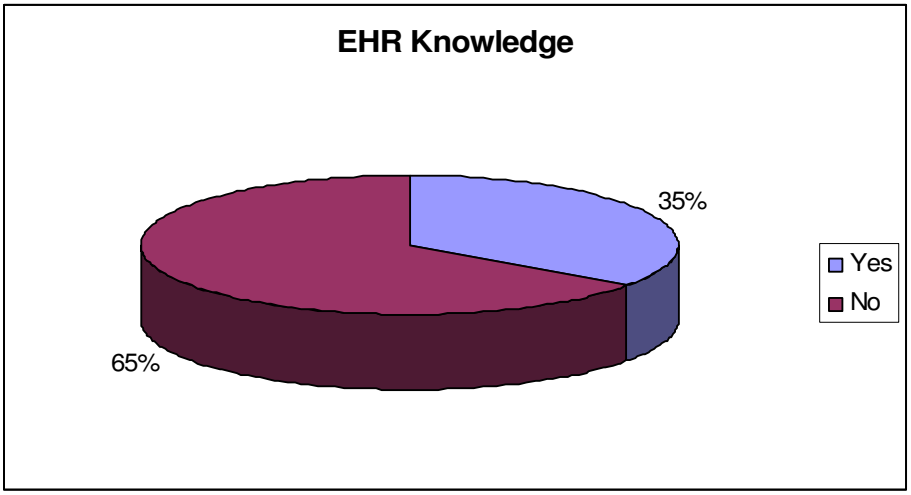

Figure 11: EHR Knowledge

81% of the public were in favour of accessing their current drug prescriptions, though it should be noted that 17% were neutral on this which was a higher response than many of the questions. This is surprising as most pharmacies are required to record patient medications as part of the drug payment scheme, which works on an

individualised card system. There were three questions asking the respondents about their opinion on quicker access, viewing and the loss of test results. The results were almost identical with a positive response of between 89% and 92%.

When questioned regarding the ability to give access to see their health records 90% felt this was a positive facility, 8% were neutral with no correlation with age observed. 19 people did not feel positively when asked about making their medical appointments on line which corresponded with the amount of respondents that did not use e-mail. One positive respondent stated "I spend half my day queuing to get an appointment and the other half queuing to be seen. If I could cut one of them out it would be great". The ability to record one's wishes on the system was overwhelmingly positive with only 4 % disagreeing.

4.1.4 Security and your record

The question asked at the beginning of this section of the questionnaire was about the publics concern regarding privacy and confidentiality of their Health Records. In this study 62% of respondents were concerned with a further 20% being unsure figure 12. These figures are comparative with the US where 67% of patients stated privacy concerns (National Consumer Health Privacy Survey 2005). However Flanagan (2006) conducted a study examining confidentiality, privacy and data protection of an EHR and found that 79% of patients surveyed were 'concerned' or 'somewhat concerned'. It appears that the general public are concerned about security issues, this study did not categorise the level of concern. There was a definite correlation between the age of the respondents and their concerns regarding privacy and confidentiality of an EHR with those under 40 years of age being less concerned that those over 40 years of age.

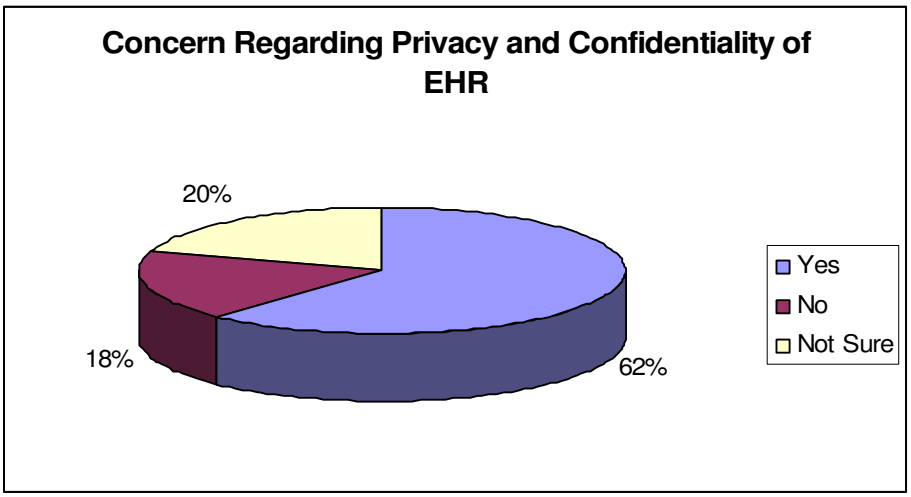

Figure 12: Concern Regarding Privacy and Confidentiality of EHR

Looking into the figures in more detail it can be seen that in the under 40 age group there was marginally less concern but more were unsure regarding the question and in converse the over 40 age group had a 20% swing to being more concerned and less unsure (figure 13).

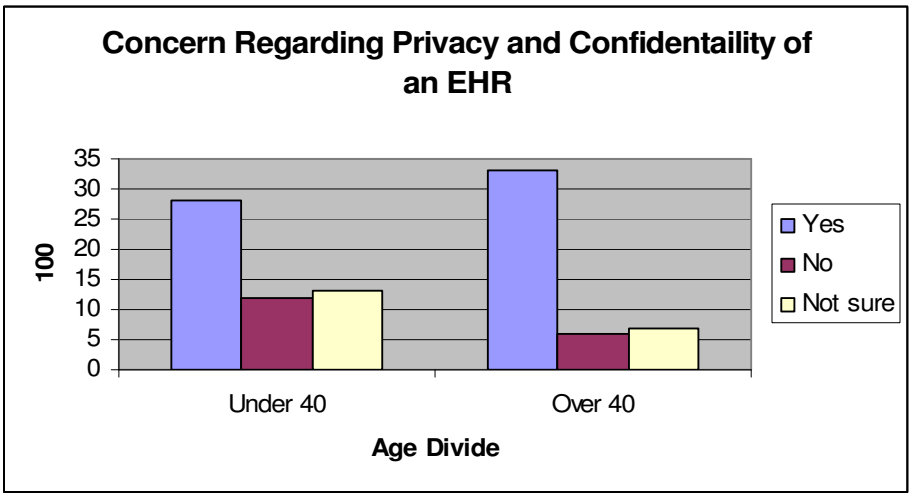

Figure 13: Concern Regarding Privacy and Confidentiality of an EHR in the Under and Over 40 Age Group

With the high percentage of the public showing concern regarding the privacy and confidentiality in question 12 the issues that may arise with the implementation of an EHR were probed further. When asked about the potential for an EHR to cause an

increase in medical error there was a one third split between positive, neutral and negative. Of this, the highest percentage of respondents in the neutral group was from the over 60 age group. This could be deduced to be a lack of knowledge as this group used a computer the least. The results proved interesting when the public were questioned on the statement that EHRs could lead to leakage of sensitive health information, only 9% felt that leakage of information would not occur with and EHR but 73% agreement with the statement that it could occur. As detailed in chapter 2 the recent media reports on the loss of laptops containing sensitive information could have influenced the response to this question. This was also reflected in the concern regarding the unauthorised sharing of health information where the percentages almost match the previous question. Opinion was not as strong regarding the robustness of installed data security systems with over 20% being neutral in their response.

Question 13 broadened the potential problems to reflect those that affect other IT systems. The responses as seen in figure 14 were that 71% agreed that malicious software that could affect their EHR was a potential problem. This is supported by the increase in malware as detailed in chapter 2. The response to the potential risk of deliberate acts of harm was almost identical to the above question. Vendor access did not appear to cause the same degree of concern with one third of the respondents' claiming a neutral stance. Half of the participants agreed or strongly agreed that storage and accessibility could be a potential problem. Backup risks were viewed by 54% to be a potential hazard to their EHR.

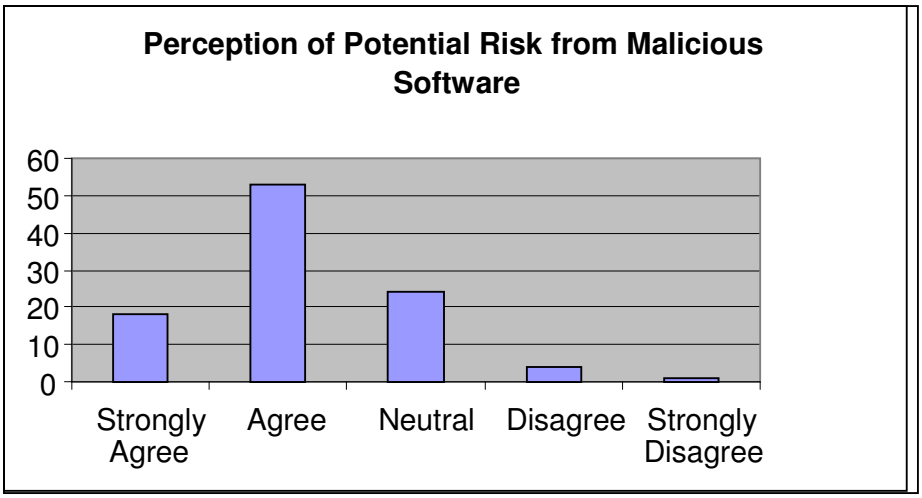

Figure 14: Perception of Potential Risk from Malicious Software

Question 14 examined the participant's response to the question if security systems were installed to protect an EHR would their concerns of privacy and securities decrease? The response was overwhelmingly positive with no negative respondents when asked about the implementation of a restricted access system, audit trail and encryption. Indeed, 86% and 88% respectively felt that with the implementation of anti-virus software and firewalls an EHR would be more secure.

The final question was to ascertain if the public felt that EHR's were more secure than the present paper based system. The response as demonstrated was very positive at 75% (figure 15).

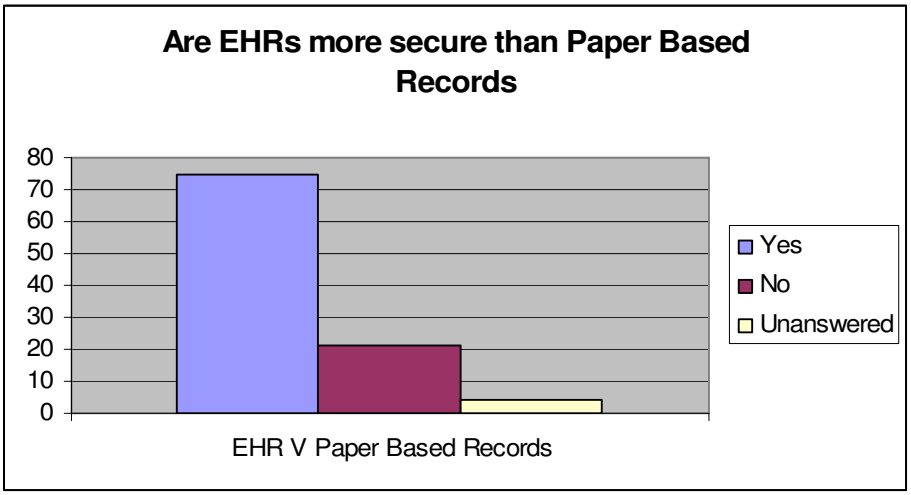

Figure 15: Are EHR's more secure than Paper Based Records?

There are interesting findings when associating usage of the Internet and E-banking with the respondent's perceptions of privacy and confidentiality of EHRs. Eighty one respondents stated they used the Internet 'regularly' or 'fairly regularly' and when asked if they were concerned about the privacy and confidentiality of their health record of these 51(63%) replied yes, 13 replied no and 17 were not sure. This compares to the result from the complete study population of 62%. When the Internet users were asked if they thought an EHR was more secure than paper based records 64 (79%) answered yes, 13 answered no and 4 had no opinion. Interestingly, 74% of the complete population thought EHR was more secure than paper. Sixty participants stated they used E-banking 'regularly' or 'fairly regularly' and when asked if they were concerned about the privacy and confidentiality of their health record 36 (60%)

replied yes, 11 replied no and 13 were not sure when questioned if they thought an EHR was more secure than paper based records 46 (76%) answered yes, 10 answered no and 4 had no opinion. (Figure 16)

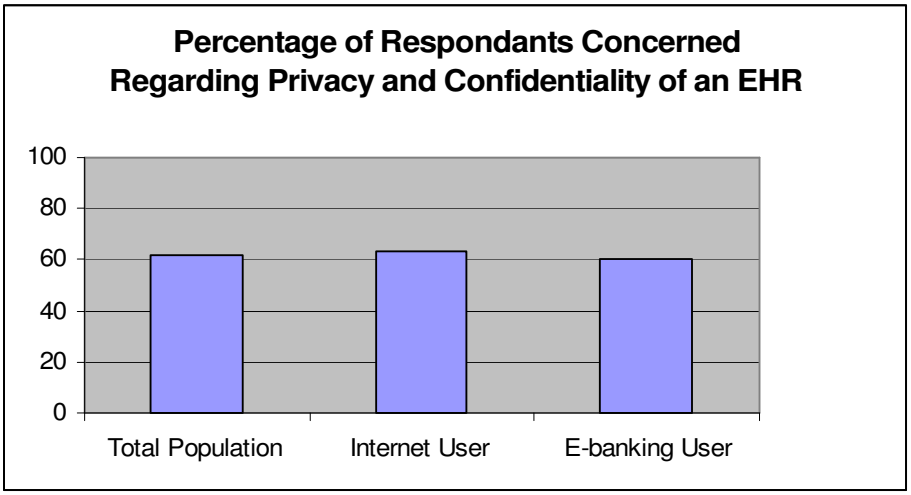

Figure 16: Percentage of Respondents Concerned Regarding the Privacy and Confidentiality of an EHR

Of the 6 members of the public questioned who stated they never used the Internet, they were split equally when asked regarding privacy and confidentiality of their health record and which health record type was more secure. Interestingly of those questioned who stated they never used E-banking (27%), 17 (63%) stated they were concerned regarding the privacy and confidentiality of their health record and 21 (78%) people felt that EHRs were more secure than paper based records. The results obtained from the entire study population indicating their privacy and confidentiality concern were 62%. This would indicate that the use or non use of E-banking had little or no affect on the participant's perception of privacy and security of their health record and that the EHR is regarded in as positive a light. Interestingly those who never use the Internet showed a marked difference in results with an even split. The number of participants in this group was 6 and came from the 50 and over age groups.

Of those who made comment many stated the importance of robust security setting to protect their data. One participant stated that "it would be expected that all safeguards would be in place prior to the implementation of an EHR". The system backup was frequently mentioned in relation to security but also regarding risk of damage with one respondent stating "Well it's less likely the records would be damaged as there

would be a backup/master copy". An interesting comment drew a comparison between E-banking stating that "if the banks can do it why can't healthcare. If people have a choice to use it like banking in time it could take over from paper". The issue of the authenticity was raised relating to reliance of signature in the identification of health officials. It was also stated that "both systems have their flaws" although it was felt that e-records could be circulated more easily and if "correct processes and security services (encryption, 2 factor authentication) were in place they could negate the risks". The reverse opinion was also stated, participants felt that "computers are as accessible, probably more so than a paper chart is in a warehouse" also "keeping a hard copy reduces the risk of people hacking into it. With fewer people involved less chance of malpractice".

There was concern stated as to who would have access to their EHR, whilst others felt that records were shared all the time now in paper format. Two respondents questioned that if all health information was stored electronically would insurance companies or mortgage providers acquire access. One comment stated that "I'm happy with things as they are why do we have to change things". There were three references to previous development of ICT systems (PPARS and E-Voting), where the implementation was perceived as poor and costly. Only 5% of those asked had knowledge of the Health Information National Strategy which was issued in 2004.

In conclusion, the majority of results concur with the study conducted by Chhanabhai and Holt and this will be discussed below. However, in answer to the question which motivated this research, the publics' use of E-banking did not affect their perception of privacy and confidentiality of the EHR. However in a limited number of respondents who did not use the internet the level of concern regarding privacy and confidentiality of their health record was lower than the study population and paper health records were perceived by 50% of this group as more secure than EHRs which was 21% higher than the study population . It was planned to ascertain the public understand and opinion of an EHR, two thirds of the respondents had no knowledge of an EHR. The study also aimed to establish that if adequate security system were in place would the public be willing to accept the move to an EHR. The response to this was overwhelmingly positive.

4.2 Comparison with Chhanabhai and Holt 2007 study

The sample group in this study was restricted to 100 while Chhanabhai and Holt (2007) had 300 respondents from a total of 400 questionnaires left at General Practice Surgeries throughout New Zealand, a response rate of 75%. The male female split in Chhanabhai and Holts study was weighted more towards females at 60% while in this study the split was more even with 53 male and 47 female. The mean age in this study was 41 while Chhanabhai and Holt states that the majority of participants were 20-39 years old. Both studies showed remarkable similarities when questioned on computer usage and e-mail use at >80%. The use of the Internet had a 10% increase in this study which could be due to the increase that would have occurred over the two year intervening period that has lapsed between studies.

Chhanabhai and Holt state that 44% did not purchase over the Internet while only 17% stated in this study that they had never purchased over the Internet and 51% stated that they regularly or fairly regularly purchased over the Internet. There were similarities at 62.6% from the Chhanabhai and Holt study compared with 65% from this study who had not heard of EHR. When asked regarding their privacy and confidentiality concerns with an EHR 73% replied that they had concerns in New Zealand while there were 10% fewer concerned respondents in this study. There appeared to be a much higher knowledge of health service initiatives with over 30% having knowledge of the National Health Index in New Zealand. In stark contrast, only 5% of respondents documented having any knowledge of the Health Information Strategy in Ireland. Chhanabhai and Holt established that most participants perceived that an EHR would lead to their medical information being leaked. This study concurred with those results with only 9% disagreeing with the statement. There was an almost even split with concern regarding an increase in errors and the implementation of an EHR in this study while there appears to be less concern with this in New Zealand, Chhanabhai and Holt (2007) deduces that it is not the publics' major concern with an EHR.

While comparing respondents' answers to potential problems with an EHR there are clear differences in concerns. The primary concern in the New Zealand study is unauthorised access to records as opposed to back-up failure or long term storage with

76% of their respondents being concerned regarding hacker and vendor access. In this study while the potential of hackers accessing their records produced a 72% concerned response, vendor access only concerned half the participants with even a lower number concerned regarding the long term accessibility of their records (Figure 17). Whether it can be assumed that concern is reduced with more frequent use of ICT systems is not answered. With security mechanisms in place both studies showed >80% positive response believing that it would make an EHR system more secure.

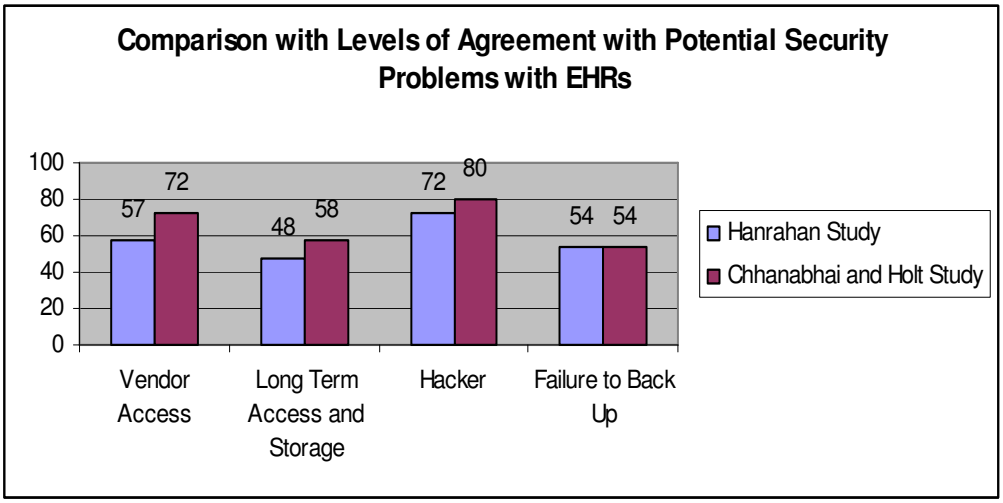

Figure 17: Comparison with Levels of Agreement with Potential Security Problems with EHRs

The final question, which asked whether electronic health record are more secure than paper based, showed quite a marked difference between the two studies. Chhanabhai and Holt (2007) documented that 55% believed that paper based records were more secure, this contrasted with this study where 21% believe that to be so. The most common comment noted in Chhanabhai and Holt's (2007) study was "I don't trust computers as they tend to crash" which was never mentioned in this study. It could be deduced that technology has become more reliable and "crashing" is not such an issue since the study was carried out by Chhanabhai and Holt in 2007.

Chhanabhai and Holt (2007) concludes from their study and this study concurs that

from the results the consumer is ready to accept the transition, as long as one can be assured that security systems are in place and the health consumer has involvement in who receives access to their records. Interestingly, in the Chhanabhai and Holt study those who purchased items using the Internet appeared to be less apprehensive about security concerns, these results conflict with the results from this study where no marked difference was established with the exception of the 6 respondents who did not use the internet.

4.3 Research Limitations

It is important to acknowledge that there were limitations to this research. Time was a crucial factor. This study was limited to one year and thus had to be scoped to ensure that the available time would produce valid and meaningful results. This was achieved within this period however with a longer time frame; this study could have been conducted on a larger population sample. This population sample could have been divided into urban and rural categories in a similar manner to Chhanabhai and Holt (2007) The JNIR (2008) detailed the differing usage groups associated with provincial location, the results showed a dramatic percentage difference.

An area where Chhanabhai and Holt (2007) also stated that there were limitations in his study was ethnic origin. Ireland has a growing number of ethnic minorities and this subject was not included in the questionnaire and could have added an extra dimension to this study as the JNIR (2008) survey showed a higher percentage of computer use in those born outside of Ireland.

The fact that the author diversified from Chhanabhai and Holt (2007) methodology by conducting the interviews rather than leaving questionnaire in General Practice waiting rooms may also be viewed by some as a limitation. The study carried out in New Zealand had a 75% response rate with an average respondent's age of 31. There was a concern that the response rate would be poor within the time frame dictated by the college. To repeat this study periodically would prove interesting as this area is in its infancy in Ireland and open to change.

4.4 Conclusion

The purpose of all research is to solve a problem (LoBiondo-Wood and Haber 2002). The problem or objective which sought to be deciphered or achieved by this research was to determine how the publics' use of the Internet including their experience of E-banking affects their perception of privacy and confidentiality of Electronic Health Records? This was accomplished by approaching 100 people and asking them to complete an adapted version of a questionnaire used by Chhanabhai and Holt (2007), the results of which are discussed in detail above.

Chhanabhai and Holt (2007) aimed to establish and document the importance of secure EHR systems from the public's perspective. Their objective was to firstly establish what the general public perceive as the main threat to the EHR and use this to build more robust systems. They concluded from their study that the consumer is ready to accept the transition to the EHR, as long as they can be assured that security systems are in place and the health consumer has involvement in who receives access to their records. The majority of the results discussed above are similar between the studies and this study would support the above conclusion.

However there was a marked difference in response to whether the EHR is more secure than paper based records. Chhanabhai and Holt (2007) documented that 55% believed that paper based records were more secure, this contrasted with this study where 73% believe that electronic based records are more secure. In answer to the research question that the author of this dissertation sought, there does not appear in this study to be a correlation between the publics' experience of E-banking and their perception of privacy and confidentiality of an EHR. There was, with a limited number of participants (6) who do not use the Internet a lower concern regarding privacy and confidentiality of their health record and surprisingly 50% of those felt that paper was as secure as the electronic solution. Whether these respondents were referring to the present paper based solution is unknown.

Chapter 5
Discussion

5.0 Discussion

From the literature review it is clear there is a vast amount written on the concept and indeed the potential of an EHR. There are many countries where an EHR is already part of the integral fabric of that Health System and many countries including Ireland have committed to development programmes of such systems. Within these development programmes there have been issues raised that will fundamentally affect what type of system is implemented and how accepting the health consumer is. The question of who owns the records and who controls the access rights have proved difficult to answer and indeed there are not clear answers apparent in current literature.

The public are proving to be cautious and have voiced their concern regarding the privacy and confidentiality of their records. In this study 62% stated they were 'concerned' regarding the privacy of their health record and a further 20% were 'not sure' which means that the alarmingly low number of only 18 respondents stated confidence. In Ireland the Health Service is dominated by paper based charts, indeed one of the respondents to the questionnaire stated the she had different charts in 3 different hospitals. The Health Service issued a Health Information strategy document in 2004. This detailed document puts forward the vision that the Department of Health and Children has for collection usage and storage of all health information. Yet when the public were asked had they heard of this strategy only 5% stated they had any knowledge of it. Could this lack of knowledge be responsible for the negative response and indeed, negative perception in relation to security and the EHR?

HIQUA are at present addressing the concern expressed above by a respondent with 'the 3 different charts' by examining the issues of a patient single identifier. From previous studies there are differing opinions on how the public view the single identifier as a means of identification and access. Flanagan (2006) concluded from her study which sought to investigate the issues surrounding privacy, confidentiality

and data protection of the EHR that 54% of those surveyed were not in favour of the use of a single identifier. It would appear that lack of knowledge was an influencing factor in these findings also. The formation of HIQA has provided a central authority that is charged with the task of implementing this strategy. In December 2005 the Health Service Executive signed a €56 million contract with iSoft to provide a standardised patient management software platform. This 10 year roll-out of patient administration software is underway with 30 hospitals now live. This system in its present form only captures patient's administrative information but is expected to solve some of the interoperability problems. However, there has been no documented formal evaluation of these systems to date.

It was also established in this study that there is an apparent lack of knowledge in relation to the EHR, with only slightly more than one third of respondents being aware of its existence. From those that were aware of its existence, it is clear that their privacy and confidentiality concerns are not solely related to an electronic record but arise from concerns with the current Irish system which is paper based, in addition to the negative publicity surrounding ICT and security. As recent as August 2008 a leading Sunday newspaper's headline concerned the unauthorised access to electronic data. The paper reported that highly sensitive confidential records containing the social welfare details of a significant number of Irish citizens were lost by a government official when a laptop was mislaid. It is not stated whether safeguards were employed to prevent unauthorised access to information contained in this laptop. In addition the Irish Payments Organisation were forced to reassure credit card customers that they would not be liable for fraudulent transactions that occurred recently after hundreds of customers had their details stolen by hackers some months ago. Indeed a survey carried out by the Sunday Business Post showed that a large number of retail outlets were using outdated Internet security defences that are ineffective against hackers. These media reports will have added to the concerns of people in relation to the privacy and confidentiality and the EHR. However, the media cannot be accused of scare mongering as the documented events have occurred and the potential threats to peoples' personal information are very real.

The affect of fraudulent transactions though inconvenient and costly is repairable with the issuing of new credit cards or altering of account details. The affect of

unauthorised access to personal health information is irreparable as this information is not transferrable and cannot be re-issued or altered. The facility to issue a new card is not available to a health consumer whose personal data has been accessed by someone unauthorised to do so. With a paper based health record system the potential for unauthorised access is limited to those in the immediate area where notes are held. However, when moving to an electronic system the potential for unauthorised access is global. This re-enforces the need for robust security measure in IT health system to allow only authorised personal access personal health data and facilitating an increase in confidence of the general public in relation to the EHR.

There is no doubt that the use of technology has infiltrated all aspects of Irish society. This study showed that 81% of respondents used the Internet and their usage was across all age groups, with 100% usage in the under 40 age group. As this under 40s age group matures further, the percentage use of ICT will increase. It can be assumed that as E-banking acceptance has evolved over the past decade so will the publics expectations in relation to other forms of ICT. The health sector is an ideal industry for such application of technology due to the large volumes of information it produces. Indeed, it is anticipated that the current country wide implementation of the iSoft patient administration system will provide a common platform to work from. The inception of HIQA, the health information: a national strategy document and the introduction of the health information bill in the near future, should pave the way for a framework that will facilitate the development of an EHR.

Information gained from this and previous studies carried out by Flanagan (2006) in Ireland and Chhanabhai and Holt (2007) in New Zealand highlights the importance of the healthcare consumer's involvement. These studies showed that the public wish to have access to their health records. They also felt strongly regarding who has access to them. They expected that the highest levels of security would be in place and if that was the case, the majority of those surveyed would be accepting of an EHR. The respondent's usage of E-banking did not make the participants of this study any more relaxed regarding security measures. While results from those who had never used the Internet stated less concern regarding the privacy and confidentiality of their health record and a higher percentage feeling that paper based systems were more secure. This study did not elicit whether this reduced concern regarding privacy and

confidentiality related to the present paper based solution.

The economic down turn that has occurred in Ireland over the past 6 months, is without doubt going to have an impact on the Health Service. The exchequer is already showing a deficit of €5,648 million for the first half of 2008 (Lenihan 2008). Each ministerial department will no doubt be asked for cost savings. The impact of this on the Health Service may result in withdrawal of funding for projects which may include ICT. Should the Irish Government decide that ICT and healthcare are not a priority the HSE will fall further behind in the realisation of the EHR? Kohn et al (1999) stated that 98,000 citizens in the USA died annually as a result of medical error. Still (2005) claims, that the introduction of an EHR could reduce those errors by as much as 90%. If these statistics can be applied pro rata to the Irish health service, the implementation of an EHR must become a priority. Indeed the following quote indicates that the Department of Health and Children view this implementation with the same urgency:

> "ICT enabled healthcare is essential to ensure that care is delivered in a safe and more efficient manner by providing complete, accurate and timely information at the point of care whether within the hospital setting, in the community or in the home."
>
> (Department of Health and Children 2008)

Chapter 6
Conclusion

6.0 Conclusion

Privacy and confidentiality are core aspects in the roles of health providers and are paramount when documenting this provision of care. All healthcare professionals have a professional duty to maintain medical records in confidence (Department of Health and Children 2008). Indeed, it is not only the healthcare professionals who have a legal and ethical obligation to the patient and their details but the vendors of these hospital information systems. The literature is clear that ICT and healthcare can work together effectively. In fact, some researchers would argue that such an information intensive industry could not survive without the use of ICT (NCNM 2006). A major technological advancement in the domain of health informatics is the emergence of the EHR. However, not everybody is welcoming this advancement with open arms.

The literature is unambiguous that there are many concerns in relation to the security abilities of such applications and the hacking abilities of some intruders. The literature highlights that there are similar issues which exist in relation to security and E-banking and yet some 60% of people are conducting their banking business 'regularly' or 'fairly regularly' online with a further 12% having used it at sometime. Unfortunately, leakage of electronic personal information has made headlines in Irish newspapers on a weekly basis recently. In spite of advancements made in security abilities, the perpetrators of technology crime are forging ahead with ever more ingenious methods. There must also be blame laid at organisations who do not insist on adherence to procedures relating to the storage of sensitive information and hardware access. Technological advancements are rendered useless if lax security procedures are in place that can allow a laptop containing sensitive information to be misplaced (Kennedy 2008). Despite these very public security breeches, the general public are still using on-line services on a daily basis. It therefore has to be asked if the general publics use of the Internet including their experience of E-banking affect their perception of privacy and confidentiality of Electronic Health Records.

Research aims to add to what is already known to a body of knowledge. Chhanabhai and Holt (2007) concluded from their study entitled: Consumers Are Ready to Accept the Transition to Online and Electronic Records If They Can Be Assured of the Security Measures, that in order to fully integrate an EHR in the health sector, two main issues needed to be addressed. Firstly, the system requires the highest level of security protection with monitoring and updating governed by accredited standards policed by a regulated body. Secondly, the health consumers require a more proactive role in the ownership and maintenance of their health record. These two issues, they argue, must be adequately addressed before the health consumer will accept Electronic Health Records.

It was planned to replicate the study discussed above with a slightly different slant. The author aimed to establish if experience of the Internet and/or E-banking usage would affect the publics' perception relating to the capture, use and storage of the personal health information in the form of an EHR. One hundred people were asked to complete a questionnaire that was adapted from a similar study carried out by Chhanabhai and Holt (2007). The results of this study indicate that the public perceive a risk associated with ICT. This perception is not exclusive to health information and has been re-enforced by the almost weekly media revelations detailing breeches in security leading to unauthorised systems access. If the appropriate security systems are in place to protect their health information the majority of the general public will accept the transition to an EHR.

In conclusion, the objective of this research was to determine whether the publics' use of the Internet including their experience of E-banking affect their perception of privacy and confidentiality of Electronic Health Records? The answer to the question is that the publics' use of E-banking did not alter their perception of privacy and confidentiality of EHR. Though with a limited number of those who did not use the Internet there was a lower degree of concern regarding the privacy and confidentiality and 50% felt that paper based health records were more secure than electronic solutions. With this in mind, there are many challenges ahead for those involved in the EHR's implementation in Ireland. The Health Information: A National Strategy (2004) document will provide an excellent framework for the development and implementation of an EHR. They are aware of the challenges ahead and state:

> "The successful transition from a paper based system to a digital environment will require robust change management processes and training arrangements, hardware and software support and support of information governance processes to ensure confidentiality, privacy and security."

The change management process mentioned must be aimed at healthcare consumers and healthcare users to ensure an open and trusting relationship. However, it is feared that in today's unstable economic environment the successful transition as stated above will not be allocated the priority it requires. It is clear that publics' usage of the Internet and E-banking will not make the transition smoother or lessen the demands for robust security measure to protect the collection and dissemination of sensitive health information.

The author plans to present the findings at health informatics conferences, and publish in a scholarly journal. The results of this study will be shared with Mr. Prajesh Chhanabhai and Mr. Alec Holt who have already expressed an interest in conducting further research together in relation to this topic.

References

1. Abdolrasulnia, M., Menachemi, N., Shewchuk, R., Ginter, P., Duncan, W. and Brooks, R (2008). Market effects on Electronic Health Record Adoption by Physicians. *Health Care Management Review*. 2008 Vol 33; pp 243-52.

2. Aburrous, M., Hossain, M.A., Thabatah, F. and Dahal, K. (2008). Intelligent Quality Performance Assessment for E-banking Security using Fuzzy Logic. I.T.N.G. 2008. *Fifth International Conference.*.pp 420 – 425.

3. Alvarez, R., (2006) e-Health: integrating information technology into health care International Organisation of Standardisation [Internet], ISO Available from: <http://www.iso.org/electronic+health+record>. [Accessed on 18tth April 2008].

4. Amatayakul, M. (1999). EHRs and the consumer: a new opportunity. In Murphy G.F, Hanken, M.A, Waters, K.A., (Eds.) *Electronic Health Records Changing the Vision.* Philadelphia: WB Saunders Co; 1999. pp. 26–68.

5. America on Line and National Cyber Security Alliance (2005). AOL/NCSA on line safety study. December 2006. Available from: < http://www.staysafeonline.org/pdf/safety_study_2005.pdf>. [Accessed on 2nd June 2008].

6. Anderson, J., (2006). Social, Ethical and Legal Barriers to E-Health. *International Journal of medical informatics*. 76, pp 480-483.

7. Annas, GJ.(1989). *The Rights of Patients: The Basic ACLU Guide to Patient Rights*. 2nd ed. Carbondale, Ill: Southern Illinois University Press.

8. Bagchi, L. M. and af Ursin, R. (2007). Considerations in designing personal health records for the undeserved population. Available from < http://www.mathematica-mpr.com/publications/pdfs/hlthcaredisparib1.pdf>. [Accessed on 10th April 2008].

9. Bainbridge, R. (2006). The History of Online Banking. Available from <http://ezinearticles.com/?History-of-Online-Banking&id=270075>. [Accessed on 14th May 2008.]/

10. Ball, M. And Collen, M.,(1992). *Aspects of the Computer-based Patient Record*. USA: Springer. pp.1-10.

11. Bernie, B. (2008). Canada Leads World in Online Banking Usage. comScore Inc. Available from <http://www.comscore.com/press/release.asp?press=2318 >. [Accessed on 28th July 2008].

12. Bishop, L., Holmes, B. and Kelley, C., (2005). National Consumer Healthcare Privacy Survey 2005. Available from < http://www.chcf.org/>. [Accessed on 18th April 2008].

13. Boehm, E. (2007). Plans' PHRs must overcome member anxiety. Why non users of plan-hosted personal health record aren't onboard. Available from: < http://www.forrester.com/rb/search/results>. [Accessed on: 9th May 2008].

14. Buddle, P. (2008) Internet world overview report. Available from: < http://www.budde.com.au/reports/listReports.aspx?r=51>. [Accessed on 5th August 2008].

15. Califf, R. M. and Muhlbaier, L. H. (2003). Must There Be a Trade-Off Between Privacy and Quality of Health Care, or Can We Advance Both? *American Heart Association*.108, pp915-918.

16. Card Technology Today, (2004) Australian Health Card Launched. 16 pp 5.

17. Carter, M. (2000) Integrated Electronic Health Records and Patient Privacy: possible benefits but real dangers. *Medical Journal of Australia*. 172, pp28-30.

18. Chhanabhai, P., Holt, A. and Hunter, I. (2006). Consumers security and electronic health records. Available from: < http://www.business.otago.ac.nz/infosci/pubs/papers/papers/dp2006-01.pdf>. [Accessed 1st October 2007].

19. Chhanabhai, P. (2006). EHRs: Fear of Breach? The New Zealand public's opinion. Research Masters Thesis. University of Otago

20. Chhanabhai, P. and Holt, A. (2007). Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. *Medscape General Medicine*. 9(1), pp8-16.

21. Cormack, D. F. S. (1991). *The Research Process in Nursing*. Blackwell Science:Oxford.

22. Corrigan, D. (2006) E-banking new era. Available from: <http://archives.tcm.ie/businesspost >. [Accessed 13th May 2008].

23. Cowan, S., (1997) Continuing Education –Research. Available from: <http://www.ino.ie/DesktopModules/Articles/ArticlesView.aspx?TabID=202 &ItemID=1846&mid=7303>. [Accessed on 15th July 2008].

24. Daniel, E. (1999). Provision on electronic banking in the UK and the Republic of Ireland. *International Journal of Bank Marketing*. 17(2), pp72-83.

25. Data Protection Agency (2008). The Data Protection Rules in Practice. Available From: http://www.dataprotection.ie/viewdoc.asp?DocID=245. [Accessed 18th July 2008].

26. Davies, E., (2001) A sense of Déjà vu. *British Medical Journal*. 322, pp287-289.

27. Davies, F. and Venkadesh, V. (1996). A Critical assessment of potential measurement biases in the Technology Acceptance Model: Three experiments. *International Journal of Human and Computer* Studies. 45, pp 19-45.

28. Department of Health and Children. (2008). Access to Medical Records in Ireland,Availablefrom:<http://www.dohc.ie/public/information/legal_matters_and_health/access_to_medical_records.html?lang=en>. [Accessed 20th April 2008].

29. Department of Health and Children (2008). Minister Harney announces a Public Consultant on the proposed Health Information Bill. Available from: <www.dohc.ie/press/releases/2008/20080619.html>. [Accessed on 15th August 2008].

30. Department of Health and Children (2008). Discussion paper on proposed Health Information Bill. Available from: < www.dohc.ie/issues/hib/discussion_paper.pdf?direct=1>. [Accessed on 16th August 2008].

31. Doty, C. (2008) Welcome to the jungle: Google, Microsoft, And revolution tout cures for healthcare maladies. Open platforms require eBusiness Executives to plan for privacy protection. Available from: <http://www.forrester.com/Research/Document/Excerpt>. [Accessed 9th May 2008].

32. Fair Isaac Inc. Available from: http://www.fairissac.com/fic/en/company/. [Accessed 30th July 2008]

33. Favier, F. (2007). Smart Cards and Healthcare. *Card Technology today*. 19, pp 10.

34. Flanagan, K., 2006. Electronic Patient Records: An Investigation into Issues Surrounding Privacy, Confidentiality and Data Protection. Unpublished dissertation. Available from Trinity College Dublin Library.

35. Fried S. (2002) Phishing: a new twist to an old game. *Information Security Management Handbook*. CRC Press.. pp559-576.

36. Gartner Research Inc: Phishing and Online Attacks Cause Dip in Consumer Confidence (2005). Available from < http://www.gartner.com/> [Accessed on 26th July 2008]

37. Givens, P. (1996). Medical records privacy: fears and expectations of patients. San Diego: Privacy Rights Clearinghouse; May 15, 1996. Available from:< http://www.privacyrights.org/ar/speech2.htm>. [Accessed January 2, 2007].

38. Goldman, J. (2007) Health Privacy Project. Centre for Democracy and Technology. Available from<http://www.healthprivacy.org/usr_doc/Wired_ letter_7-23.pdf >. [Accessed on April 20th 2008].

39. Goodin, D. (2007) Data For 800,000 Job Applicants Stolen. The Register. Available from http://www.theregister.co.uk/2007/09/28/gap_data_breach/ [Accessed on 10th August 2008].

40. Gordon, W. and Langmaid, R.(1988). *Qualitative market research: A practitioner and buyers guide.* London: Gower.

41. Gostin, L. (1997). Health care information and the protection of personal privacy: ethical and legal considerations. *Annals of Internal Medicine.* 127(5), pp 683-690.

42. Hanrahan, D. (1999) Internet Banking: The potential of the Internet for Virtual Banking in AIB. Unpublished dissertation. Available from University College Dublin Library.

43. Health Information. A National Strategy. (2004) Available from: <www.dohc.ie/publications/nhis.html> [Accessed on 15th October 2007]

44. Holmes, B. and Hanson, J. (2007). Which consumers share medical information? Sharing is linked to consumer attitudes towards medical community and basic trust.
Available from : <http://www.forrester.com/Research/Document/Excerpt > [Accessed 9th May 2008]

45. Hodge, J.G. Jr. (2003). Health Information Privacy and Public Health. *Journal of Law, Medicine and Ethics*. 31, pp663-671.

46. Hyrinen, K., Sarento, K. and Nikanen P. (2007). Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International Journal of Medical Informatics.* 77(5), pp 291 – 304.

47. Internet World Stats. (2008). Internet usage statistics – The Internet big picture. Available from: < http://www.internetworldstats.com/stats.htm> [Accessed on 5th August 2008].

48. I-onlinebanking .com. (2008). Online Banking. Available From:< http://www.i-onlinebanking.com> [Accessed 1st August 2008].

49. ISO TR 20514:2004 "Health Informatics - EHR Definition, Scope, and Context"International Organisation for Standardisation (2005). Available from: <http://www.iso.org/>. [Accessed 18th April, 2008].

50. Jairneth, N., Hogerney, M. and Parsons, C. (2000). The role of the pilot study: a case illustration from cardiac nursing research. *Applied Nursing Research.* 13(2) pp92-96.

51. Kelly, M. (2006) BoIs E-banking Service gets a facelift. Available from: < http://www.electricnews.net/article/9703655.html> [Accessed 3rd December 2007]

52. Kennedy, E. (2008). Victim of BoI laptop treble to 31,5000. Available from: < http://www.independent.ie/national-news/victims-of-boi-laptop-theft> [Accessed on 24th May 2008].

53. Key Points on Patient Consent in Cork University Hospital Group – a guide for staff (2006) Health Service Executive Available from: < http://handbook.muh.ie/pat/Consent_CUH_Guide_For_Staff_2006.pdf>. [Accessed on 21 July 2008].

54. Kohn, L., Corrigan, J. and Donaldson, M. (2000). To Err is Human. Building a Safer Health System. *National Academy Press 2000.*

55. Kornokov, K. (2006). Mastercard credit card details stolen in UK. Available from: <http://www.viruslist.com/en/viruses/news?id=185885481> [Accessed 15th July 2008].

56. Leiner, B., Cerf, V., Clark, D., Kahn, R., Kleinrock, L., Lynch, D., Postel, J., Roberts, L., and Wolff, S. (1999). A brief history of the Internet. Available from: <http://arxiv.org/abs/cs/9901011v1>. [Accessed 13th May 2008].

57. Lenihan, B. (2008) End-June 2008 Exchequer Returns. Available from: < www.finance.gov.ie/viewdoc.asp?DocID=5329>. [Accessed on 22nd August 2008].

58. Li, M.and Poovendran, R. (2005). Enabling Distributed Addition of Secure Access to Patient's Records in A Tele-Referring Group. Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference.

59. The Linux information project. (2006) Malware Definition. Available from: <http://www.linfo.org/malware.html>. [Accessed 14th July 2008]

60. LoBiondo-Wood, J. and Haber, J. (2002) *Nursing Research Methods, Critical Appraisal and Utilisation*. Molsby: Missouri.

61. MacDonald, R. (2001). A sense of Déjà Vu. *British Medical Journal.* 322, pp 287-288.

62. The Medical Council 2004. A Guide to Ethical Conduct and Behaviour. 6th Edition.Available from:http://www.medicalcouncil.ie/_fileupload/standards/Ethical_Guide_6th_Edition.pdf.> [Accessed 25th April 2008].

63. Mandl, K., Szolovits, P. and Kohane, I. (2001). Public standards and patients' control: how to keep electronic medical records accessible but private. British Medical Journal. 322, pp283-284.

64. Mathematica Policy and Research Inc. Using Personal Health Records to Address Disparities in Health Care Available from: < http://www.mathematica-mpr.com/health/pershealthrecords.asp>. [Accessed 19th April 2008].

65. May, N and Pope, C (1995) Qualitative Research: Rigour and qualitative research. *British Medical Journal*.31, pp109-112.

66. McSherry, R., Artley, A., Holloran, J. (2006). Research Awareness: An Important Factor for Evidence-Based Practice? *Worldviews on Evidence-Based Nursing*.3(3), pp103–115.

67. Mori, T. (2002). Growing acceptance of E-banking (trends). *New Media Age*. 16(1), pp12.

68. Moutaz, A. (2005). A study of E-banking security perceptions and customer satisfaction issues. Unpublished dissertation. Available from Dublin City University Library.

69. National Consumer Privacy Health Survey 2005 Available from: < http://www.chcf.org/topics/view.cfm?itemID=115694> [Accessed 11th October 2007].

70. The National Council for Professional Development in Nursing and Midwifery (2006). The Evolving Role of ICT in the Healthcare Sector. Health Informatics Society of Ireland Conference. Dublin, Ireland. May 2006.

71. National Joint Internet Research Survey (2008). Available from: < http://www.jnir.ie/jnir/Main/Methodologies.htm> [Accessed 4th August 2008].

72. National Programme for Information Technology (NHS). The public view on electronic health records. October 7, 2003. Available from:< www.dh.gov.uk/assetRoot/04/05/50/46/04055046.pdf > [Accessed 11th October 2007].

73. Neame, R. (1996). Privacy and security issues in a wide area health communications network. *International Journal of Bio-Medical Computing*. 43(1-2), pp123-127.

74. The No-Computer Virus – IT in the healthcare industry (2005). *Economist*. 375(8424), pp71-74.

75. Ovretveit, J., Scott, T., Rundall, T., Shortell, S. and Brommels, M. (2007) Implementation of Electronic Medical Records in Hospitals: Two Case Studies. *Health Policy*. 84 (2-3), pp181-190.

76. Parahoo, K. (1997). *Nursing Research. Principles, Process and Issues*. Palgrave: New York.

77. Peleg, M., Beimel, D., Dori, D. and Denekamp, Y. (2008). Situation based accessed control: Privacy management via modelling of patient data access senarios. *Journal of Biomedical Informatics*. 41(1), pp180-201

78. Polit, D.F., Beck, C.T. and Hungler, B.P. (2001*). Essentials of Nursing Research. Methods, Appraisal and Utilization*. 5th Edition. Lippincott: New York.

79. Pyper, C., Amery, J., Watson, M. and Crook, C. (2004). Patients experiences when accessing their online electronic patient records in primary care. *British Journal of General Practice.* 54, pp 38-43.

80. Ray, P. (2006). The need for technical solutions for maintaining privacy of EHR. Proceeding of the 28th IEEE EMBS Annual International Conference. NYC USA Aug-Sept 2006.

81. Raysman, R., Brown, P. and Nemeth, K. (1998). Corporate Internet, Intranet and E-mail policies. New York Law Journal. Available from:< http://www.law.com/jsp/nylj/index.jsp> [Accessed 25th April 2008].

82. Retail Payment Systems Booklet. Available from:http://www.ffiec.gov/ffiecinfobase/booklets/Retail/retail.toc.htm. [Accessed on 12th April 2008].

83. Robertson, E. (2004). *A Phish Tale? Moving from Hype to Reality.* Needham M.A. Towergroup.

84. Roger, M. (2006). Social Engineering. The Human Factor in information assurance. *European Journal for thenInformatics Professional.* VII(1),pp59-62.

85. Runyon, B., Rischel , W., Heib, R., Shaffer, V., Handler, T., Lovelock, J.D. and Edwards, J. (2008). Hype cycle for healthcare provider technology and standards. Gartner Inc. Available From: http://www.gartner.com/DisplayDocument?id=707112 [Accessed 4th April 2008].

86. Slater. W. (2002). Internet History and Growth. Chicago Chapter of the Internet society. Available From: < http://www.google.ie/search?hl=en&q=Internet+History+and+Growth.+Chicago+Chapter+of+the+%09Internet+society%2C++September+2002.&btnG=Google+Search&meta=> [Accessed 14th June 2008.]

87. Sohail, M. and Shanmugham, B. (2003). E-banking and customer preferences in Malaysia: an empirical investigation. *Information Sciences—Informatics and Computer Science: An International Journal.*15, pp207-217.

88. Still, T. (2005). Electronic Health Records can save lives and improve medical care. Available from: < http://wistechnology.com/articles/1545/> [Accessed on 23rd November 2007].

89. Taft, J. (2007). An examination of the antecedents of electronic banking technology acceptance and use. Unpublished dissertation. Available from< http://proquest.umi.com.>. [Accessed 12th April 2008]

90. Tarling, M. and Crofts, L. (2002). *The Essential Researchers Handbook.* Bailliere Tindall.

91. Tipton, H. and Krause, M. (2004). *Information Security Management Handboook.* 5th Edition. CRC press. USA.

92. Trinity College Dublin 2008. What is Health Informatics? Available From: < https://www.cs.tcd.ie/courses/mschi/>. [Accessed 25th April 2008].

93. Tubin, G. (2005).The sky IS falling: The need for stronger consumer online banking authentification. Available from: < http://www-304.ibm.com/jct03004c/businesscenter/fileserve?contentid=82467>. [Accessed on 12th May 2008].

94. Vainio, H.M. (2006). Factors influencing the corporate customers' acceptance of Internet banking: Case of Scandinavian trade finance customers. Unpublished dissertation. Available from: <www.pafis.shh.fi/graduates/hanvai03.pdf > [Accessed on: 17th April 2008].

95. Wang, Y.S., Wang, Y.M., Lin, H.H. and Tang, T.I. (2003). Determinants of user acceptance of Internet banking: an empirical study'. *International Journal of Service Industry Management.* 14, pp501–519.

96. Watson, N. and Halamka, J.D. (2006). Patients should have to opt out of national electronic care records. *British Medical Journal.* 333, pp39-42.

97. Weagemann, C. (2002). "Status report 2002: Electronic Health Record" Medical recordsinstitute.Availablefrom:<http://medrecinst.com/pages.libArticle.asp?id=44>[Accessed on 11th October 2007]

98. Weitz, M., Drummond, N., Kingle, D., Ferris, L.E., Globerman, J., Hibert, H., Tracy, C. and Cohen, C. (2003) In Whose Interest? Current issues in communicating personal health information: A Canadian Perspective. *Journal of law, Medicine and Ethics.* 31(2), pp 292-301.

99. Welcome to the Federal Financial Institutions Examination Council's. Available from: < http://www.ffiec.gov/> [Access from booklet E-banking 17th April 2008].

100. Westin, A. F. (2005). Public attitudes towards electronic health records. Privacy and American Business. Available from:<http://www.webcitation.org/5HnyoU41Z >[Accessed on 11th October 2007].

101. Wikipedia. Available from:< http://en.wikipedia.org/wiki/>

102. Wilson, D. (1998). Health services research and personnel health information: privacy concerns new legislation and beyond. *Canadian Medical Association Journal.*159(11), pp1378-80

103. Yin, R. (1994). *Case study research: Design and method* (2nd ed.). Beverly Hills, CA: Sage.

Appendices

Appendix 1

Phishing Letters

From: HSBC Banking <mailto:hsbcmessage@hsbc.co.uk>
Sent: Tuesday, May 02, 2006
Subject: Security Message - Phishing attacks

May 02 2006 11:04:08

Message

Like other UK banks, we are currently seeing very large numbers of "phishing emails" in circulation. Many of these look as if they are from HSBC, typically encouraging you into Fraudant Activities.

Such attempted frauds only work if you don't upgrade your HSBC details. Also, a copy of this message has been sent to your HSBC online banking messages too.

Please remember to click the link below for HSBC Account Upgrade:

http://www.hsbc.co.uk/1/2/account/upgrade

From: HSBC Bank <mailto:system@hsbc.co.uk>
Sent: Thursday, May 25, 2006
Subject: HSBC Bank new security system

HSBC

HSBC Bank plc

Dear valued member ,

We are glad to inform you that our bank has a new security system. The updated technology will insure the security of your payments trough our bank. Hoping you'll understand that we are doing this for your own safety, we suggest you to renew your account .

Once you have renew your records, your session will not be interrupted and will continue as normal.

To renew your HSBC Bank PLC. account information click on the following link:

https://www.hsbc.co.uk/1/2/personal/pib-home

Note: If we do not receive the appropriate account verification within 48 hours, the account will be suspended. The purpose of this verification is to ensure that your bank account has not been fraudulently used and to combat the fraud from our community .

Best Regards ,

J. S. Smith
Security Advisor
HSBC Bank PLC.

Appendix 2

Online Fraud Information - Staying secure online

Bank of Ireland supports makeITsecure-go to www.makeitsecure.org for information.

This month's tip for staying secure online . . .

- **<u>Do</u> regularly check your bank and credit card statements for any suspicious or irregular activity.**

Remember, Bank of Ireland never requests, on any single occasion, your **full** personal log on information such as Online User ID, **full** 6 digit PIN and password information (i.e. Date of Birth and last 4 digits of your telephone number), either over the phone or online.

Proceed

Sellers, Buyers BEWARE new PHISHING Scam! Watch Out

by: Top 10,000 Reviewer

This scam is a new twist on an old favourite. SCAMMERS, we know what you're up too!!!

Recently at Emucade we're seeing an increase of "phishing" attempts. Now these are not a new idea, but it seems the scammers are getting more industrious in their attempts to scam the good folks of EBAY. This scam actually did fool someone in our office 2X. So BEWARE.

In a normal "phish" a scammer will try to get you to log into a phony site that looks like a legitimate site. For example, you'll receive an email saying "your payment for $1000.00 was received". Now if you have not paid for anything recently you'll be FREAKING OUT!!! So you'll log into your account to see what's going on. Of course you will use the convenient link within the email that was sent to you, and BAM!!! You logged into a bogus site and some loser now has your "username" and "password". The email looked legit, but in reality it was a bogus email "phishing" attempt, and you took the bait.

That's the old version and it's been around for a while, but here's the new twist and it's sometimes hard to spot.

The scammers are now searching through legitimate seller auctions and store items and setting up their phony email "phishing" with legitimate items from EBAY. As a seller, you'll certainly be excited about any interest in your items and you will be happy to answer any questions, BUT BE CAREFUL. The link within the email may look like it was a question sent through EBAY, and the item may be an item your selling, but it reality, the email did not come through EBAY and you'll be logging into a bogus site. We've had this happen twice in the last month where someone in the office answered a question and did not realize they were giving away our user name and password.

Making things worse, we've seen some "phishing" attempts come from legitimate EBAY accounts. For example the scammers set up or break into a legit EBAY account, so the user ID is valid and upon some research you'll find that user is active on EBAY but has had no activity for a while. Often times these accounts are un-used for long periods of time or "abandoned" by the originator so the scammers use the accounts without hassle.

Here are some things we have done to thwart the enemy...

1. Check feedback and history. This is a staple of the EBAY community and is much of the reason why EBAY works as well as it does. If something looks shady, IT

PROBABLY IS. No seller or buyer would go out of their way to deliberately "look" shady. That doesn't help anyone's cause.

2. We set up an email account on our domain and use it only for EBAY. All other email accounts used on our web site or as technical support are different entirely. This way if a question looks like it's from EBAY and was not sent to our EBAY email we know it's bogus. This works because we only use the EBAY email for EBAY and never give it out.

3. We are also in the habit of changing password on a regular basis, and good backups are worth their weight in gold. Sometimes the old standards make the most sense.

We're hopeful someday the community will find a way to eliminate these types of scams, but until that happens we all need to be on guard. Much of what keeps non-EBAYers off EBAY is the fear they will get ripped off. I know a ton of folks who would love to use online auctioning to find "hard-to-find" goods but just won't do it for fear of getting burned.

Hope this helps! If it does, Please pass it around.

Emucade Arcade Machines

Appendix 3

Prajesh C show details 04/12/2007 Reply

to me

Hi Diane

Sorry to hear that you have reached the dreaded point when you find that some else has done what you were planning to do. I had the same problem with mine, but i did exactly what you thinking about doing, i stayed in the same area but shifted my angle slightly, to make it different, yet able to reference the flaws from the study that had already taken place.

With regards to across hemispheres, we could possibly look at security fears that consumers are worried about, in Ireland and in NZ the similarities and the differences or something to that effect.

Ireland is not on my agenda, but I've been changing my trip so much, who knows what will happen.

Great to hear from you as well, and do keep in touch. I am interested in what you are doing.

Regards
Prajesh

On Dec 3, 2007 1:55 PM, Diane Stella Mary Hanrahan < hanrahad@tcd.ie> wrote:
Hi Prajesch,

Thank you so much for the prompt reply. I have come to a bit of a standstill at the moment as my proposed topic had been covered in a similar manner in a dissertation two years ago but was not available for me to see until last week. As you can imagine I'm really disappointed. I'm still keen to do something related but just have to find an angle. I was looking at medical record fragmentation due to security fears, I'm just not sure. You mentioned that we might be able to look at something across the hemispheres. I would be keen to hear any of your ideas.

I hope your having a good trip and enjoy Europe. Are you planning to visit Ireland at all?

Thanks again. It was great to hear from you.

Diane

Prajesh C show details 16/11/2007 Reply

to me

Hi Diane,

Firstly call me Prajesh. I'm really pleased to hear from you. This was a very interesting study and produced interesting results. It would be great to see if the hemispheres produce differing results.

I would be delighted to help you with anything I can. Unfortunately I am limited at the present as I am travelling though Asia on my way to Europe for a couple of months.

I should be back in New Zealand at the beginning of December. Don't hesitate to contact me if you need anything.

Regards,
Prajesh

On Oct 10, 2007 4.25PM, Diane Stella Mary Hanrahan < hanrahad@tcd.ie> wrote:
Dear Mr. Chhanabhai,

I am a Msc Student of Health Informatics, attending Trinity College, Dublin, Ireland. I am interested in the area of Privacy and Confidentiality relating to the implementation of an Electronic Health Record.

I have read with interest the study you carried out with Alec Holt. I am interested in adapting your study to the Irish setting and would be delighted to hear of your thoughts.

Kind regards,

Diane

Appendix 4

Original Questionnaire from study carried out by Chhanabhai and Holt 2007

About you

1. My age is: 19 or under ☐ 20-29 ☐ 30-39 ☐ 40-49 ☐ 50-59 ☐ 60-69 ☐ 70-79 ☐ 80 or over ☐
2. Gender: Male ☐ Female ☐
3. At the time of filling on this Questionnaire what part of New Zealand are you in?
Auckland ☐ Christchurch ☐ Wellington ☐ Dunedin ☐

Your Computer Use

	Regularly	***Fairly Regularly***	***Sometimes***	***Seldom***	***Never***
4. I use a computer	☐	☐	☐	☐	☐
5. I use E-mail	☐	☐	☐	☐	☐
6. I use the Internet	☐	☐	☐	☐	☐
7. I buy things over the Internet	☐	☐	☐	☐	☐

Electronic Health Records

8. Before participating in this study had you heard of Electronic Health Records? Yes ☐ No ☐

9. The following are **proposed** benefits to YOU of Electronic Health Records. How do you feel about them?

	Strongly Agree	***Agree***	***Neutral***	***Disagree***	***Strongly Disagree***
Give you access to your records whenever you need to make decisions about your treatment	☐	☐	☐	☐	☐
Giving those who treat you 24hour access to your health records to make	☐	☐	☐	☐	☐

decisions about your treatment					
Enable you at any time to look at your medical history	☐	☐	☐	☐	☐
Enable you at any time to look at your current prescriptions and dosages	☐	☐	☐	☐	☐
Enable you to see your recent test results	☐	☐	☐	☐	☐
Quicker access to your test results	☐	☐	☐	☐	☐
Fewer lost records and/or test results	☐	☐	☐	☐	☐
Allow you to choose who can and cannot see your health records	☐	☐	☐	☐	☐
Enable you to make or change appointments online For GP or hospital visits	☐	☐	☐	☐	☐
Enable you to record your wishes.(i.e. organ donor? Life support?)	☐	☐	☐	☐	☐

Security and Your Records

		YES	*NO*	*Not Sure*
10.	Are you concerned about the privacy and confidentiality of your medical records?	☐	☐	☐
11.	Do you know about the National Health Index	☐	☐	☐

12. Despite the proposed benefits that have been mentioned, there are also some anticipated problems with Electronic Health Records. How do you feel about them?

	Strongly Agree	*Agree*	*Neutral*	*Disagree*	*Strongly Disagree*
Electronic Health Records could increase medical errors	☐	☐	☐	☐	☐
Electronic Health Records could lead to sensitive medical-record information leaking out	☐	☐	☐	☐	☐
Electronic Health Records could allow sharing of your medical information without your knowledge	☐	☐	☐	☐	☐
Electronic Health Records may not have strong enough data security installed into the system	☐	☐	☐	☐	☐

13. The above were potential problems that may face Electronic Health Records, below is a list of problems that are faced by most current online systems not just Electronic Health Records. Do you think these would affect YOUR Electronic Health Record?

	Strongly Agree	***Agree***	***Neutral***	***Disagree***	***Strongly Disagree***
Malicious software (Viruses, Spyware)	☐	☐	☐	☐	☐
Vendor access to the system (Super users) **Vendors are the sellers, suppliers or retailers of the Electronic Health Record system*	☐	☐	☐	☐	☐
Long-term accessibility and storage of information	☐	☐	☐	☐	☐
Deliberate acts to harm the system (hackers, crackers)	☐	☐	☐	☐	☐
Failure to backup of your medical records	☐	☐	☐	☐	☐

Below is an explanation of common computer security terms that are in use today.

- ***Anti-virus software:*** *is a computer program that can be used to scan files to identify and eliminate computer viruses and other malicious software (malware).*
- ***Firewalls****: A firewall is equivalent to a lock on a door. It permits only authorised users such as those with a key or access card to enter. A firewall has built-in filters that block unauthorised or potentially dangerous material from entering the system. It also logs attempted intrusions.*
- ***Restricted system access:*** *this allows only authorised people to access parts of a system, they will not be able to access the whole system, only certain relevant parts of it.*
- ***Audit Trail:*** *a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorised.*
- ***Encryption****: the process of mathematically changing characters into a form that can be read only by the intended receiver. This allows for information to be sent and stored electronically in a secure manner.*

14. Do you think that if the following were implemented your Electronic Health Record would be more secure?

	Strongly Agree	***Agree***	***Neutral***	***Disagree***	***Strongly Disagree***
Anti-virus software	☐	☐	☐	☐	☐
Firewalls	☐	☐	☐	☐	☐
Restricted system access	☐	☐	☐	☐	☐
Audit trails	☐	☐	☐	☐	☐

(so you can see who has been doing what with your record)					
Encryption	☐	☐	☐	☐	☐

15. Do you think Electronic Health Records are a **more secure** method of storage then Paper based records?

Yes ☐ No ☐

Why?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

16. Do you have any other concerns or issues regarding Electronic Health Records? Please feel free to make any comments?

_____
_____
_____
_____
_____
_____

Thank you for completing
the survey

Appendix 5

Adapted Questionnaire

About you

1. My age is: 19 or under ☐ 20-29 ☐ 30-39 ☐ 40-49 ☐ 50-59 ☐ 60-69 ☐ 70-79 ☐ 80 or over ☐
2. Gender: Male ☐ Female ☐

Your Computer Use

	Regularly	*Fairly Regularly*	*Sometimes*	*Seldom*	*Never*
3. I use a computer	☐	☐	☐	☐	☐
4. I use E-mail	☐	☐	☐	☐	☐
5. I use the Internet	☐	☐	☐	☐	☐
6. I buy things over the Internet	☐	☐	☐	☐	☐
7. I use E-banking	☐	☐	☐	☐	☐

Electronic Health Records

8. Before participating in this study had you heard of Electronic Health Records? Yes ☐ No ☐

9. The following are **proposed** benefits to YOU of Electronic Health Records. How do you feel about them?

	Strongly Agree	*Agree*	*Neutral*	*Disagree*	*Strongly Disagree*
Give you access to your records whenever you need to make decisions about your treatment	☐	☐	☐	☐	☐
Giving those who treat you 24hour access to your health records to make decisions about your treatment	☐	☐	☐	☐	☐
Enable you at any time to look at your medical history	☐	☐	☐	☐	☐
Enable you at any time to look at your current prescriptions and dosages	☐	☐	☐	☐	☐

Enable you to see your recent test results	☐	☐	☐	☐	☐
Quicker access to your test results	☐	☐	☐	☐	☐
Fewer lost records and/or test results	☐	☐	☐	☐	☐
Allow you to choose who can and cannot see your health records	☐	☐	☐	☐	☐
Enable you to make or change appointments online For GP or hospital visits	☐	☐	☐	☐	☐
Enable you to record your wishes.(i.e. organ donor? Life support?)	☐	☐	☐	☐	☐

Security and Your Records

		YES	*NO*	*Not Sure*
10.	Are you concerned about the privacy and confidentiality of your health records?	☐	☐	☐
11.	Do you know about the Health Service Executive - Information Technology plan	☐	☐	☐

12. Despite the proposed benefits that have been mentioned, there are also some anticipated problems with Electronic Health Records. How do you feel about them?

	Strongly Agree	*Agree*	*Neutral*	*Disagree*	*Strongly Disagree*
Electronic Health Records could increase medical errors	☐	☐	☐	☐	☐
Electronic Health Records could lead to sensitive health-record information leaking out	☐	☐	☐	☐	☐
Electronic Health Records could allow sharing of your medical information without your knowledge	☐	☐	☐	☐	☐
Electronic Health Records may not have strong enough data security installed into the system	☐	☐	☐	☐	☐

13. The above were potential problems that may face Electronic Health Records, below is a list of problems that are faced by most current online systems not just Electronic Health Records. Do you think these would affect YOUR Electronic Health Record?

	Strongly Agree	*Agree*	*Neutral*	*Disagree*	*Strongly Disagree*
Malicious software (Viruses, Spyware)	☐	☐	☐	☐	☐
Vendor access to the system (Super users) **Vendors are the sellers, suppliers or retailers of the Electronic Health Record*	☐	☐	☐	☐	☐

system					
Long-term accessibility and storage of information	☐	☐	☐	☐	☐
Deliberate acts to harm the system (hackers, crackers)	☐	☐	☐	☐	☐
Failure to backup of your medical records	☐	☐	☐	☐	☐

Below is an explanation of common computer security terms that are in use today.

- ***Anti-virus software:*** i*s a computer program that can be used to scan files to identify and eliminate computer viruses and other malicious software (malware).*
- ***Firewalls****: A firewall is equivalent to a lock on a door. It permits only authorised users such as those with a key or access card to enter. A firewall has built-in filters that block unauthorised or potentially dangerous material from entering the system. It also logs attempted intrusions.*
- ***Restricted system access:*** *this allows only authorised people to access parts of a system, they will not be able to access the whole system, only certain relevant parts of it.*
- ***Audit Trail:*** *a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorised.*
- ***Encryption****: the process of mathematically changing characters into a form that can be read only by the intended receiver. This allows for information to be sent and stored electronically in a secure manner.*

14. Do you think that if the following were implemented your Electronic Health Record would be more secure?

	Strongly Agree	***Agree***	***Neutral***	***Disagree***	***Strongly Disagree***
Anti-virus software	☐	☐	☐	☐	☐
Firewalls	☐	☐	☐	☐	☐
Restricted system access	☐	☐	☐	☐	☐
Audit trails (so you can see who has been doing what with your record)	☐	☐	☐	☐	☐
Encryption	☐	☐	☐	☐	☐

15. Do you think Electronic Health Records are a **more secure** method of storage then Paper based records?

Yes ☐ No ☐

Why?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

16. Do you have any other concerns or issues regarding Electronic Health Records? Please feel free to make any comments?

_____
_____
_____
_____
_____
_____
_____

Thank you for completing
the survey