Electronic Patient Records:
An Investigation into Issues Surrounding Privacy, Confidentiality and Data Protection

Katherine Flanagan

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

2006

Declaration

I declare that 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: _____

Katherine Flanagan

12th September 2006

Permission to lend and/or copy

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

Signed: _____

Katherine Flanagan

12th September 2006

Acknowledgements:

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

Mary Sharp, for her excellent supervision, guidance and advice.

Ian Brennan, for his constant counsel and encouragement, which gave me the confidence to pursue this course of study.

My employer, Bon Secours Hospital Cork, for facilitating and allowing me the time to complete this study.

My work colleagues, for their help and support over the last two years.

My family and many friends, for their constant good humour and patience.

And finally, my fellow Health Informatics students, who were always a source of inspiration.

.

Summary

The proliferation of information and Communications Technology (ICT), particularly in the health arena will ultimately mean that medical records, which have traditionally been stored on paper, will be stored electronically. Thus, the Electronic Health Record (EHR) has become the 'Holy Grail' for Health Informaticians worldwide. While the EHR will improve the delivery of healthcare, it also poses some serious threats to the confidentiality and privacy of patients' personal health records.

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 professional health carer. With the infiltration of ICT, governments and other organisations have implemented guidelines and legislation in an effort to address the issues of privacy and confidentiality in the information age.

This dissertation set out to examine the EHR from the viewpoint of privacy, confidentiality and data protection. The author undertook two studies; examining the subject, firstly, from the perspective of the Health Organisations where the EHR's were implemented; and secondly, from the patient's viewpoint.

Findings from the research undertaken suggest that although organisations are adhering to the guidelines and legislation that is in place, there is opportunity for improvement, particularly in the areas of access attributed to casual staff, audit trails, and patient information and consent.

Findings from the patient survey, display a certain level of confusion and ambiguity amongst patients, with the majority of patients being both unconcerned and unaware of their rights pertaining to the privacy and confidentiality of their personal health records. The majority of patients rejected the use of a unique identifier, which is a necessary precursor to implementation of the EHR.

TABLE OF CONTENTS

TABLE OF FIGURES

ABBREVIATIONS

ICT	Information and Communications Technology
EHR	Electronic Healthcare Record
EHCR	Electronic Health Care Record
PHR	Personal Health Record
EPR	Electronic Patient Record
EMR	Electronic Medical Record
CPR	Computerised Patient record
HIPPA	Health Insurance Portability and Accountability Act
OECD	Organisation for Economic Co-operation & Development's
PIPEDA	Personal Information and Electronic Documents Act

1 INTRODUCTION

1.1 Background

Respect for patient privacy and confidentiality has been enshrined as a professional responsibility of the health care professional since ancient times, with pledges to protect privacy and confidentiality being a standard feature of medical oaths and codes of ethics. In the famous oath attributed to Hippocrates, which is still used by the medical profession today, ancient Greek physicians pledged to respect confidentiality with the words *'What I may see or hear in the course of the treatment, or even outside of the treatment in regard to the life of men, which on no account may be spread abroad, I will keep to myself, holding such things shameful to be spoken about'* (Hippocratic Oath). Comparable statements have been included in the codes of ethics of nurses, dentists, and other health professionals ever since (Gorlin, 1999), for example, An Bord Altranais (The Nursing Board), stipulates that information regarding a patient's history, treatment and state of health is privileged and confidential and that the confidentiality of patient's records must be safeguarded at all times (An Bord Altranais, 2000).

Health care professionals deal with patient information, which is given to them in trust, every day. Patients providing the information expect that it will be treated confidentially and kept private. Generations of health care professionals have managed to maintain high standards of confidentiality and sustain the trust and confidence of those patients they provide care for, but the manner in which data is collected, stored and used is rapidly changing.

We are living in an era where Information and Communications Technology (ICT), particularly health informatics is growing rapidly. Health organisations, which have traditionally stored medical records on paper, are advancing towards storing them electronically. While the prospect of an Electronic Health Record (EHR) offers enormous benefits to the health care professional, the patient and the public at large (Grimson, Grimson & Hasselbring, 2000; Rindfleisch, 1997; Waegemann, 2003), it also brings with it greater threats to the privacy and confidentiality of personal health information (Chhanabhai et al, 2006; Mulligan, 2001; Kerr, 2004;

Anderson, 2001). Incidences of inappropriate access to paper records, while always serious are usually confined to a small number of records, however, the risks associated with inappropriate access to electronic records have the potential to be catastrophic due to the large volumes of records that can be accessed.

The proliferation of ICT since the 1970's has also lead to a greater awareness of the risks associated with the improper use of personal data. The ability of powerful computer systems to process large volumes of information has prompted countries to develop to specific rules to govern the collection, storage, use and disclosure of personal information. This has resulted in an increase in the legislation and standards that have been developed to protect personal data.

As a health care professional in an organisation, which is working towards implementing a complete EHR, the author has a personal interest in the area of patient privacy and confidentiality. The author believes that patients have a right to expect that their personal health information is collected, stored and treated confidentially, and is not shared with any other person or organisation without the patient's full knowledge and consent. It is important that we acknowledge the threats to privacy and confidentiality and attempt to balance these risks with the benefits. With the appropriate legislation in place, the EHR if properly implemented and safeguarded, has the potential to protect patient information, ensuring that patients can engage with their health care professionals confident in the knowledge that their personal data is safe and secure.

In this dissertation the author will explore the state of the art, looking at current thinking and practices relating to the protection of privacy and confidentiality, specifically in relation to the EHR. She will carry out research among international organisations, where an EHR has been implemented to identify their practices relating to the protection of patient data. She will also undertake a study amongst patients to identify their knowledge, views and experiences surrounding the confidentiality and privacy of their personal health information. Finally, the author will reflect on her dissertation, and offer some interpretation and recommendations ensuing from her work.

1.2 Objectives of the Study

- To review the state of the art to establish current thinking, practices and legislation in the area of privacy and confidentiality of medical records, particularly electronic medical records
- To undertake research in organisations where an EHR has been implemented and to establish:
    - What data is distributed to outside organisations?
    - What procedures each organisation has in place to protect electronic patient information?
    - What policies are in place to guard against unauthorised access to electronic patient information?
    - What measures are in place to protect the privacy of data stored in Electronic Health Records?
- To undertake research among patients to establish:
    - Patients' concerns regarding their personal health information.
    - If patients practice 'privacy protecting behaviour'.
    - If patients support the use of unique patient identifiers.

1.3 Thesis Structure

Chapter 2: Is a review of the literature, outlining the evolution of the EHR, its advantages, barriers, and particularly, privacy and confidentiality as a barrier.

Chapter 3: Outlines the legislation and standards that exist in relation to privacy and confidentiality of electronic health records.

Chapter 4: Describes the methodology used to undertake this study.

Chapter 5: Analyses the results of the EHR questionnaire

Chapter 6: Analyses the results of the questionnaire distributed to patients.

Chapter 7: Discussion

Chapter 8: Conclusion

2 LITERATURE REVIEW

2.1 Medical Records

Medical records are collections of data, which are used to record, diagnose and treat patients' health problems. Patients' medical history, current illness, diagnosis, laboratory and x-ray results, details of treatments and medications, chronological progress notes by clinicians, nurses and therapists, as well as discharge recommendations are all documented in the medical records. Healthcare professionals, administrative staff, researchers, patients, legal advisers, hospital planners and commercial product developers, all use medical records which are legal documents which patients are entitled to read, and are authenticated by the physician's signature. There are strict rules regarding their confidentiality. Amongst other things medical records:

- Are a chronological account of interventions and care given
- Are a means of communication between healthcare professionals
- Provide a single access point for relevant active data about the patient
- Act as a source of information to support administrative functions
- Provide material to support research

Traditionally all medical records have been recorded on paper, in single folders or manila binders called 'the chart' with the patient's identification data on the cover. It is usual for each patient to have several charts in a lifetime, each one stored and maintained at a different location. The patient's GP maintains one file, any consultant that the patient may consult; i.e. cardiologist, gynaecologist, orthopaedic surgeon, each has a separate chart, and any hospital that the patient has ever visited has another chart of its own. In addition, each chart will have its own unique identifier.

Schoenberg & Safran (2000) stated that a patient's medical record has always been a 'dispersed entity' and that literally defined, it is the accumulation of medical information concerning the patient. In an ideal setting, all the patients' information is bundled together in a single folder with the patients' identification on the cover.

In real life, this information is scattered between several archives in various locations, often under different identification numbers.

In addition to the obvious problem of storage, there are also many other documented problems associated with the traditional paper based medical record. Barrows & Clayton (1996) describe the inability to allow an accurate audit trail of who has seen the record and what portions of the record were accessed; difficulty in restricting certain classes of users to see only particular types of information; the ease at which records can be altered by removal or substitution of documents; the fact that they can only be in one place at any one time, and the fact that they are costly to pull from the medical records department for each patient visit, as major disadvantages. Bakker (1998) concurs and highlights the limitations; information is available only at one location, records are 'fixed structures' and are therefore difficult to sort or analyse systematically, and they are difficult to read.

Traditionally the institution where the record was created, be it the hospital, GP surgery, or the health centre, has been perceived as owner of the medical records. Access to the traditional paper record was therefore to a large degree tightly controlled. In order to gain access to the medical record the patient had to write to the institution to request a copy of their notes, or was required to present themselves to the medical records department. Another individual would need to have a legitimate reason to access an individual patient's medical record. There was therefore a relatively low risk that a patient's medical record would be available to an unauthorised individual (Veroesi, 1999). Bakker (1998) however does not agree, arguing that the traditional medical record also poses risks:

- Access to the record is not restricted in some instances, and it is possible for unauthorised persons, e.g. a person posing as a doctor to access patients notes
- Reports are often distributed in an insecure manner
- Data and even in some cases, complete files get lost
- Data is difficult to read, so they may be misinterpreted
- Data is not always at the place where they are needed

Due to the proliferation of ICT in the area of healthcare, the traditional paper based medial record is slowly being replaced by electronic versions, with the electronic healthcare record being seen as the ‘holy grail’ of health informatics.

2.2 Privacy

‘When all is said and done, will our medical records be used to heal or reveal us?’ (Shalala, 1997).

According to Lennon (2005), the concept of privacy has been around since biblical days, however, it is still probably the most difficult of all human rights to define and limit. The Oxford English Dictionary defines it as ‘a state in which one is not observed or disturbed by others’, but perhaps the simplest definition is given in a paper entitled ‘The Right to Privacy’, where Brandeis & Warren (1890) quoted Judge Cooley’s defined of privacy as ‘The right to be left alone’.

In the UK, the Calcutt Committee defined privacy as ‘the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information’ (Calcutt, 1990). In Ireland, the Law Reform Commission, when considering why privacy was deserving of legal protection concluded that ‘Privacy is not merely instrumental to the achievement of other goals, but is a basic human right that applies to all persons in virtue of their status as human beings’ and ‘As such, it is now universally recognised as a human right, and is to be distinguished from other interests such as secrecy and confidentiality’ (Law Reform Commission, 1998).

Clarke (2000) describes the key aspects of personal privacy concerns as being issues concerning the privacy of the person; the privacy of personal behaviour; the personal right to communicate freely; and the right of the person to control data about themselves. Privacy can be viewed therefore as a fundamental (though not an absolute) human right, deserving of legal recognition and protection. Most people consider health information to be highly personal and, therefore, need to be confident that their privacy will be protected whenever they use a health service (Lennon, 2006).

Information Privacy is the interest that an individual has in controlling, or at least significantly influencing, the handling of data concerning him or herself (Clarke, 2000), or the ‘claim of individuals, groups or institutions to determine when, and to what extent information about them is communicated to others’ (Agranoff 1993). Therefore it can be seen that definitions of privacy have evolved to incorporate both the direct aspects and associated factors associated with privacy.

2.3 Confidentiality

Confidentiality is closely related to privacy, but the two are not identical. The Oxford English dictionary defines ‘confidential’ as ‘intended to be kept secret’ and ‘entrusted with private information’ Confidentiality therefore refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. The rules of confidentiality are observed out of respect for, and to protect and preserve, the privacy of others (University of Miami, 2005). Manning (1997) claimed that confidentiality is the ‘sine qua non’ of the physician-patient relationship, and it is the rules of physician-patient confidentiality and other related doctrines that protect one's privacy. Confidentiality is a significant mechanism by which a patient's right to privacy is maintained and respected.

Gostin et al (1993) distinguishes between confidentiality and privacy. His definitions are as follows:
Privacy is information about a person, which is beyond the range of others without specific authorisation and the individual has the right to limit access by others to personal information.
Confidentiality is a form of informational privacy characterised by a special relationship, such as the physician – patient relationship. Personal information obtained in the course of that relationship should not be revealed to others unless the patient is first made aware of and consents to its disclosure

For the general public however, confidentiality means privacy, and refers to keeping information about yourself to yourself unless you choose otherwise. Confidentiality is a foundational principle of medical ethics, with physicians

pledging never to reveal the secrets in the Hippocratic oath. Patients therefore expect that information they share with their doctor in the context of receiving proper medical attention will be treated as confidential. This view is demonstrated in an American qualitative study carried out to identify patients' views and understanding of medical confidentiality, where participants identified confidentiality as an expectation that something said or done would be kept private (Jenkins, Merz & Sankar, 2005).

The importance therefore of privacy and confidentiality with respect to the patient – doctor relationship cannot be underestimated. Our medical records hold some of our most intimate and private information. Medical records can reveal a history of drug abuse, a venereal disease, or a life-threatening illness. Psychiatric notes reveal inner fantasies, sexual peccadilloes, crimes, or the crimes and abuses of family members. The information from genetic tests can reveal not only that a patient is susceptible to some disease, but that her children and other family members are susceptible as well. If medical records are revealed, a person can lose their insurance, their job, or even their marriage (Stein, 1997).

Braunack-Mayer & Mulligan (2003) also highlighted the importance of confidentiality stating that it:

- Benefits the patient by providing a secure environment in which they are most likely to seek medical care, and give a full and frank account of their illnesses
- Supports public confidence and trust in healthcare services
- Expresses respect for patients' autonomy, allowing them to choose who will have access to information about them, and to determine who will be privy to their secrets

The arguments for maintaining confidentiality was reiterated by the same authors in 2004, when they stated that confidentiality confers a number of practical benefits by shielding patients from harm, which might flow from disclosure of health information, and encouraging patients to be candid with their health care providers (Mulligan & Braunack-Mayer, 2004).

2.4 The Electronic Health Record

The concept of the EHR has been around since the 1960's, however, there were very few EHR systems implemented anywhere until the 1980's, and the uptake of EHR's is still very low in most countries, with the exception of a few countries in Europe (Schloeffel, 2004). Although the US is a leading country in ICT generally, the fact that the health system there is predominantly private has led to many disparate systems, thus acting as a barrier to the introduction of a national EHR. Uptake has been more successful in countries like the Scandinavian countries, the Netherlands, and Belgium.

The EHR therefore remains the 'holy grail' for those working in the area of health informatics, with the development of a national EHR being a priority for governments in many countries at the moment. National initiatives are currently underway in the UK, Australia, New Zealand and Canada. In Ireland the Government document 'Health Information – A National Strategy' (DHC, 2004) has also indicated that a national EHR would be developed, implemented and rolled out nationally.

However, the EHR should not be seen simply as a replacement for the paper–record, but more a way in which to create a new concept of a virtual, distributed, and complete healthcare record, providing a single access point for relevant, concise, and active data about a patient, which would be readily available to authorised users for patient care, administration, clinical and financial audit, and research and education. Terry (2004) states that the EHR will fundamentally change the way patient data are acquired, stored, aggregated, processed, accessed and distributed.

While EHR is accepted globally as the generic term for the vision of the electronic patient care systems, the terminology used to describe the EHR varies and the concept for the EHR is sometimes described using the following acronyms interchangeably:

- EHCR Electronic Health Care Record
- PHR Personal Health Record

- EPR Electronic Patient Record
- EMR Electronic Medical Record
- CPR Computerised Patient record

Many different definitions have evolved for the EHR since its conception. Neame (1996) defined the EHR as ‘a confidential record that is kept for each patient by a healthcare professional or organisation, containing the patient’s personal details (such as name, address, date of birth), a summary of the patient’s medical history, and documentation of each event, including symptoms, diagnosis, treatment and outcome. Relevant documents and correspondence are also included’.

The NHS description of an EHR is ‘a longitudinal record of patient’s health and healthcare – from cradle to grave. It combines both the information about patient contacts with primary healthcare as well as subsets of information associated with the outcomes of periodic care’ (NHS 2001).

The Centre for Health Informatics, (2002), defines it as ‘an integrated longitudinal record of individual patients demographics, health care interventions, illnesses and accidents from cradle to grave. The health record data is stored electronically and can be readily retrieved by authorised users. The EHR allows easy access by authorised healthcare personnel in different locations and sectors according to the data protection regulations’.

The Australian National Electronic Health Records Taskforce defined an EHR as ‘an electronic longitudinal collection of personal health information usually based on the individual, entered or accepted by health care providers, which can be distributed over a number of sites or aggregated as a particular source’ (Terry, 2004).

While it appears that there are many definitions for the EHR, when examined, they are all similar in their purpose, function and goal. All definitions refer to the longevity, completeness, and shared-care aspect of the record, which would be accessed by authorised users. It is the goal of so many working in the area of

Health Informatics to produce an all-encompassing system to effectively capture and access all significant healthcare data for all patients in the health system.

For the purpose of this dissertation, the author has applied the **ISO** definition, which states that:
'*the EHR is 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'* (ISO, 2005).

The author choose this definition as it is broadly applicable to all health sectors, professional health disciplines and methods of health delivery, and it focused on the content, privacy, security and shareability of the EHR, which is the area of interest to the author. The author believed that the ISO definition allowed most scope to include as many organisations as possible in the survey.

2.5 Benefits of the EHR

Although paper records can be easily browsed, and are directly accessible, portable and self-contained, they are also seen as fragmented and cumbersome, lacking in structure, fragile and degradable, illegible, incomplete, inaccurate and can only be accessed by one person at any given time. The institute of Medicine in the US also identified 'illegibility, poor organisation, incompleteness and poor availability as being weaknesses of the paper record' (Meijden et al, 2001). These problems among others have lead to the evolution of the EHR.

The concept of the longitudinal, complete EHR, which allows appropriate access to authorised personnel, provides many benefits to the patient, to the clinician, and to the public in general, with many pieces of research available, which support this belief. Rindfleisch (1997) considers that implementation of an EHR has the ability to improve health care through timely access to information and decision support aids, while allowing doctors, nurses, and the multidisciplinary team to access records simultaneously, thus improving cost effectiveness based on analyses of outcomes and utilisation of information, and the need for better support of clinical research.

Grimson, Grimson & Hasselbring (2000), agree, stating that the advantages of the EHR over its paper-based counterpart are clear- it is always available, information can be transferred, and it can support different views of the record for nurses, doctors and other users. In a survey carried out by the Medical Records Institute, Mass. USA, 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 were given as benefits of EHR's (Waegemann, 2003). One of the most important benefits to be gained from EHR implementation is the reduction of medication errors. According to the Institute of Medicine, up to 98,000 Americans die each year from medical errors resulting from incomplete or incorrect health records. It is estimated that this could be reduced by up to 90% with a correctly monitored EHR (Chhanabhai, Holt & Hunter, 2006). Hodge, Gostin & Jacobson (1999), and Waegemann (2003) also claim that the reduction of medication errors is seen as a major advantage to the EHR.

Hodge, Gostin & Jacobson (1999) highlighted the benefits of the EHR to the consumer, by allowing them to make more informed choices about health providers, products and treatments, improving clinical care through faster and more accurate diagnoses, making instantaneous research of medical conditions possible, as well as disseminating of expert medical information to areas that have traditionally been underserved. Rothstein & Talbott (2006) support this view, adding that the EHR will permit real-time public health surveillance, allow for distribution of evidence-based standards of care tailored to each patient, and will facilitate outcomes research.

The Consumers Association in the UK also highlighted consumer benefits, claiming that there would be:

- More information available about the relative performance of doctors
- Fewer lost records
- More research leading to new treatments
- Shorter waits for treatments (NHS, 2002).

The EHR benefits the clinician, by saving time in obtaining patient histories, allowing prescriptions to be written electronically with greater accuracy, thus reducing medical errors, and easing co-ordination of care (Rothstein & Talbott 2006)

In Ireland, The National Health Strategy outlined increased patient safety, better access to services, better planning, more efficient services, cost effectiveness, better availability, transfer and retrieval of information, decision support, multiple views, quality and standards, improved clinical support, health surveillance, and health promotion among the potential advantages of a national EHR (DHC, 2004).

Some of the above benefits could have been realised in Ireland, where the investigation into Dr Michael Neary in Drogheda, highlighted the fact that over 40 patients' medical records have gone missing. One would question if this could have happened had an EHR been operating in the hospital at the time.

2.6 Barriers to the EHR

Despite the many advantages of the EHR that have been outlined, uptake in general has been slow, for a variety of different reasons, and there are some well-documented problems associated with its implementation. Clinical users can be lacking in confidence with regard to their computer skills, making it difficult to bring them on board, IT projects are complex to implement, and the requirement for business management and procedural changes, along with associated data entry problems are all obstacles that are encountered. Technology immaturity, health administrator focus on financial systems, application unfriendliness and physician resistances were all barriers to acceptance during the earlier time period (Berner et al, 2005).

Barrett (2000) and Kerr (2004) have both identified the need for standard or universal clinical terminology as a precursor to the implementation of the EHR. However, despite much discussion about the issue, there is still no single descriptive system. Coding schemes such as ICD-9 cm, SNOWMED and CPT have gone a long way towards providing a standardised coding system but much still needs to be done to make them effective.

The absence of standardised terminology and outcomes has also resulted in confusion over what data should be collected, let alone how frequently and in what format. End users, and clinical researchers therefore don't know what data has value**.** As a result, organisations have tended to automate their paper forms without considering the value of the specific data or how best to collect it for monitoring and reporting uses (Barrett, 2000).

Protocols and pathways have been widely accessible for some time. However, universal acceptance of a source has not been attempted, thus inhibiting the implementation of EHR's (Barrett, 2000).

Kerr (2004) identifies the challenges associated with data entry into EHR's by health providers and both Kerr (2004) and Schloeffel (2004) identify the difficulties of integrating EHR's with other sources of information, and interoperability as obstacles to the deployment of the EHR.

All these problems need to be tackled before an EHR can be implemented successfully.

2.7 Privacy and Confidentiality as a Barrier

'Unauthorised access to paper records was always feasible, but the computer takes a small problem and has the potential to magnify it enormously' (Chhanabhai et al, 2006).

Medical information is among the most personal and sensitive information recorded, collected and shared with another person. The author believes that it is imperative that patients' privacy is respected and that information shared with their doctor or other healthcare professional is treated confidentially.
However, it is well documented (Adams et al, 2004; California HealthCare Foundation, 2005; Carman & Britten 1995; Harris Interactive inc, 2005; Pyper et al, 2004; Flynn et al, 2003; Mulligan, 2001; O' Brien & Chantler, 2003) that patients have fears about their privacy being violated with respect to their medical records.

As already mentioned, where medical records are paper-based, privacy and confidentiality are always considered to be significant issues (Bakker 1998). Paper charts are not always securely located on wards or other clinical settings**,** and in some instances all a person needs is a 'white coat' to access records through the medical records department. Having said this however, if there is a breach of confidentiality, damage in the paper system is generally incidental, relating only to one patients chart or to a 'bundle' of patients' charts. However, when considering the EHR, this outcome is somewhat different, with the effects being enormous and systematic.

Where an EHR is implemented therefore, confidentiality and privacy become more complex issues. Having patients' records available electronically creates an environment where it is possible to access sensitive patient data, from any computer that is linked to an EHR network. Information technology can offer a higher level of security, but breaches of this security can have much greater consequences. Unauthorised users can then access, copy, alter, delete, or distort hundreds or thousands of medical records within minutes (Waegemann, 1996).

These views are substantiated by Neame (1996) who claims that health records stored on paper are perversely secure because of the fundamental difficulty of accessing and searching them, and this hinders their usefulness both to users and to abusers who might breach their confidentiality. However, where records are stored in computerised information management systems, they become more accessible so creating the potential for wider and more systematic abuse of personal privacy. This is further increased when the systems are regional, national, and global systems. Barrows & Clayton (1996) concur that the potential confidentiality breaches are greater in an EHR, where health data is pooled from multiple sites in a central repository, than with either paper records or isolated EMR systems.

As Chhanabhai et al., (2006) highlighted, one of the functional disadvantages of a paper based records system can also be seen as an advantage: its sheer volume when stored makes it difficult for someone to access a large number of records.

It was recognised by the end of the 1970's that one of the major negative effects of ICT in health care was access to patient data by unauthorised persons (Bakker, 1998), thus putting patient privacy and confidentiality at risk. It is therefore not surprising to learn that patient concern about the privacy and confidentiality with respect to their health information is obstructing the establishment of an EHR in many instances. Kerr (2004) identified data privacy, confidentiality and security issues as being barriers to implementation of EHR's in New Zealand and Australia.

The introduction of the EHR in the NHS was delayed by several years when it became evident that the HIV status of a patient would become part of the minimum dataset that would be accessible not only by clinical staff but also by administrative and clerical staff (Basu & Sriskandabalan, 1996). This fact caused much concern, undermining confidence in confidentiality of the NHS networking that it delayed the introduction of technology into the NHS by several years (Anderson, 2001).

Electronic patient records have many advantages, however, personal data can be used and misused in ways that may have devastating consequences for the

financial emotional or security interests of the patients (Ilene & Goldberg, 2002). It is these issues that concern the author and she intends to focus her project on the area of patient confidentiality, privacy and data protection in relation to the EHR. The author has a personal interest in this area, and strongly believes that confidentiality of health information is a basic human right and that patients should be guaranteed that their health information will be kept private at all times. The author will question how patient privacy and confidentiality is dealt with in organisations where an EHR has been introduced, as well as patient concern and knowledge with respect to privacy and confidentiality of their medical records.

2.8 Patients' Perceptions

There have been a number of studies carried out which examine how patients perceive confidentiality in relation to their medical records, and while attitudes vary it is evident that privacy and confidentiality is considered to be important. Some studies would suggest that patients are not concerned about confidentiality, and are unaware that their medical information is shared at all, while other studies show that patients are indeed concerned.

In an online US survey, most patients surveyed were not concerned about the confidentiality or privacy of their medical record (Hassol et al, 2004). In South Staffordshire, a pilot project was undertaken to ascertain if patients were concerned about the use of their health information in an EHR, and were offered the option to have their record excluded for the study. The study found no evidence that people were seriously concerned about their information being shared, and there were no requests from patients wishing to be excluded from the study (Adams et al, 2004). Despite a large local publicity campaign informing patients about the project, this author considered it interesting that the study also found that only 38% of those interviewed were aware of the project, and of these only 15% understood that they had an option to opt out. These statistics would suggest lack of knowledge and interest in privacy of personal health records among the patients interviewed.

Most other studies however, suggest that the public do have confidentiality concerns. Studies have shown that the public are concerned that computerised systems allow too many people easy access to their health records. A 1999 survey undertaken by the California HealthCare Foundation found that 67% of Americans were concerned about the confidentiality of their personal health information and were largely unaware of their privacy rights, A repeat study by the same foundation in 2005 after the implementation of the Health Insurance Portability and Accountability Act (HIPPA), suggested no major improvement in the statistics (Forrester Research, 2005). Carman & Britten (1995) found when they surveyed patients in a general practice, that patients expected nurses and medical students to have limited access to patient medical records, and clerical staff to have no

access at all. Some patients also had reservations about a doctor not involved in their medical care having access to their records. Respondents to a survey in Sheffield, UK, concur with this opinion. That survey found that a significant minority (11.6%) of respondents were unhappy with personnel not directly involved in their medical care having access to their health records (O' Brien & Chantler, 2003).

In a study of patients accessing their medical records on-line for the first time, it was found that patients have strong views on what they find acceptable regarding access to electronic records and that they were concerned about security and confidentiality, including the potential exploitation of records (Pyper et al, 2004). Research carried out by the consumers association in conjunction with the NHS; found that 60% of respondents would not restrict access to any of their health record. However, in this survey, a significant minority said they would restrict access to some of their record to their GP (9%), and 17% said they would restrict access to their hospital doctors, and nearly half said they would restrict access to some of their record by other health professionals. In addition, people surveyed were not happy with receptionists or private data processing companies having access to their EHR. Respondents believed that information for care should be shared on a need to know basis, and ability to isolate some particularly sensitive information from routine sharing should be possible with an EHR (NHS, 2002).

These findings were similar to a survey carried out in the US to ascertain how the public sees Health Records and the EHR Programme. 56% of those surveyed displayed concerns about privacy of medical information and 47% believed that privacy risks associated with the EHR outweighed the expected benefits (Harris Interactive inc, 2005). A study which compared psychiatric patients who refused to have their records transferred to and electronic format with those who did not, found that a majority a patients reported numerous concerns about electronic records, with 90% have concerns about unauthorised access of their records by persons outside the hospital. All patients had concerns about the use of information contained in the record, stigmatisation, and the security of the electronic record system (Flynn et al, 2003).

In a study in South Australia, to determine attitudes towards doctors and hospitals as data custodians, it was found that 9.6% of those surveyed were not confident that healthcare providers keep and use information responsibly. Many Australians believe that there is less privacy now than there was previously and that computers have made it easier for confidential information to fall into the wrong hands (Mulligan, 2001). A survey carried out in New Zealand, found that although patients were willing to have their health information shared amongst health professionals, they were unwilling to have information viewed by administrators, researchers and government departments. They were also more likely to allow their information to be shared where the information was anonymous and more willing to share information of a less personal nature. Findings also suggest that the respondents prefer to be consulted about the distribution of their information. (Whiddett et al, 2006).

The literature would suggest that although most patients are in favour of their health information being available / shared, a significant minority have concerns over what information is shared and want to have control over who has access to some or all of it. Patients are willing to allow information from their medical records to be used for research, but most prefer to be asked for consent either verbally or in writing (Wilson et al 2003). It would also appear that the more sensitive the information the less likely patients are to share it. The 'Share with Care' report (NHS, 2002), identified that patients are less likely to share information of a confidential / sensitive nature, such as termination details, sexual health details, mental health details, and are more likely to agree to shared their information once it remained anonymous.

2.9 Implications for Patients

Research has shown that patients who believe or who are worried that their privacy is being violated act in certain ways; they avoid or delay seeking medical treatment, they withhold information or they lie about their illness or lifestyle. The California HealthCare Foundation (2005) refers to this as 'Privacy Protecting Behaviour'. Jones (2003) found however, that although it is usually assumed that patients consider confidentiality to be important and that they would be less likely

to seek treatment if this were not assured, few studies have actually asked patients' directly. In addition, research in this area has been undertaken to a large extent within certain groups such as psychiatric patients, adolescents, HIV patients, and patient with genetic disorders, rather than random studies of the general public.

Psychiatric patients expressed significantly more concerns about confidentiality than did patients with a physical illness (Mechanic & Meyer, 2000). This is possibly due to the stigma attached to mental illness, and the perception among patients that they may suffer embarrassment should their illness become known. Adolescents also rank highly as a group who delay or avoid seeking medical attention due to confidentiality concerns. It was found that 25% of high school students reported that they would forego seeking medical care rather than risk information disclosure to their parents. Those who sought healthcare did not seek it from their family practitioner (Cheng et al, 1993). Woods & McNamara (1980) also found that undergraduate students were more likely to reveal personal information in scenarios where confidentiality was assured. A more recent study by Carlisle et al (2006), also confirmed that concern over confidentiality might discourage adolescents from consulting their doctors.

Clamp, Felton & Heatherfield (2001), who studied patients' views on confidentiality, found that overall patients' valued confidentiality, and that patients might be deterred from seeking treatment if it were not guaranteed. Studies have also found that patients will withhold information when they are worried about confidentiality. Moneyham et al (1996) in their study examining disclosures of women infected with HIV found that many women withheld their diagnosis from their doctors because they did not trust him or her to keep the information confidential. Marks et al (1995) found that HIV patients withheld information because they feared refusal of treatment or discrimination. Without a guarantee of confidentiality, patients will lie to their doctors about lifestyles and genetic risk factors, delaying important clinical decisions and driving up health costs (Ilene & Goldberg, 2002).

Holahan & Slaikeu (1986) found that fears of loss of confidentiality could be 'devastating' to the treatment of patients receiving psychotherapy. It is therefore important that patients who require medical attention are not discouraged from seeking it because of the fear of confidentiality or privacy breaches. By withholding important information or delaying seeking medical attention, patients put not only their own health, but also the health of the general public at risk.

2.10 Breaches of Confidentiality

Do the public have reason to be worried about privacy and confidentiality when their medical records are stored in an EHR? The author would suggest that they have. The literature has many examples of instances where patient privacy and confidentiality has been breached, both from inside and outside the organisation.

2.10.1 Accidentally from Inside the Organisation

This occurs when somebody with legitimate access to the patient record does not take due care with patient data, and patient information may be released accidentally. Breaches of confidentiality in such instances are due to carelessness and are not malicious, as occurred when the Harvard Community Health Plan entered psychiatrists' detailed notes from patient sessions into computerised records that were accessible to hundreds of clinical HMO employees (Anderson, 2000), and also in the Michigan Medical Centre where thousands of patient records were left exposed to the public on the Internet for two months (Anderson & Carter 2000). Public access was only terminated after a news reporter notified the medical centre. The University of Montana attributed 'human error' as the reason why 400 pages of patient records which included names, dates of birth and address, and describing care provided by therapists to patients with mental retardation, depression and schizophrenia were posted on the Internet (Layman, 2003).

2.10.2 Maliciously from Inside the Organisation

Malicious breaches of confidentiality can occur when somebody with legitimate access to patient records abuses their access privileges in search of gossip

material, and knowingly passes information to a third party. These occurrences are usually financially motivated. This happened in the US, when a member of a state health commission, who also worked in a local bank, printed out a list of cancer patients, cross referenced it with a list of bank customers with callable loans, and then called in the patient loans (Ohno-Machado, Silveira, & Vinterbo, 2004). Again in the US, a Florida state public worker brought home a computer disk with the names of HIV-positive patients and sent the names to two Florida newspapers. A total of 4,000 names were released and printed in newspapers (Chhanabhai Holt & Hunter 2006; Ilene & Goldberg, 2002).

In 1992, the U.S. representative Nydia Velazquez had her hospital records accessed and forwarded anonymously to the press, when she was running for congress. The New York Post broke the story, and Velazquez was forced to acknowledge publicly that she had attempted suicide, which was something even her family did not know (Gorman, 1996).

2.10.3 Malicious Intrusion from Outside the Organisation

Breaches of confidentiality also occur from outside the organisation, when somebody 'hacks' into the organisations records for malicious reasons. This happened in the US when a government's database was accessed by a computer hacker who subsequently used the information to carry out heinous sexual crimes (Chhanabhai, Holt & Hunter, 2006). There is also an example of hackers breaking into a hospital's computer system, changing patient cancer tests from positive to negative, and altering CT scans causing patients' surgery's to be delayed (Layman, 2003). In the UK, The Foundation for Information Policy Research (FIPR), suggested that over 200,000 attempts are made every year to get health information on patients, by investigators who call up pretending to be doctors or administrators (FIPR, 2003).

2.10.4 Organisations to whom Data has been Distributed

Beaches of confidentiality can also occur where patient data that has been legitimately distributed to an outside organisation, such as the patients' employer, insurance company or pharmaceutical company, and the data is used inappropriately. This data could be used to bombard patients with commercial

advertisements, or employers and insurance companies could discriminate against patients based on information they have received.

Examples of this can be been seen in the already proliferating misuse in the sale of consumer information to pharmaceuticals companies, thus when individuals have prescriptions filled, they may find themselves receiving mail from companies promoting different medications, treatment or equipment. In the US it was found that several chain pharmacies were selling patient-specific information on prescriptions to a number of drug companies, including Glaxo, Wellcome, Warner-Lambert, and Merck. Companies were then using this information to encourage patients to refill prescriptions with their drugs (Carter, 2000).

There is also well-documented evidence to support the fact that insurance companies are refusing to sell insurance, and employers are discriminating against employees due to information gleaned from electronic health records. For example one woman was denied life insurance when the insurance company learned that her family had a history of Huntington's chorea even thought the woman herself had not been tested for the order. Another company refused to hire a 53-year-old man who had a history of haemochromatosis, even though the condition was asymptomatic (Anderson, 2000). In 1996 a group of people with genetic predisposition to certain diseases reported discriminatory actions made by insurance companies when they were asymptomatic (Miller, 1998). Another study found over 200 instances where employers and insurance companies had used information from genetic tests to discriminate against applicants (Anderson, 2000). Other studies have also indicated that people are discriminated against based on their genetic characteristics. These were in the USA (Billings et al, 1992), in the UK (Low, King & Wilkie, 1998), and in Australia (Barlow-Stewart & Keays, 2001).

2.11 The Effects

While there are many examples of breaches of confidentiality, there has been little research carried out which determines the extent to which people are actually harmed by breaches of confidence. The California HealthCare Foundation (2005) found that one in five adults experienced improper disclosure of medical

information and half of these indicated that this resulted in ‘harm or embarrassment’. Another survey, this time in Australia, displayed a lower rate, finding that 1.7% of South Australians reported unauthorised disclosures of health information which caused ‘trouble or problems’ for them (Mulligan & Paterson, 2003).

It is the author’s opinion that any breach of confidentiality is significant. Having said that it would appear that disclosure of health information for the general population does not cause any harm, it is those patients with illnesses of a sensitive nature or those with a family history of a genetic disorder for instance that would suffer most from such disclosures without their consent. This will become even more important in the future, when information such as family history and DNA profile will be stored on electronic health records. Disclosure of information in these situations could prove detrimental to the patient, affecting not only their private lives, but their employment prospects and eligibility for insurance cover also.

2.12 Irish Situation

Most of the evidence relating to breaches of confidentiality has been documented in the International literature. The author has been unable to find documented examples of breaches of confidentiality relating to personal health information here in Ireland. However, the author believes that the Irish public are becoming more aware of the importance of confidentiality with respect to data protection.

This was highlighted late last year when the revenue department began investigating the fact that social welfare details of the euro millions winner Dolores Mc Namara, were viewed 125 times by members of staff curious to find out about her financial affairs. Criminal prosecutions have not been ruled out when the investigation ends (Sunday Independent, 2005).

Awareness is also evident as for the last three years running, a case study relating to data protection of patient health information has been published in the Annual Report of the Data Protection Commissioner. In 2003, a medical consultant's clinical notes were referred for review without his or the patients' consent (Data Protection Commissioner, 2003), in 2004, a health board had voluntarily disclosed to the data protection office that they had inadvertently disclose patient data to a research body (Data Protection Commissioner, 2004), and in 2005, a patient complained that data relating to the patient had been disclosed to the National Treatment Purchase Fund (Data Protection Commissioner, 2005). Correspondence with the Data Protection Commissioners office has revealed that no health organisation has yet received penalties for being in breach of the Data Protection Acts.

3 LEGISLATION and STANDARDS

3.1 Ireland Data Protection Act 1998

In Ireland, The Data Protection Acts 1988 and 2002 deal with protection of health data. The Act states that access should be assigned appropriately to the extent necessary to enable each discipline to perform their functions, and that access should only be given on a need to know basis.

The act is based on the eight data protection principles, which are:

1. Obtain and process information fairly
2. Keep only for one or more specified, explicit and lawful purpose
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up to date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the proposed purpose
8. Give a copy of his / her personal data to the individual on request.

It creates both rights for individuals and responsibilities for those holding data on the computer (Data Protection Act, 1998). The act defines the data controller as any person who controls the content and use of personal information and a data processor as any person who processes personal data on behalf of the data controller. Therefore any organisation, be it a hospital, clinic, GP surgery or dental surgery who process patient information are covered by the act.

The act outlines specific duties, which relate to the handling of medical records. These include:

- Ensure that information held on a computer is accurate and up to date
- Use information only for the purpose for which it was collected
- Put in place adequate security measures to prevent unauthorised access
- Register with the data commissioner
- Provide a copy of personal information held on computer to patients if requested

Serious penalties exist for organisations that are found to be in breach of the act (Data Protection Acts, 1998 & 2003).

3.1.1 Data Protection (Amendment) Act 2003

This legislation was passed to give effect to the provisions of the EU Data Protection Directive 95/46/EC. This act strengthens the privacy rights of individuals, and adds to the obligations on data controllers to fairly process personal information. The most important change is that it extends the current data protection principles to manual records as well as those held on computer. The act now covers any file, which forms part of a structured filing system. The new Act provides for:

- The right to be informed about who is collecting their data, the purpose for retaining it.
- Improved right of access
- The right of the consumer to object
- The right to block certain uses of data

The full effect of this legislation will not take effect until 2007 (Data Protection (Amendment) Act, 2003).

3.1.2 Freedom of Information Act 1997 & Amendment 2003

The Freedom of Information (FOI) Act, 1997 overlaps with data protection to the extent that it too confers a right of access to personal records. However, the freedom of information applies only to government departments and other bodies with public functions. It asserts the right of members of the public to obtain access to official information to the greatest extent possible consistent with the public interest and the right to privacy. The Act establishes three statutory rights:

- A right to access records held by public bodies
- A right to have inaccurate personal material on file corrected
- A right to obtain the reasons for a decision, which affects them personally (FOI, 2003).

Following the implementation of the amendment to the Act (2003), FOI legislation became less relevant from a data access perspective, as this is now covered under data privacy legislation, and also because the threshold for refusal by a data controller is generally lower than under the data protection legislation (Madden, 2002).

3.2 United Kingdom

The Data Protection Act 1998 is the data privacy legislation of most relevance with respect to privacy and confidentiality of personal health information in the UK. The Act, which came into force on March 1st 2000, replaced the 1984 Data Protection Act and similarly to Ireland, implements the requirements of the EU Data Protection Directive 95/46/EC. The UK legislation is similar to legislation in Ireland, and provides for patient access to their health records as well as limitations on disclosure and security of personal health information (Meade, 2002).

3.3 EU Data Protection Directive 95/46/EC

This directive was developed in the context of creating the infrastructure necessary for the completion of the Internal Market. It set a baseline for a common level of privacy in EU member states. The direction reinforced existing data protection law and also extended it to establish a range of new rights for individuals with additional obligations for those keeping personal information, the data controllers. They included improved protection over the processing of sensitive personal data by generally requiring the 'explicit and unambiguous' consent of the individuals concerned. The directive also emphasised 'enforceability' effectively meaning that data subjects have rights enshrined in explicit rules with a national supervisory authority that can act on their behalf. The deadline for having the directive transposed into national law was originally 1998 but Ireland did not enacted the directive until the 2003 data Protection act. (Lennon, 2006)

3.4 European Charter on Patients' Rights

At European level, patients' rights groups have prepared the 'European Charter of Patients' Rights' of which one principle refers to the right to Privacy & Confidentiality of personal information, including information regarding his or her state of health and potential diagnosis or therapeutic procedures. The principle envisages that all information relating to the individuals stat of health, and to the medical / surgical treatments must be considered private and as such adequately protected (Lennon, 2006).

3.5 United States of America

Health Insurance Portability and Accountability Act 1996 (HIPPA) is the major piece of legislation governing the privacy of personal health information in the United States. This legislation was originally introduced by the US congress to primarily improve people's access to, and use of health insurance. Congress then recognised the need for national patient privacy standards and set itself a three-year deadline to enact such protection as part of the HIPPA. The law required the Department of Health & Human Services (DHSS) to adopt such protection via regulation if Congress did not address the issue by the expiry of that time. The DHSS were required to act and proposed the federal privacy standards in 1999. Eventually, after considering more than 52,000 public comments on the proposed standards, a final set of data privacy standards were produced in December 2000 and the rules became effective in April 2003.

Under HIPPA, the following changes were brought about with respect to patient privacy and confidentiality:

- Patients have the right to receive written notice of information practices
- Patients have the right to access and amend their health information
- An audit trail must be maintained of health information disclosures and written authorisation must be provided for use of patient information for purposes other than treatment, payment or healthcare functions.

The HIPPA regulations extend to all forms of individually identifiable information, including electronic, paper-based and oral communications
(HIPPA, 2003).

3.6 Canada

In Canada, privacy is regulated at both federal and provincial level. At the federal level, privacy is protected by two acts: the 1982 Federal Privacy Act and the 2001 Personal Information and Electronic Documents Act (PIPEDA).
The Federal Privacy Act regulated the collection, use and disclosure of personal information held by federal public agencies and provides individuals a right of access to personal information by those agencies. Individuals can appeal to a federal court for review if access to their records is denied by an agency, but are not authorised to challenge the collection, use, or disclosure of information. The Privacy Commissioner reviewed the act in 1999, and in order to tighten up on any loopholes, recommended over 100 changes to the law to improve and update it. Some of the changes included giving the commissioner primary authority over all information collected by the federal government, extending its coverage beyond 'recorded' information, increasing notice of disclosures, expanding court reviews, creating rules on data matching, controlling 'publicly available' information and expanding the mandate of the Privacy Commissioner (Meade, 2002).

The Canadian Parliament approved PIPEDA in 2002. It sets out ten privacy principles as standards that organisations must comply with when dealing with personal information, including:

1. Accountability for personal health information
2. Identifying the purpose for personal health information
3. Consent for collection, use or disclosure of personal health information
4. Limiting collection of personal health information
5. Limiting use or disclosure or retention of personal health information,
6. Accuracy of personal health information
7. Safeguards for personal health information
8. Openness about the management of personal health information
9. Individual access to and amendment of own personal health information
10. Complaints about handling of personal health information

(Privacy Commissioner, Canada, 2002).

3.7 European and International EHR Standards

There are two main standards bodies currently active in European and International standards directly related to security and the EHR

3.7.1 CEN/TC 251

CEN is the main European standards body for the EHR and other health informatics standards. The scope of CEN is to provide standardisation in the field of Health Information and Communications Technology (ICT), to achieve compatibility and interoperability between independent systems, and to enable modularity. This includes requirements on health information structure to support clinical and administrative procedures, technical methods to support interoperable systems as well as requirements regarding safety, security and quality. Working Group 3 deals with security safety and quality of information systems, and base their recommendations on current European and National legislation (CEN, 2006).

3.7.2 ISO/TC 215

ISO (International Organisation for Standardisation) is the main International standards body for the EHR and other health informatics standards. ISO is a non-governmental organisation, which consists of a network of the national standards institutes of 156 countries, with a Central Secretariat in Geneva, Switzerland. ISO develop standards that are consensual, voluntary, and industry wide.

ISO standards are developed by Technical Committees, which comprise of experts from the industrial, technical and business sectors which have asked for the standards, and which subsequently put them to use. Technical Committee 215 deals with Health Informatics, the scope being to ensure standardisation in the field of information for health, and Health Information and Communications Technology (ICT) and to achieve compatibility and interoperability between independent systems.

ISO 22857:2004 provides guidance on data protection requirements to facilitate the transfer of personal health data across national borders. This standard provides information with respect to the protection of health information within national boundaries and provides assistance to national bodies involved in the development and implementation of data protection principles. The standard

covers both the data protection principles that should apply to international transfers and the security policy, which an organisation should adopt to ensure compliance with those principles (ISO, 2006).

3.7.3 Seismed Project

The SEISMED (Secure Environment for Information Systems in Medicine) Project was set-up in 1992 to conduct detailed risk analysis within Europe and to develop security guidelines for Healthcare Establishments. It was conducted as part of the Commission of European Communities AIM (Advanced Informatics in Medicine) programme. It was the first effective identification, at a European level, of the issues arising from the increasing clinical use of Health Telematics in direct patient care. The SEISMED Project ran for duration of three and a half years, and identified the need for high levels of data integrity and availability within the Health Telematics environment as well as the internationally accepted high levels of confidentiality.

The SEISMED Project collated and highlighted these issues at a European level, and the results were published in a three-volume handbook and have been passed for reference in the current development of healthcare security standards in the Comité Européen de Normalisation (CEN) Technical Committee 251 (Network Research Group, 1999).

3.8 Comment

Despite the numerous laws and standards in existence, which address the areas of patient privacy and confidentiality, they are all similar in principle. They all recognise the patient's right to be informed, to access, and to correct inaccuracies. Meanwhile, the organisations that collect and store the data have an obligation to ensure that data is collected, stored and used in a fair and lawful way, thus ensuring that confidential patient data is neither misused nor abused.

4 METHODOLOGY

4.1 Introduction

The purpose of this chapter is to consider the research topic and to demonstrate how the most appropriate research methodology was employed during the research phase. It describes the research methodology employed to carry out the research for this study, which was to investigate the issues surrounding data protection, confidentiality and security in relation to the EHR, and to ascertain patients concern and practices regarding the privacy and confidentiality of their medical records, and their level of awareness regarding data protection.

The author undertook two studies, and will address the methodology used for each survey in turn.

- Study one, targeted hospitals who had implemented or were implementing an EHR, (EHR Survey).
- Study two targeted patients who attended outpatient's clinics over a period of two days (Patient Survey).

In both instances, a cross-sectional, non-experimental, self-completion survey design tool was use. A cross sectional study is extremely simple in design, where the researcher decides what they want to find out, identifies the study population, selects a sample and contacts the respondents to find out the required information (Kumar, 2005). This type of study requires only one contact with the study population, is comparatively cheap to undertake, and is easy to analyse. The biggest disadvantage is that it cannot measure change. It is useful for taking an overall 'picture' as it stands at the time of the study. It is not a survey of a total population, but rather a small sample representative to some degree of attitudes (Bowling, 1997).

4.2 Sample

A literature review was carried out to research current 'state of the art' and ascertain any previous research that had been carried out in the area. Due to the fact that EHR's are implemented in a relatively small number of hospitals, it became evident that the study would need to target organisations spread over a large geographical area. Although many surveys include a large number of

subjects, in the hope that it will increase representation and thus the generalisation of the findings to a wider population (Saba & McCormick, 2001), other studies, as was the case for the EHR study, use smaller samples and non-random sampling techniques. For the EHR survey, it was the intention of the author to survey a larger sample but this proved impossible due to the difficulties encountered in locating hospitals that met with the inclusion criteria. This reduces generalisation and is arguably a limitation of this study and is recognised as such.

The author contacted the authors of papers that she had read, and universities that had health informatics departments by email, in order to locate hospitals where EHR's had been implemented. The author also used some personal contacts in hospitals where she had worked previously. The author finally distributed questionnaires to suitable organisations in Ireland, the United Kingdom, Australia, New Zealand, America, Canada, and the Netherlands.
In effect the findings of this study refer to a particular group of hospitals where an EHR has already been or is currently being implemented, at a particular time, and covering a wide geographical area.

For the patient survey, the author used convenience sampling, distributed questionnaires to one hundred and twenty patients attending an outpatient clinic in an Irish hospital.

4.3 Ethical Approval

It was not deemed necessary to obtain ethical approval when undertaking the survey with the hospitals. Voluntary completion of the questionnaire by IT professionals was indicative of their consent to partake, and therefore written consent was not required. Ethical approval was sought in an Irish hospital to undertake the patient survey. A letter was written to the chairperson of the ethics committee, outlining the reason for the study, and requesting permission to undertake the study in the outpatient clinic department over a period of two days. A copy of the proposed questionnaire was also included. The ethics committee passed ethical approval on the understanding that both the hospital and the patients involved in the survey would remain anonymous.

4.4 Inclusion Criteria

In order to carry out the research, it was necessary to identify the inclusion criteria that would be applied. The inclusion criteria for the EHR required the organisation have an EHR implemented in a particular area or for a particular specialty. As previously discussed, the ISO definition of the EHR was used. The inclusion criteria for the patient survey required that the participant be a patient attending a clinic in the hospital on the day specified and be willing to partake in the survey.

4.5 Survey Instrument

Structured self-completion questionnaires were deemed the most suitable method of data collection for both surveys. This method of data collection rests on the assumption that questions can be worded and ordered in a way that will be understood by all respondents, as there is no opportunity for them to have the meaning clarified, thereby avoiding interviewer bias, and providing for greater anonymity. They also have the advantages of being convenient, quick and easy to complete without assistance, and are a relatively inexpensive method of collecting routine unambiguous answers, which are easy to count and analyse. For the EHR survey, it was possible to gather data from the study population who were scattered over a wide geographical area. Interviewing in these circumstances would have been difficult and very expensive.

However, the data obtained is generally less reliable, as the interviewer is not present to clarify questions or to probe, and there is the potential for low response rates, possibly because the respondent has less of an incentive to respond when they do not have face-to-face encouragement. In addition, there is a self-selecting bias, as not everyone who receives a questionnaire returns it, and those who do return it may have attitudes or motivations that are different from those who do not, for example those who responded may be those with extreme opinions

Pre-coded response choices may not be sufficiently comprehensive, not all answers may be easily accommodated. (Bowling, 1997), and in-depth or spontaneous answers cannot be captured. Some respondents may therefore be

forced to choose inappropriate pre-coded answers that might not fully represent the situation or their views.

Bearing these points in mind, the author, following completion of the literature review, designed both questionnaires.

4.5.1 Question Format

The form and wording of questions is extremely important in a research instrument as they have an effect on the type and quality of information obtained (Kumar, 2005). The author sought to use simple everyday language, and avoided using ambiguous, double-barrelled or leading questions. Answers were pre-coded, with the response choices to most questions being closed because:

- They take less time to complete than open ended questions
- They are easy to code and analyse because the possible responses are already categorised
- A 'ready made' list of categories, help to ensure that the information needed by the researcher is obtained.
- They enable comparisons to be made across individuals or groups of respondents

Most questions required that the respondent choose only one answer, but 'multiple responses' could be chosen in some of the questions. Dichotomised (Yes / No) response choices were used in many of the questions in the patient questionnaire. As is recommended by McColl et al (2001), when designing a questionnaire with closed-ended questions, a category 'other' was included in questions where it was deemed necessary, to accommodate any response not listed. The author also sought to include comprehensive response categories to fit every possible response, and care was taken with pre-coded numbers, such as age groups and time periods to ensure that the each answer was mutually exclusive.

4.5.2 Question Order

The patient questionnaire contained twenty questions, which followed a logical progression with the simpler, easier to answer questions being asked first. This is the method recommended by Kumar (2005), as it gradually leads the respondents

into the themes of the study, starting with the simple themes and progressing to the more complex ones, sustaining the interest of the respondents and gradually stimulating them to answer the questions. Schuman et al (1983) also highlighted the fact that the position of a question may affect the way the respondent answers it, therefore the EHR questionnaire which contained a total of thirty-one questions, asked general questions first and then followed with specific questions, which were blocked by topic.

4.5.3 Questionnaire Layout

McColl et al (2001) recognises the importance of enhancing the appearance and layout of questionnaires. It is generally suggested that self-completion questionnaires be short and contain mostly closed ended questions (Bourque and Fielder 1995). Kane (2000) also suggests that the layout of a self-completion questionnaire should be simple, particularly spacious, with a minimum of questions, and clear instructions about completion. The author gave consideration to all the above points when designing the general layout of the questionnaire. Both questionnaires were formatted clearly; font was 12-point times new roman, section headings and questions were displayed in bold font, pages were numbered and the questions were laid out to ensure that responses were not split over 2 pages. A brief introduction with instructions on how to complete was included at the beginning of the questionnaire. A note of thanks was printed after the last question.

4.5.4 Administering the Questionnaires

The most common approach to collecting information is to send the questionnaire to prospective respondents by mail. The author used a variation of this approach by e-mailing the EHR questionnaire to the participants, providing the authors e-mail address for reply and any questions that may have arisen.

The approach used for the patient questionnaire was collective administration, which is recommended as one of the best ways of administering a questionnaire by obtaining a captive audience. Kumar (2000) advises that if a captive audience is available for the study, the opportunity should not be missed, as it is the quickest way of collecting data, ensures a very high response rate, as few people

would refuse to participate in the study. It also saves money and postage. As the author was in attendance, the purpose, relevance and importance of the study could be explained and any questions that the audience may have had could be clarified.

4.6 Advance and Covering Letter's

Advance letters were sent to the IT manager, or information managers in the hospitals chosen for the survey, informing them about the research and requesting that they partake in the survey. The reason for this was two-fold: The author needed to ensure that she had obtained a sample population for the study and also because advance letters have been shown to increase response rates and increase the credibility of the study, explain its value, and emphasise confidentiality (Campanelli, 1995).

It is recommended that all self-administration questionnaire surveys should give all sample members a covering letter about the study, to keep for reference, and reassurance that the organisation and study are bone fide (Bowling, 1997). Therefore, covering letters were included with both the EHR and the patient questionnaires.

For both surveys, the covering letter began by introducing the author, outlining the course being undertaken, the reason for the study outlining the study's aims and benefits, and the reason why they had been chosen to partake in the study. In the case of the EHR survey, the letter explained how the respondent's names had been obtained.

The letters then outlined the inclusion criteria, and provided instructions for completing and returning the questionnaire by a defined deadline. Contact details for the author were clearly documented and complete anonymity of the information provided was assured. The importance of responding to the questionnaire was highlighted, and respondents were invited to tick a box at the end of the questionnaire if they were interested in receiving a copy of the results once they

were available. Both letters concluded by thanking respondents for participating in the study.

4.7 Pilot Study

A pilot study was undertaken for both surveys. A pilot study is a small-scale test of the main study to check that all procedures are working properly, and if not, to rectify them before the main study (Meadows, 2003). The author wanted to test not only the questionnaire but also the whole administrative procedure, the aim being to test the letter of introduction, the questionnaire, the instructions to the participants and the response rate using a smaller but representative sample of the participants before the main study. The author wanted to ensure that each questionnaire flowed properly, that the wording was understood, the questions being clear and meaning the same thing to each person, that it did not take too long to complete, that the information required for analysis was gathered, and that it was possible to code the questions adequately.

As already explained it was difficult to obtain participants to partake in the EHR survey, therefore 3 IT managers in Irish hospitals and the MSc class members piloted this survey. The patient questionnaire was piloted among the author's colleagues. Pilot respondents were asked to inform the author of any instances where questions or instructions were not properly understood, if the appropriate responses were available for all questions, or if there were instances where responses were not applicable to them.

Feedback to the EHR questionnaire was very positive, and the author did not need to change any of the questions or responses. It was necessary however to specify more clearly how to respond to the questionnaire, in the pilot study the author's email address was displayed on the questionnaire and some respondents believed this to be a link to reply, and commented that 'it would not work'. Therefore for the main study, specific instructions on how to respond were included in the covering letter.

Feedback to the patient questionnaire created a high level of interest in the subject, and it was agreed that the author had included all relevant issues in the questionnaire. However, it did highlight some responses that were not clearly understood by all of the respondents. Following a discussion with the respondents, these responses were changed. Coding and analysis of the pilot study results did not require any further changes to be made.

4.8 Data Collection

At the beginning of April 2006, the EHR questionnaire was emailed to the 23 respondents who had agreed to participate in the research. They were given two weeks to complete and return the questionnaires. A master list of participants was kept on an excel spreadsheet and as each questionnaire was returned, the participant was ticked off the list. An email thanking the respondent was sent as soon as the completed questionnaire was received. A follow up letter was mailed reminding participants who had not returned a completed questionnaire mid–way through the second week. A further email which included a new covering letter explaining why their co-operation was important, and included a new questionnaire was emailed to respondents who still had not replied, two weeks after the closing date and they were given a further week to reply. A total of seventeen questionnaires were returned, but of these three replied saying that they could not participate, one didn't give a reason why, and the other two stated that on reading the questionnaire, they did not meet the criteria necessary to complete it. The author did not receive any response from six of the organisations contacted. Therefore the fourteen completed questionnaires that were returned, and included in the study represent a 60% response rate.

The patient survey was conducted in an outpatient clinic department of an Irish hospital. Survey participants were randomly selected on the day and requested to complete a questionnaire. The author was in attendance for the duration of the study, in order to respond to any questions that the patients may have had. The patient completed the questionnaire in the waiting area, and once completed, placed them the envelope in a special box provided for the study. 120 questionnaires were handed out in total, and 109 were completed and returned.

This represents a 90% response rate, which was helped by the fact that the author was in attendance at all times to answer any questions that the patients may have had in completing the questionnaire.

4.9 Data Analysis

Data analysis is conducted to reduce, organise, and give meaning to the data collected (Burns & Grove, 1997). Data analysis was conducted for each study, after all data had been collected from that study. In both instances, initial data analysis, was undertaken, using Microsoft excel. The Chart Wizard was used to generate column, bar, and pie charts.

As the response to the patient survey was so positive (90% response rate), further statistical analysis was undertaken to ascertain whether results were statistically significant. The statistical package SAS (r) 9.1 (TS1M3) was used for this analysis. Hypothesis tests were undertaken to test for age and gender significance, and the 'Wilcoxon Mann-Whitney Test', and the 'Kruskal-Wallis Test', was used to analyse and interpret the results.

4.10 Limitations

The survey of hospitals was small, with questionnaires only been sent to twenty-three hospitals. There were seventeen replies, fourteen of which were included for analysis. The small sample size was due to the difficulty in identifying hospitals who had actually implemented an EHR and who met with the criteria identified by the author. This is arguably not only a limitation of this study, but also highlights the fact that implementation worldwide is still at a very early stage. However, 65% of hospitals surveyed had an EHR implemented for at least one year and were therefore in a good position to comment on privacy, confidentiality and data protection with respect to the EHR in their organisations.

5 DATA ANALYSIS OF HOSPITAL SURVEY

5.1 Introduction

This study was carried out in April 2006. As previously discussed, the author had difficulty in recruiting organisations that met with the inclusion criteria. A total of twenty-three questionnaires were distributed, seventeen were returned, but three of these replied saying that they could not participate, one didn't give a reason why, and the other two stated that on reading the questionnaire, they did not meet the criteria necessary to complete it. The author did not receive any response from six of the organisations contacted. Therefore the fourteen completed questionnaires that were returned and included in the study represent a 60% response rate.

5.2 General Information

This section of the questionnaire was designed to obtain general information about the organisation, the type of EHR in use, and the person completing the questionnaire.

In 44% (6) of the hospitals surveyed the EHR had been implemented more than 5 years, with 21% (3) having it implemented between 1 and 5 years. 21% (3) were implemented less than one year, and 14% (2) of those surveyed were still in the implementation phase. See figure 1.

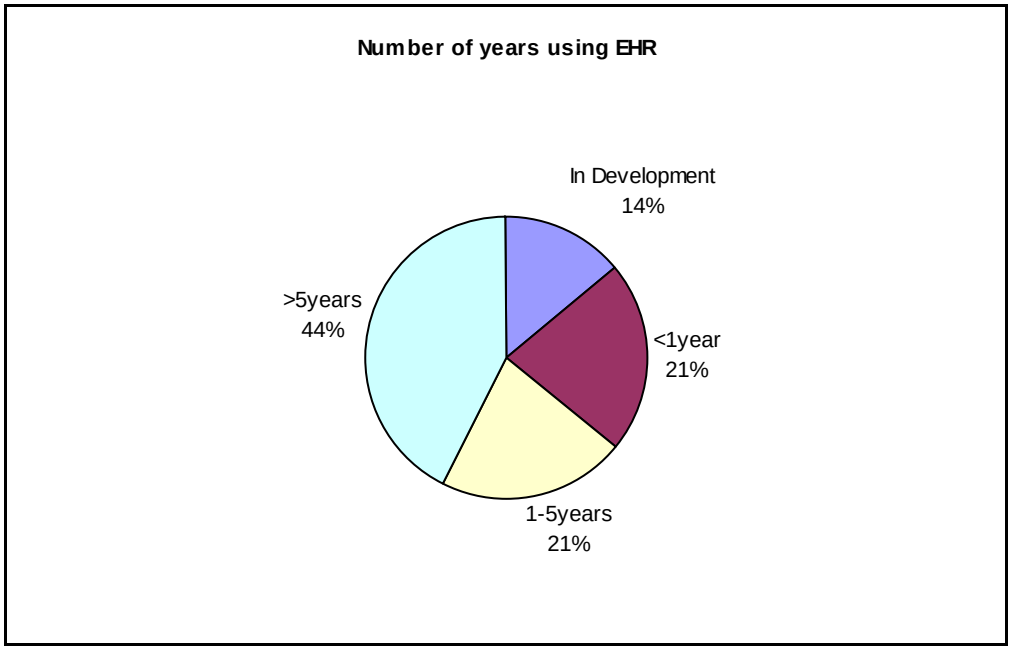

Figure 1 Number of Years using an EHR

In more than half, 57% (8), of the organisations who replied, the EHR had been purchased from the vendor as an ‘off the shelf’ product. In 29% (4) of cases, it was developed specifically for the organisation by the vendor, with only 14% (2) of systems being developed ‘in-house’.

Participants were asked how many records were held on the EHR’s database. In 61% (8) of organisations there was in excess of 10,000 patient records held. 23% (3) of organisations did not answer this question.

Although the questionnaires were mailed in the first instance to the database managers, some questionnaires were redirected, and the participants who finally completed them worked in a number of departments. While 33% of those who answered worked in the IT department, 27% reported that they were linked to more than one department, the IT department and another department within the hospital. Figure 2 shows the breakdown of departments where participants worked.

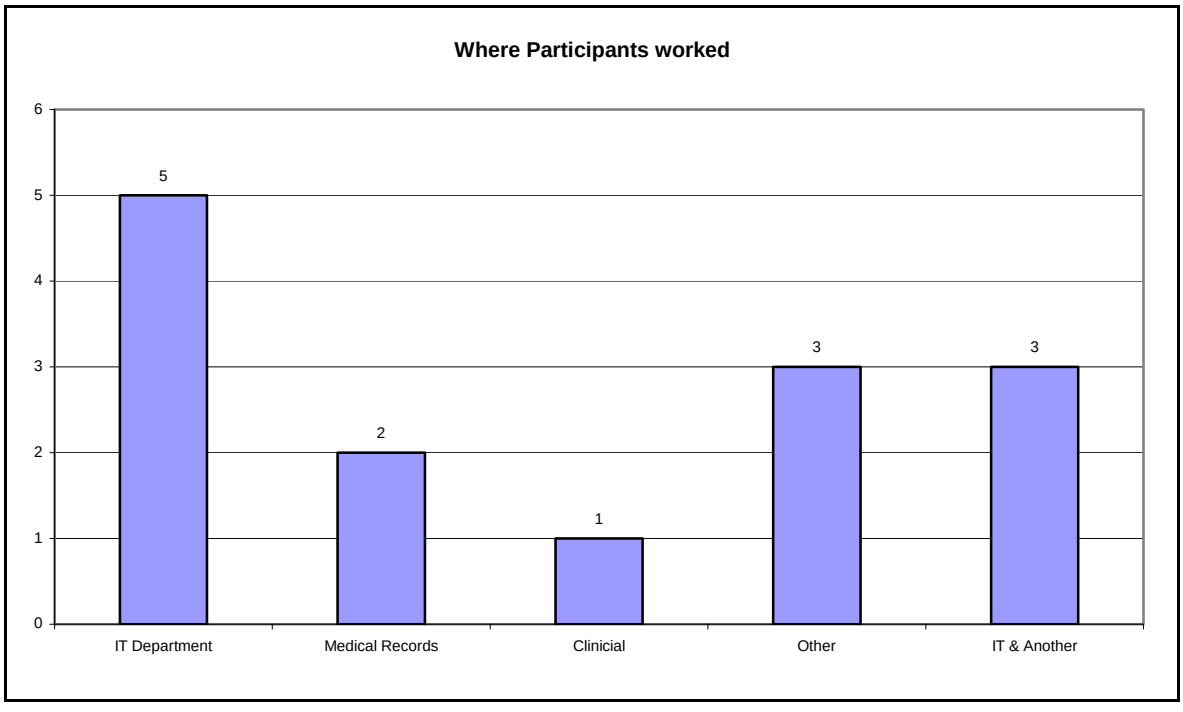

Figure 2 Departments where Participants Worked

Participants were asked whether all disciplines dealing with patients have access to those patients' EHR's. In 57% of cases (8) all disciplines dealing with patients have access to the EHR. The 43%, (6) who replied no, gave examples of what carers did not receive access such a 'household do not have access' and 'non management employees can only view in-house patients' and 'access is given on a need to know basis' as reasons why.

These results are seen as being positive as all disciplines involved in patient care require access to the EHR to ensure that a complete all encompassing electronic record for the patient is developed, thus ensuring that patients receive a high standard of care from the multidisciplinary team. Denying access to particular patient carers would leave gaps in the patient's records and could result in the patient not receiving optimal care. It would appear that none of the users omitted would require access to the patient's medical records and the author would see it as reasonable to exclude these disciplines from accessing the EHR.

5.3 Data Protection

This section of the questionnaire was designed to obtain information regarding distribution of patient data, the organisations policies on privacy, confidentiality and data protection, and any incidences of inappropriate access that may have been recorded.

Participants were asked about the type of organisations they distributed patient information that is recorded in the EHR to. Only three organisations answered that they did not distribute to any organisation outside of their own organisation. 44% (6) answered that they distributed to government organisations only, and 21% (3) distributed to more than one of the organisations listed.

What was interesting to note was that three organisations replied that they distribute information to commercial organisations. The author was surprised by this statistic, and would question the legality of such practice. However, one participant qualified what they meant by ‘commercial organisation’ and defined them as ‘general practitioners, private laboratories and other organisations in the patients circle of care providers’. This same participant replied that they distributed patient information to employers. A potential risk associated with sharing electronic health records is that employers would be privy to health records, thereby discriminating against employees on medical grounds (Anderson, 2000). Unfortunately, the respondent did not inform as to the context in which health information was distributed to the employer. Figure 3 displays the breakdown of organisations where patient information is distributed.

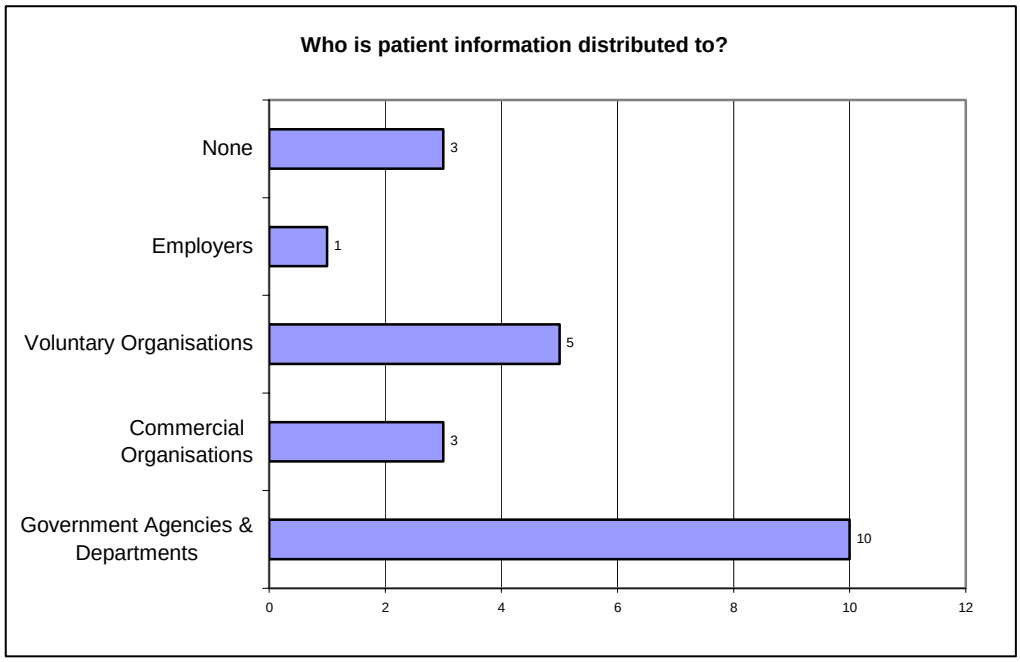

Figure 3 Organisations to which Patient Information Distributed

Participants were then asked whether data distributed to outside organisations was ‘traceable’ to the patient. ‘Traceable’ means that the patient is identifiable and can be linked to the information distributed. Only one organisation answered that information was never traceable to the patient, and this organisation distributed patient data to voluntary organisations only. 51% (7) of respondents indicated that patient data is ‘sometimes’ traceable to the patient and in 21% (3) of cases data is ‘always’ traceable to the patient. 25% replied ‘not applicable’ to this question. Figure 4 displays this data. The practice of allowing patient identifiable data to be distributed to organisation outside of where the data has been collected is potentially quite serious. Data protection legislation outlines specific duties, which relate to the handling of medical records, and states that ‘information should be used only for the purpose for which it was collected’. Once this information is available in another organisation, the organisation where the data was collected no longer has control over what happens to of what the information can be used for.

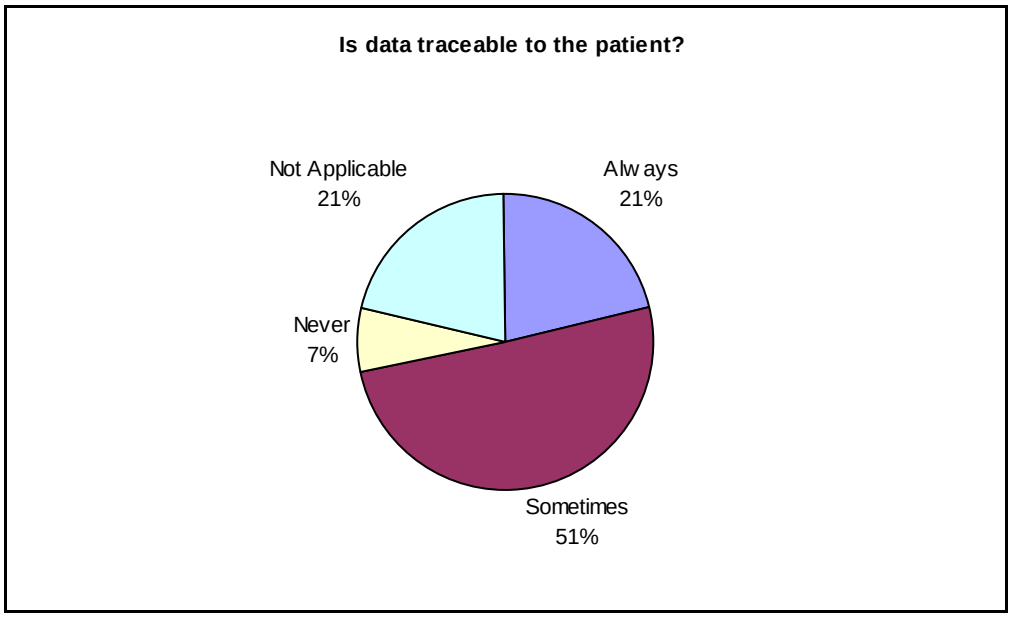

Figure 4 Data Traceable to the Patient

5.4 Staff Training

Seminars on privacy, confidentiality and data protection are held in all organisations. In 46% (6) of organisations, they are held at least once a year and in 54% (7) of cases, there are held whenever is deemed necessary. Attendance is mandatory in 86% (12) of organisations; in 50% (7) of cases attendance is mandatory prior to access to the EHR being granted, and the other 36% (5) within a given period of joining the organisation. However, although seminars are held, attendance is not mandatory in 14% (2) of organisations. When participants were asked if users sign confidentiality document specifically relating to the EHR, the answer was split with 50% answering 'yes' and 50% answering 'no'.

5.5 Maintenance of Audit Trails

Figure 5 outlines respondents' answers in relation to the maintenance of audit trails in order to monitor inappropriate user access. Audit trails are maintained in 92% (12) of organisations, but in only 15% (2) of cases are audit trails regularly reviewed. In most cases, 77% (10), they are only investigated when there is a specific complaint. This could mean that there are ongoing instances of inappropriate access in these organisations that go undetected. One organisation indicated that audit trails are not maintained at all in their organisation. The author

found this worrying and although it is a small percentage, it cannot be ignored. Inappropriate access could be an ongoing problem in this organisation, without the organisation being aware of it, and without being acted upon and the organisation could be leaving itself wide open to litigation.

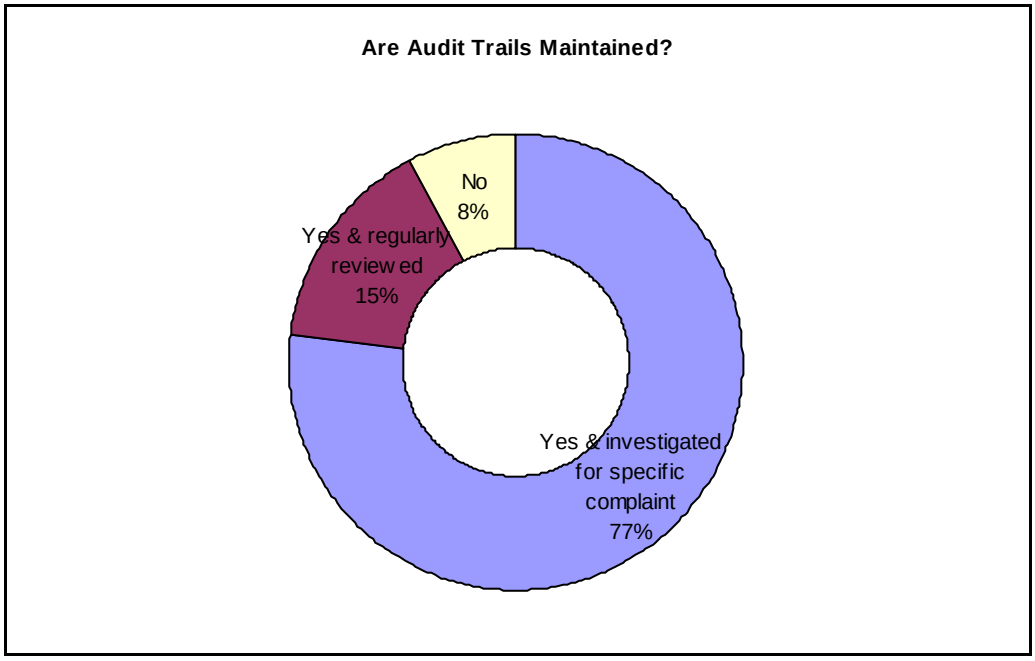

Figure 5 Maintenance of Audit Trails

In 36% (5) of organisations, medical records belonging to staff or 'VIP' patients were granted a higher level of protection than other patient's records. However in the majority of cases, 64% (9), they were not. Interestingly, in 5 of the organisations where this is the case, users do not sign a confidentiality document specifically relating to the EHR either. However, the majority of organisations did afford a higher level of security to information of a sensitive nature, such as HIV test results, genetic test results, and previous termination of pregnancies. 83% (10) of organisations answered that tests of a sensitive nature were not as freely available as a Full Blood Count Test.

5.6 Inappropriate Access

Participants were questioned about the number of incidences of inappropriate access both from within and outside their organisations. Figure 6 displays these findings.

There were no incidences of inappropriate access from within the organisation in 21% (3) of cases. Of the remaining 79% (11), there were <10 instances in 50% (7) of cases. The figure was unknown in 29% (4) of organisations. There were no incidences of inappropriate access from outside the organisation, in 77% (10) of organisations. There were <10 incidences in 8% (1), and 2 organisations (15%), answered ‘not known.

The fact that a number of organisations did not know the statistics for inappropriate access, would lead the author to question if more incidences had occurred, but had been ignored or not reported?

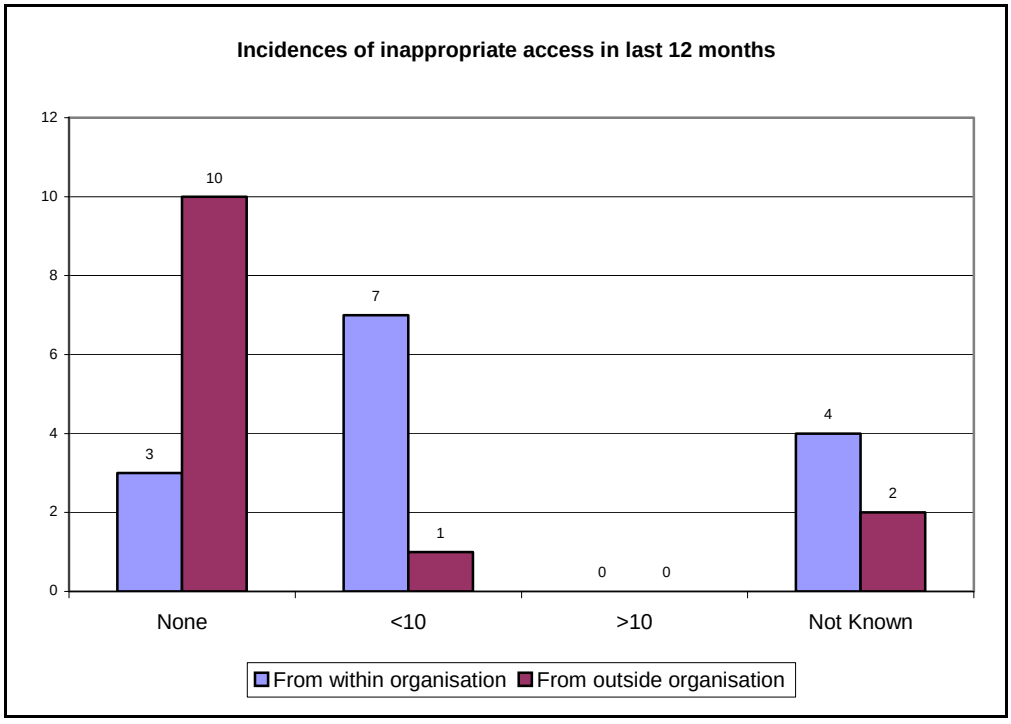

Figure 6 Incidences of Inappropriate Access

5.7 Disciplinary Procedures

Participants were then questioned about how often disciplinary procedures were followed. Four organisations did not answer this question, leaving it blank. Of the 10 organisations who did answer, 40% (4) answered that disciplinary procedures were followed in all incidences, a further 40% (4) answered that they were followed in some instances in 20% (2) of cases disciplinary procedures were never followed. See figure 7. The author would question the point of maintaining audit

trails if the organisations are not going to act on breaches. The author would recommend that disciplinary procedures be followed in all instances where inappropriate access is found to occur.

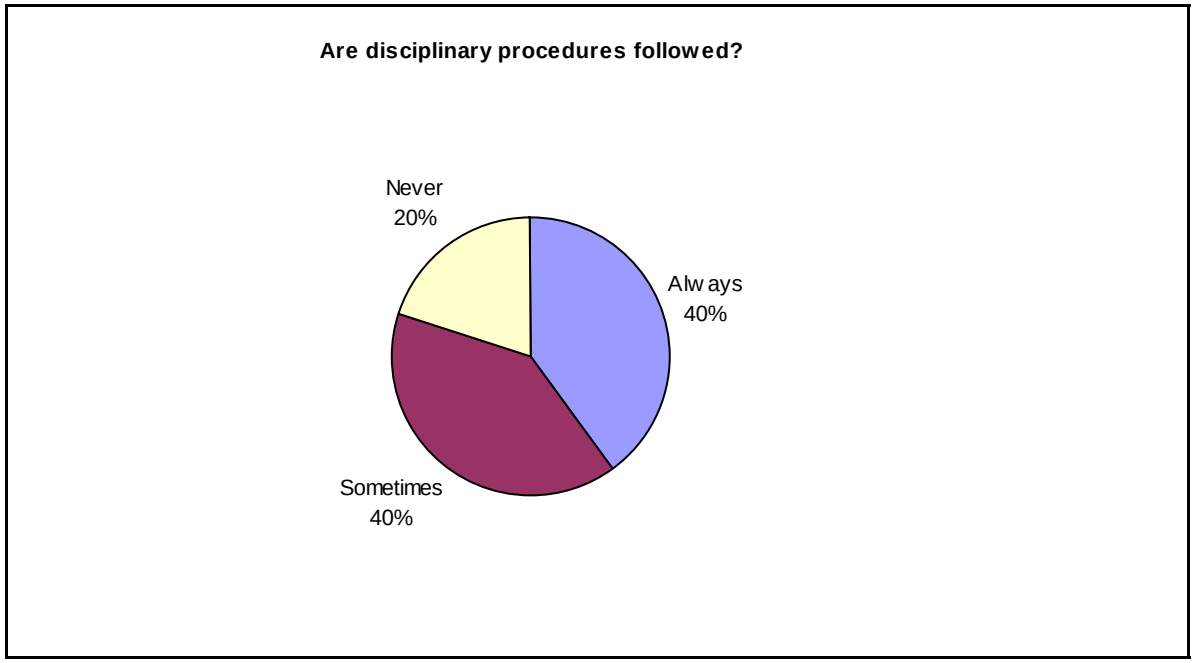

Figure 7 Adherence to Disciplinary Procedures

5.8 User Access

This section of the questionnaire was designed to ascertain, who allocates user rights, and how they are allocated, managed and made inactive.

Participants were asked to indicate who was responsible for defining user access in their organisations. These findings are outlined in figure 8. It was the responsibility of the database manager in 15% (2) of cases and the systems administrator in 23% (3) of cases. The clinical director or a person nominated by him / her was responsible in 23% (3) of cases.

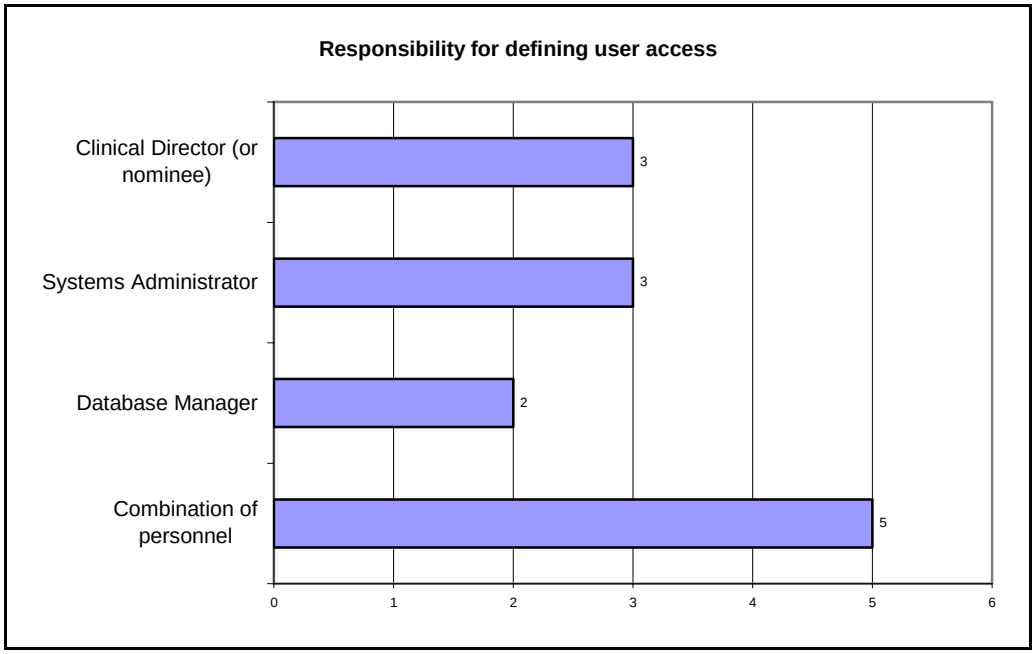

Figure 8 Responsibility for Defining User Access

In 39% (5) of cases, defining user access was the responsibility of a combination of personnel, such as:

- The IT Manager and the HIM director
- The IT Manager and the systems administrator
- The IT Manager, systems administrator and the line manager
- The IT Manager and a subcommittee developed to define user roles
- The systems administrator and the line manager.

The line manager requests access for the user in 36% (5) of cases, and in 64% (9) of cases there is a hospital policy whereby a user enrolment document is completed and submitted to the person responsible for creating new accounts. There are no instances where the user request access for himself / herself. These statistics are very positive, as the practice of having documentation such as a user enrolment document that is completed either electronically or on hard copy is preferable, as this creates a formal record of who has requested access, and ensures that only users entitled to have access to the patients EHR will have access.

5.9 Access Levels

Access levels are managed according to the users role in 93% (13) of cases. Full access to the EHR is given in 7% (1) of cases. Furthermore, in 35% (5) of cases all grades are given the same access, and in 36% (5) organisations more senior grades are given a higher level of access. 29% (4) replied 'other' and gave reasons such as 'relevant to job / role' and 'on a need to know basis'. The practice of managing user rights according to the users role is favourable as it ensures that users only see patient health information that is pertinent to their role in caring for that patient and also assists in the protection of patient privacy and confidentiality.

The author was interested in establishing how user accounts were made inactive or if they were made inactive at all. The findings are outlined in figure 9 and show that in 58% (8) of organisations, users were made inactive when the IT department is notified, as per hospital policy, and access is then terminated. Another organisation (7%) who answered 'other' added the comment 'when the user leave the department their account is made inactive'. These statistics are encouraging when patient's privacy and confidentiality is considered. Once a user is no longer involved in a patients care, access rights to the patients EHR should no longer be available to him / her.

In 7% (1) of cases, access is terminated when the user account has been inactive for a specific time period, and a further 21% (3) answered that access is terminated based on a combination of informing the IT department and when the

user account is inactive for a specified period of time, which would indicate that there is either no policy or where there is one it is not being adhered to. The most worrying case was found in one organisation that reported that user accounts are never made inactive. In the event of a user leaving this organisation and his / her password being known, patients records could continue to be accessed inappropriately over a prolonged period of time.

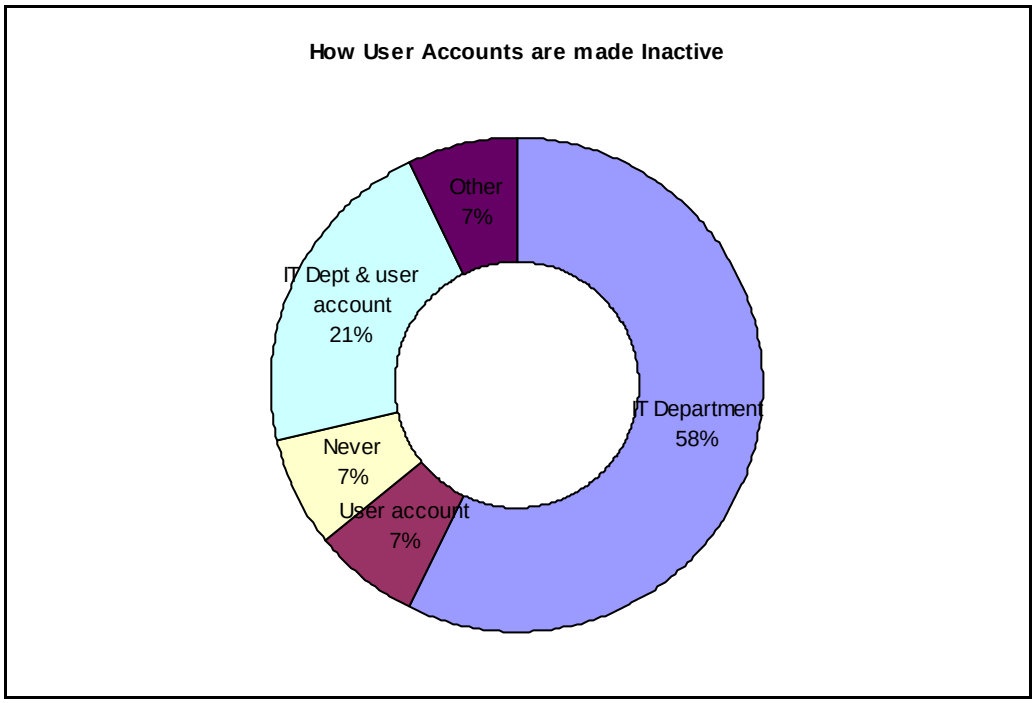

Figure 9 How are User Accounts made Inactive?

In response to the question asking what level of access was assigned to users who are not members of the organisation, for example agency nurses or locums, access is given according to user role in 57% (8) of cases. See figure 10. In 14% (2) of cases, access is not given at all, however, in 29% (4) of cases these users are given general access, which may allow them to see more than necessary to carry out their role in caring for the patient. This amounted to four organisations, two of which answered no to the question regarding users signing a confidentiality document, and in one of these organisation, data protection seminars are held but are not mandatory. The author would question the correctness of this practice with regard to the protection of patients' privacy and confidentiality in relation to medical information.

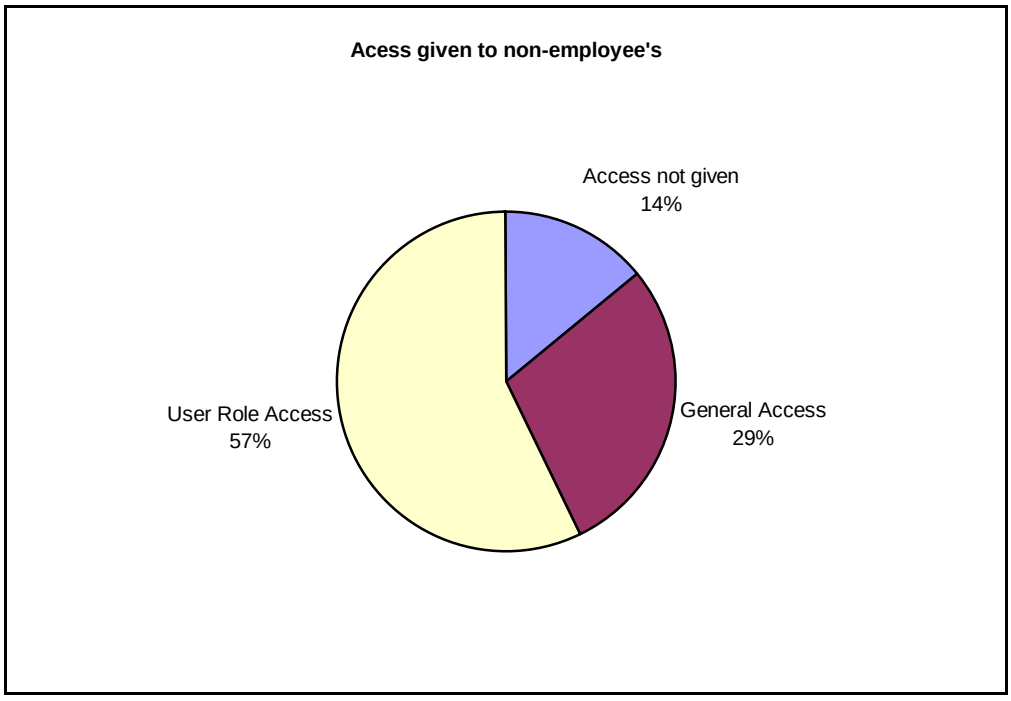

Figure 10 Access to Non – Employees

Participants were asked how often they needed to amend user rights to allow users more access. The majority of participants, 72% (5), replied that it had never been necessary to increase users access rights, 14% (2) answered that they are required to increase user rights about once a month and a further 14% (2) increased user rights about once in 6 months. In response to a question asking how often they were required to remove user rights, 60% (8) replied that they had never to remove user rights, 21% (2) replied that they removed rights from a user less than five times and 14% (2) more than five times in the last 12 months.

In the author's opinion, this indicates that most organisations manage to define user access rights correctly from the outset.

5.10 Patient Information and Consent

This section of the questionnaire was designed to ascertain if the patient was informed about information being distributed to organisations, gave consent and had the option to opt out or have their information corrected or removed.

The survey worryingly found that in most cases, 43% (6), patients are not told which organisations information about them might be distributed to. In 36% (5) of cases patients are informed. However, over half, 57% (8) of organisations, patients are informed about what information about them might be distributed to outside organisations. In 29% (4) they are not informed. Figure 11 displays the results of these questions.

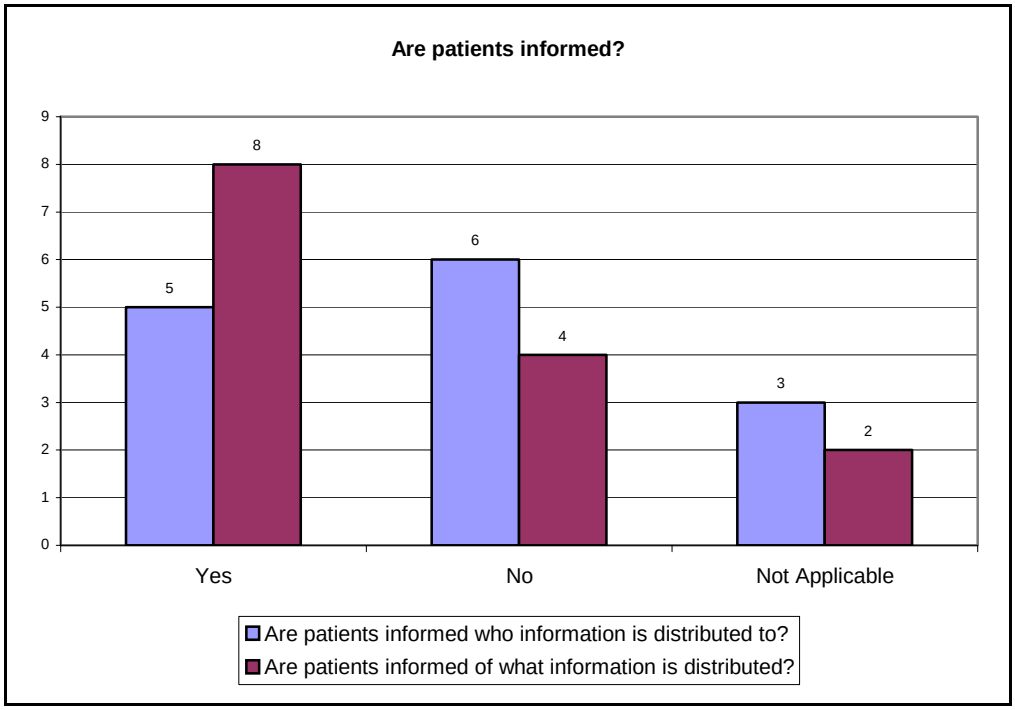

Figure 11 Information given to patients

Note: One participant answered that information was not distributed to outside organisations, but answered that patients were informed about what information about them might be shared with other health professionals or passed to outside organisations. It is possible that this participant was referring to information being shared with other health professionals. However, this was not made clear in the response.

In organisations where patients are informed about what information is shared, and whom information is shared with, the majority, 64% (9) of patients do not give written consent. 36% (5) give written consent. These statistics would not be in agreement with literature where it has been shown that patients believe that their consent should be given before their personal information is shared (Robling et al, 2004) and that patients are more likely to share information when they know the nature of the information and the person or organisation that the information will be shared with (Willison et al, 2003), See figure 12.

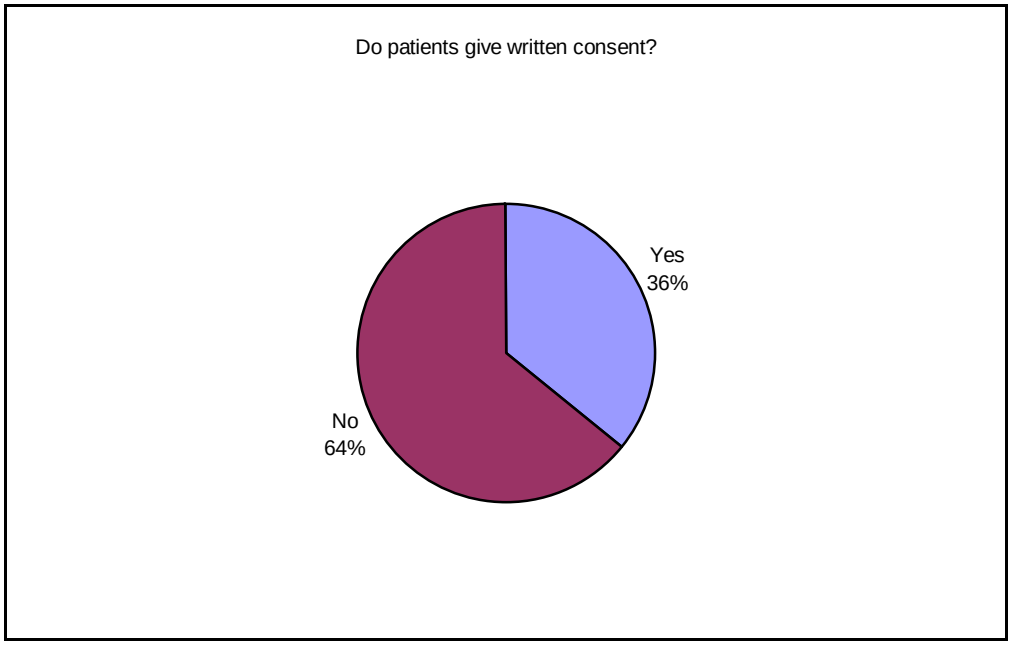

Figure 12 Consent given by patients

When participants were asked if there was an 'opt out' clause, whereby patient could choose not to have their information shared or certain information not shared, 57% (8) answered yes and 43% (5) answered no. There was also a procedure where by patients can request that information be corrected or removed in 79% (11) of cases; no procedure exists in 21% (3) of cases.

In 67% (8) of organisations, there were no reports of patients expressing concern over who has access to their medical records. There were less than 10 instances in 25% (3) of organisations and 8% (1) of organisations there were between 10 and 50 instances of patients expressing concern over who had access to their

medical records. Also 72% (10) of organisations answered that no patient had requested access to their electronic health record in the past 12 months. 14% (2) answered that between 1- 50 patients had requested access. However 14% (2) indicated that more than 50 patients had requested access to their electronic health record during the last 12 months. Unfortunately, neither of the two organisations where more than 50 patients had requested access to their records r answered question 1.3, which asked about the number of patients held in the EHR, therefore the % of patients requesting access to their records cannot be ascertained and therefore a direct comparison between organisations is not possible.

6 DATA ANALYSIS OF PATIENT SURVEY

6.1 Introduction

The research was carried out over two days in the outpatients department of an Irish Hospital. The outpatient department consists of a central reception / waiting area, from where patients are re-directed to the clinic that they are scheduled to attend. Patients visiting the following clinics were included in the study:

- Antenatal Clinic
- Breast care Clinic
- Dermatology Clinic
- Diabetic Clinic
- Dressings Clinic
- Ophthalmology Clinic
- Pain Control Clinic

A brief explanation of the study was given to each patient, and after obtaining the patients verbal consent; a pack consisting of the questionnaire, a covering letter and a blank envelope was handed to the patient. The patient completed the questionnaire in the waiting area, and placed the envelope in a special box provided for the study. 120 questionnaires were handed out in total, and 109 were completed and returned. This represents a 90% response rate, which was helped by the fact that the author was in attendance at all times to answer any questions that the patients may have had in completing the questionnaire.

The questionnaire consisted of 20 questions, which were designed to ascertain:

- How patients view, manage, and safeguard their personal health information?
- How concerned patients are about the privacy of their health information?
- If patients are participating practice privacy protecting behaviour
- How secure patients believe their medical records to be?
- Patient awareness regarding Data Protection and Freedom of Information
- If patients support the use of a unique identifier?

Hypothesis testing was performed for age and gender significance, and reference is made to those results that were significant.

6.2 Patient Demographics

64 of those surveyed were female and 44 were male. The majority of patients, 46% (51) surveyed were in the 40 – 60 age group. 32% (35) were in the >60 years, 16% (17) were between 25 years and 39 years and 6% (6) were between 18 years and 24 years. See figure 13

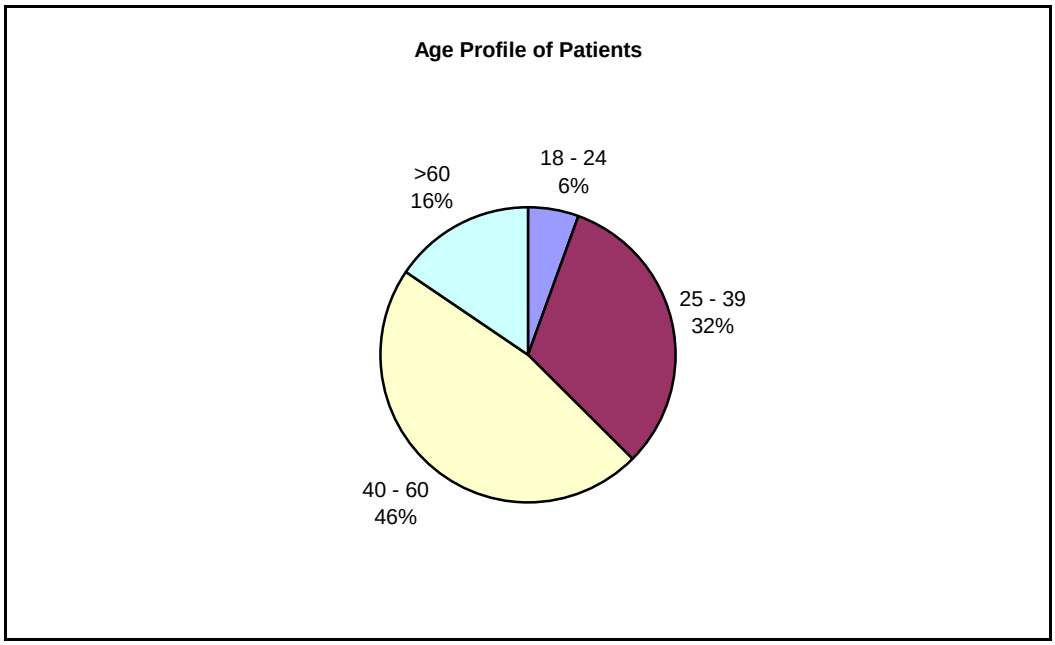

Figure 13 Patient Age Profile

6.3 Level of Concern

Patients were asked how concerned were they about the privacy of their medical records. In total 43% (55) of patients said that they were concerned, with 21% (27) being very concerned and 22% (28) being somewhat concerned. 36% (44) said that they were not very concerned, and a further 21% (27) said that they were not at all concerned. See figure 14. These results demonstrate that Irish patients are less concerned than US patients, where 67% of patients are concerned about the privacy of their personal health information (National Consumer Health Privacy Survey 2005), and are more similar to Australian patients, where a minority of about 10% were not confident that doctors or hospitals used information responsibly (Mulligan, 2001), and UK patients where there is a high level of trust in the NHS to protect patient confidentiality (NHS, 2002).

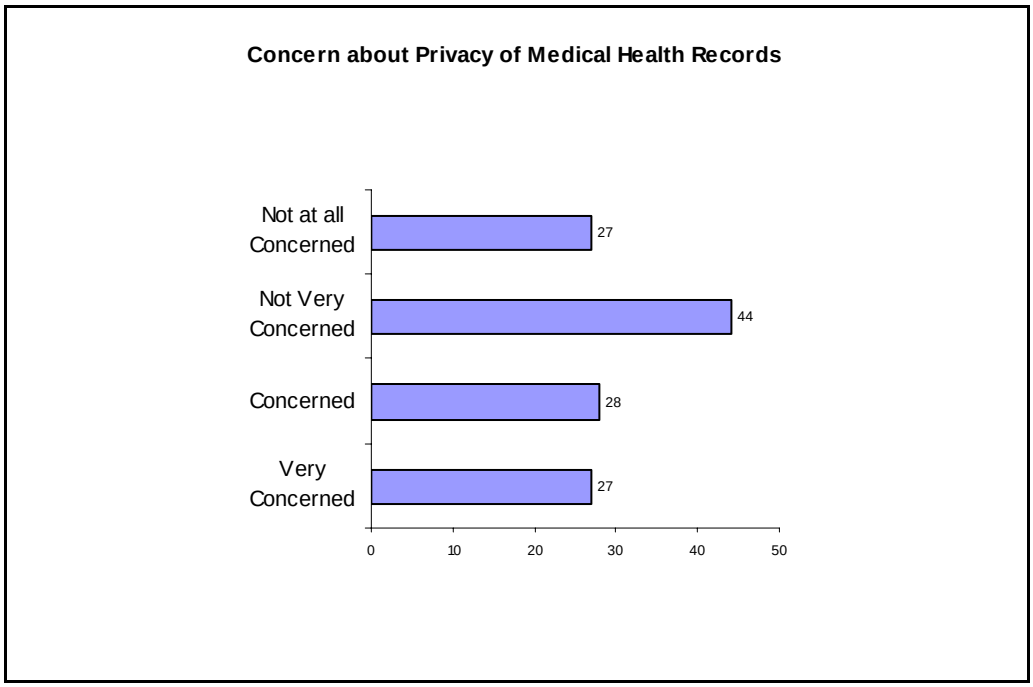

Figure 14 Level of Patient Concern

Kruskal- Wallis testing is used for comparing several independent random samples, and was conducted to test the hypothesis; H_0: there is no difference in the concern about the privacy of medical health records between age groups against H_A: there is a difference. P-values indicate how unusual a computed test statistic is compared with what would be expected under the null hypothesis, and a p-value of less than 0.05 is the same as having a 95% level of confidence. A p-value of 0.0312, was received which is < 0.05, so therefore the null hypothesis that the age group values received are equal can be rejected. The mean score for age groups tested was calculated using wilcoxon scores and showed that the >60years age group were most concerned about the privacy of their medical records.

6.4 Patient Awareness

6.4.1 Awareness regarding Health Information

Patients were asked if they knew whether insurance companies, or other healthcare organisations could access their personal health information without their knowledge or permission. 13% (14) answered yes, they thought that they could 47% (51) answered that no they couldn't and 40% of patients (44), answered that they didn't know the answer. The results are displayed in figure 15.

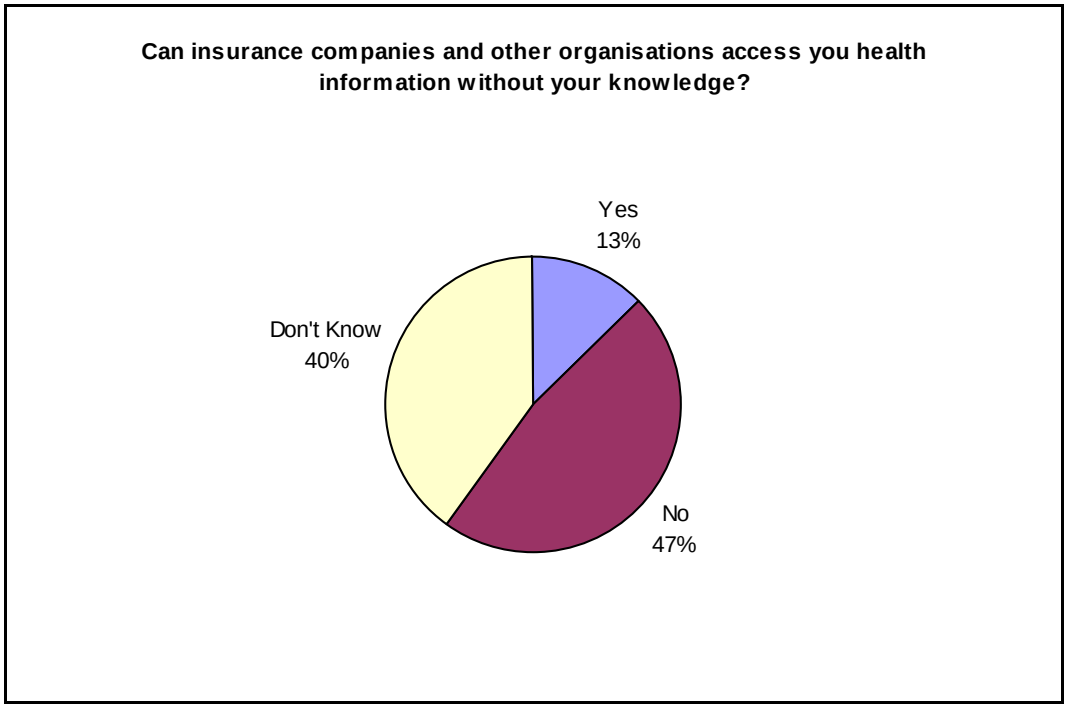

Figure 15 Patient Knowledge

This indicates the lack of awareness among the patients surveyed regarding the distribution of their personal health information. The Wilcoxon Mann-Whitney Test was used to test the significance of this finding; it is one of the most powerful of the nonparametric tests for comparing two populations, the populations here being male and female. The H_0: there is no difference in the answers to whether a patient knew whether insurance companies, other healthcare organisations, could access their personal health information without their knowledge or permission between gender, was tested against H_A: there is a difference in their median. In this case the P-value received is 0.0288, which is < 0.05 so therefore the null

hypothesis that the gender values received are equal, is rejected. In this case the wilcoxon scores showed that females were more aware than males.

The majority of patients, 95% (104), believed that their doctor should ask for permission before disclosing information about them to another person. Of the patients surveyed only two patients had decided not to be tested for a medical condition because they were concerned that others might find out the result, and only four patients had requested that their doctor not write down their health problem in their medical records or write down a less serious or less embarrassing condition than was actually the condition. Again this shows that although some patients are concerned about the privacy and confidentiality of their personal medical records, the majority do not appear to be concerned.

6.4.2 Viewing Medical Records

Patients were asked if they knew whether they had the right to see their medical records. The majority, 68% (74), answered yes, they had the right to see their medical records, 2% (2) answered no, and a significant minority, 30% (33), answered that they didn't know. See figure 16.

Under the Freedom of Information Act, patients are entitled to:

- Access records held by public bodies
- Have personal information in a record amended where it is incomplete, incorrect or misleading (Freedom of Information Act, 1997).

The above statistics display a lack of understanding among the group surveyed regarding ownership and access rights to their personal health records.

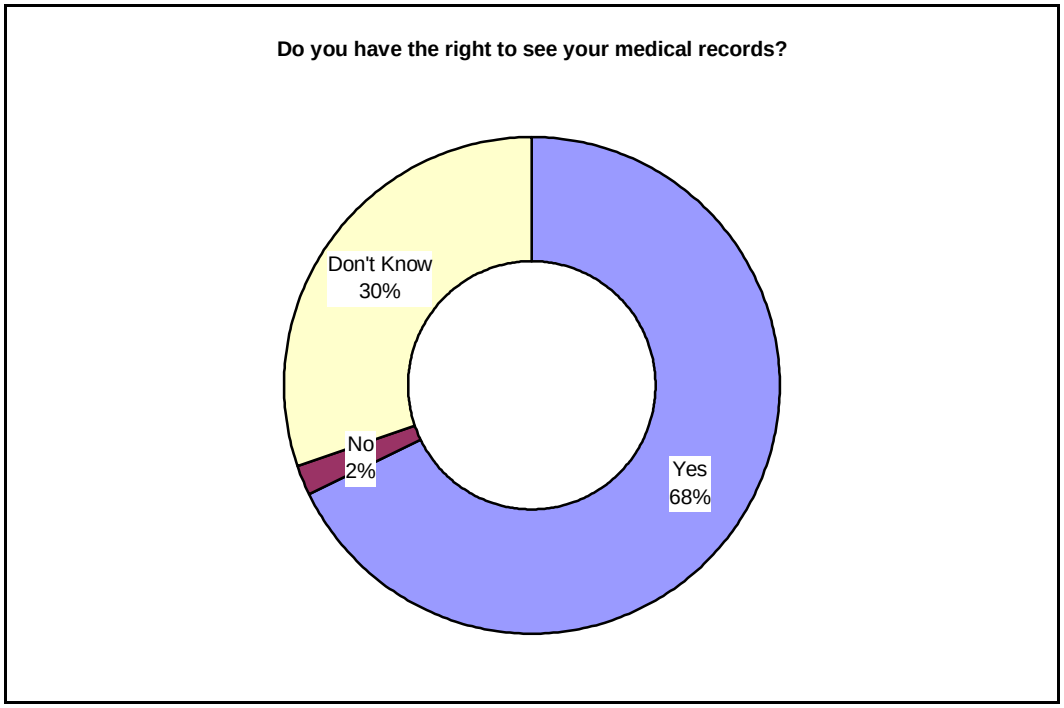

Figure 16 Right to see Medical Records

Only three patients of the patients surveyed had ever tried to see or get a copy of their medical records, and of these two patients were successful in obtaining access to their medical records.

6.4.3 Awareness of Legislation

Patients were then asked if they were aware of any Laws, which exist to protect the privacy and confidentiality of medical information. 75% (82) answered no, they were not aware of any laws that existed. See figure 17. This highlights the fact that Irish patients are largely unaware of Data Protection and Freedom of Information Acts, which protect the privacy and confidentiality of their medical information.

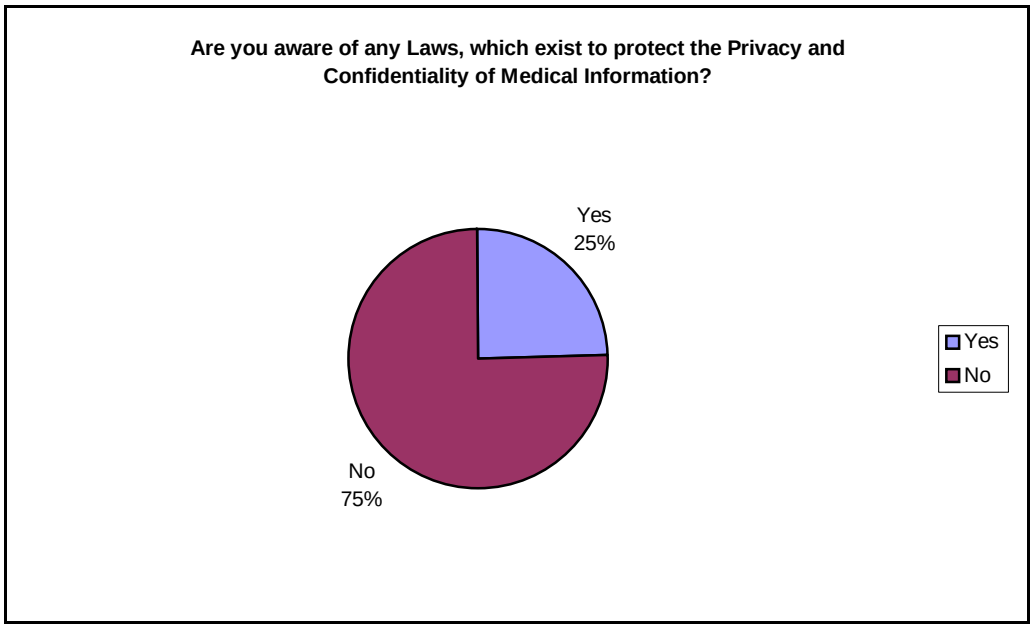

Figure 17 Awareness of Legislation

6.5 Privacy-Protective Behaviour

The survey then questioned the patients' level of privacy-protective behaviour. Several pieces of research have been undertaken (Cheng et al 1993; Sankar et al 2003; Ilene & Goldberg 2002) indicating that when patients believe their privacy is at risk, they will delay or avoid seeking medical attention, withhold information from their doctor, or visit a doctor who is not their own doctor in an effort to preserve their privacy and confidentiality. Patients were asked if they had ever practiced any of the above in three separate questions. The results to these questions are displayed in figure 18. Eight patients (7%) had delayed going to a doctor, twelve patients (11%) said they had withheld information, and twelve patients (11%) had visited a doctor who was not their own doctor. These statistics are slightly lower

than in the US where 13% of patients admitted to engaging in privacy - protective behaviours (National Consumer Health Privacy Survey 2005).

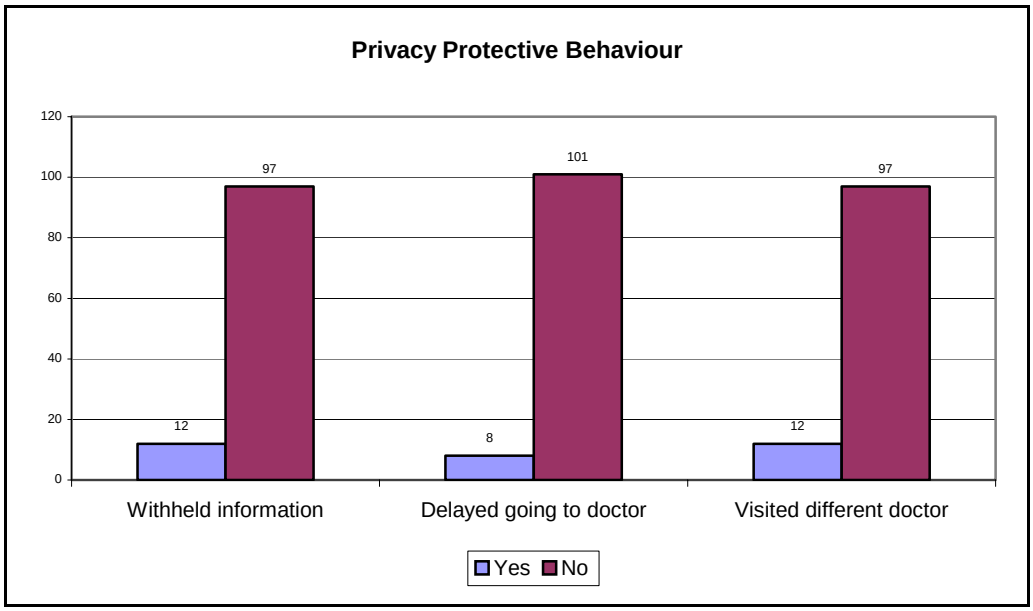

Figure 18 Privacy Protecting Behaviour

Two null hypotheses were then tested to identify whether these tests were statistically significant. The first hypothesis H_0: there is no difference in the answers to whether a patient had withheld information from their doctor because they feared that the information might not be treated confidentially between age groups against H_A: there is a difference, was tested. According to the Kruskal-Wallis Test, the p-value received is 0.0129 which is < 0.05 so therefore the null hypothesis that the age group values received are equal, can be rejected, with the 18 – 24 year old age group being most likely to withhold information.

Then the second hypothesis H_0: there is no difference in the answers to whether a patient had ever delayed going to their doctor because they feared that information might not be treated confidentially between age groups against H_A: there is a difference, was tested. According to the Kruskal-Wallis Test the P-value received is 0.0022 which is < 0.05 so therefore the null hypothesis that the age group values received are equal, can be rejected, with the 18 – 24 year old age group again being most likely to delay going to a doctor.

Generally patients answered yes to more than one of these questions and five patients answered yes to all three questions. Therefore these answers were measured for ‘correlation’ or ‘predictability’. The measure used was ‘Pearson’s Coefficient Correlation’. At its extreme, a correlation of 1 or -1 means that the two variables are perfectly correlated. This means that you can predict the values of one variable from the values of the other variable with perfect accuracy. At the other extreme, an r of zero implies an absence of correlation; there is no relationship between the two variables. This implies that knowledge of one variable gives you absolutely no information about what the value of the other variable is likely to be. The sign of the correlation implies the "direction" of the association.

The results found that there is a linear relationship between the results received in question 8 (withheld information from their doctor) and question 9 (delayed going to their doctor) r =0.80016, therefore, those who withheld information would also very likely have delayed going to the doctor, fearing that information would not be treated confidentially. And similarly between question 8 (withheld information from their doctor) and question 10 (visited a different doctor) but to a lesser extent r =0.4398, with question 9 and question10 being r =0.46298.

To reconfirm the results the Kappa statistic was used. From the Kappa statistic it can be seen that there is excellent (0.78) agreement between the questions 8 and 9 and fair (0.438) between question 8 and 10 and fair (0.4517) between question 9 and 10.
Kappa: < .40: poor; .40-.59 fair; .60-.74 good; >.74 excellent

The kappa statistic was then also used to test the null hypothesis. It is the null hypothesis that their agreement, between questions, is purely by chance. In both cases we can reject the null hypothesis that agreement between questions is due to chance.

Patients were also asked if they had ever decided not to be tested for a medical condition, because they were concerned that others might find out the results. Two patients (2%) answered yes to this question, and 107 patients (98%) answered no.

The Wilcoxon Two-Sample Test was used here to test the null hypothesis H_0: there is no difference in the answers between gender against H_A: there is a difference in their median. In this case the P-value received is 0.0464, which is < 0.05 so therefore the null hypothesis that the gender values received are equal, can be rejected, with males being more likely to answer yes to this question.

The consequences of privacy protecting behaviour can prove costly to the health service, and can be serious for the patient as diagnosis may be inaccurate if the full medical history unknown, and the illness may be prolonged if the onset of treatment is delayed.

6.6 Perception of Security

The patients were then asked how secure they thought their medical records were when they were stored on paper, and then when they were stored on computer. The overall results were similar for both methods of storage. 42% (45) believed that they were secure when stored on paper and 39% (43) believed they were secure when stored on computer. 27% (29) said they were not secure when stored on paper and 31% (33) said they were not secure when stored on computer. In both cases a small minority (2% (2) paper, and 5% (5) computer, answered that they were very secure, and 29% (31) said they were slightly secure when store on paper 25% (27) said they were slightly secure when stored on computer. The combined results are displayed in figure 19

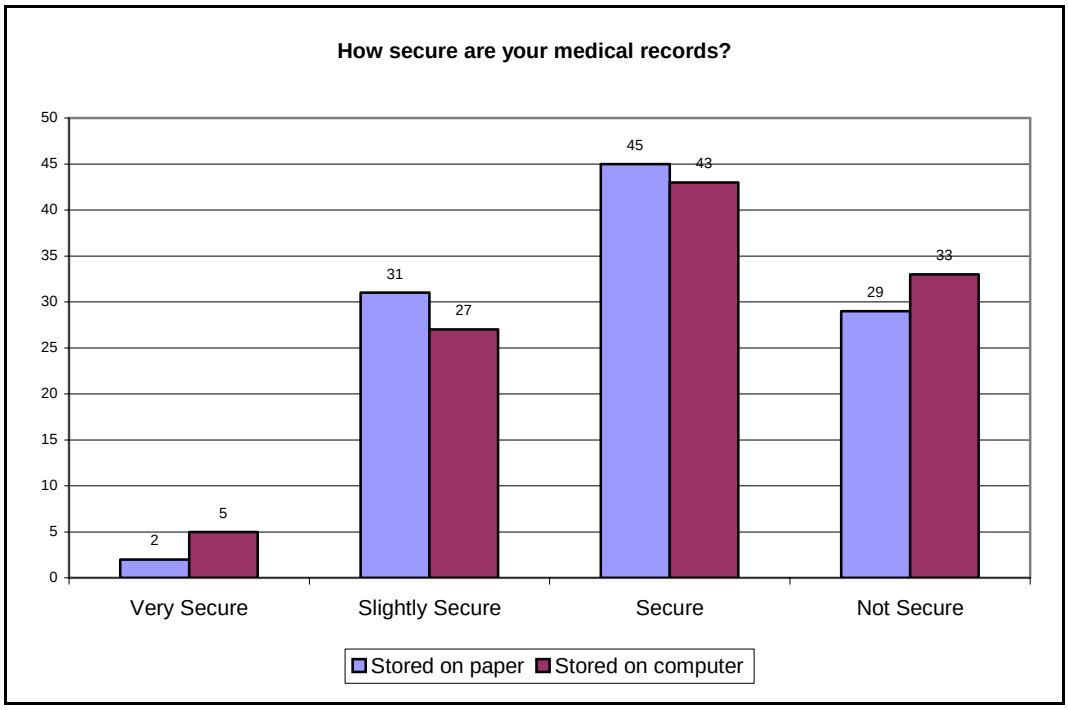

Figure 19 Patient Perception of Security

Answers were then cross checked to determine whether patients thought that one method of storage was more secure than another.
Of the 29% who thought that their medical records were not secure when stored on paper, the majority, 15 patients (51%), still thought that they were not secure when stored on computer.

Only 2 patients (7%) thought that they were very secure when stored on computer, 4 patients (14%) thought that there were slightly secure, and 8 (28%) thought that they were secure when stored on computer. However, the 2 patients who thought they were very secure when stored on paper thought they were not secure when stored on computer.

Of the 31% (33) who thought that their medical records were not secure when stored on computer, the majority, 15 patients (46%), still thought they were not secure when stored on paper.

Only 2 patients (6%) thought that they were very secure when stored on paper, 5 patients (15%) thought they were slightly secure, and 11 (33%) thought that they were secure when stored on paper.

Of the 5 patients who believed computer records to be very secure, 2 thought that paper records were not secure, 2 thought that they were secure and 1 thought they were slightly secure.

The author concluded that the patients' views of security did not differ greatly regardless of the method of storage. To validate this view the hypothesis H_0: there is no difference in the answers to how secure patients think their medical records are when they are stored on paper versus computer against H_A: there is a difference in their median, was tested. In this case the p-value received is 0. 7481 which is > 0.05. As calculating a p-value > 0.05 is the same as saying that we are 95% confident that the results we received from the 'paper question' are no more extreme than those we received from the 'computer question'. Therefore we fail to reject the null hypothesis that the computer and paper values received are equal, thus substantiating the author's conclusion that there is no significant difference between the patients views on security when comparing computer and paper records.

6.7 Incidents

Patients were asked if they were aware of any incidents where the privacy of a person's personal information had been compromised. 17% (18) of patients were aware of such an incident, which is a little lower than for US patients where 24% were aware of an incident. Of these Irish patients, 61% (11) are now more concerned about the privacy of their own health information, with 22% (4) of patients being significantly more concerned, and 39% (7) being slightly more concerned. 39% (7) of patients answered that this information has not changed their level of concern over the privacy of their medical records. See figure 20. When patients in the US were asked the same questions, slightly more patients 24% were aware of and a similar percentage of these (64%), were either significantly or slightly more concerned National Consumer Health Privacy Survey 2005).

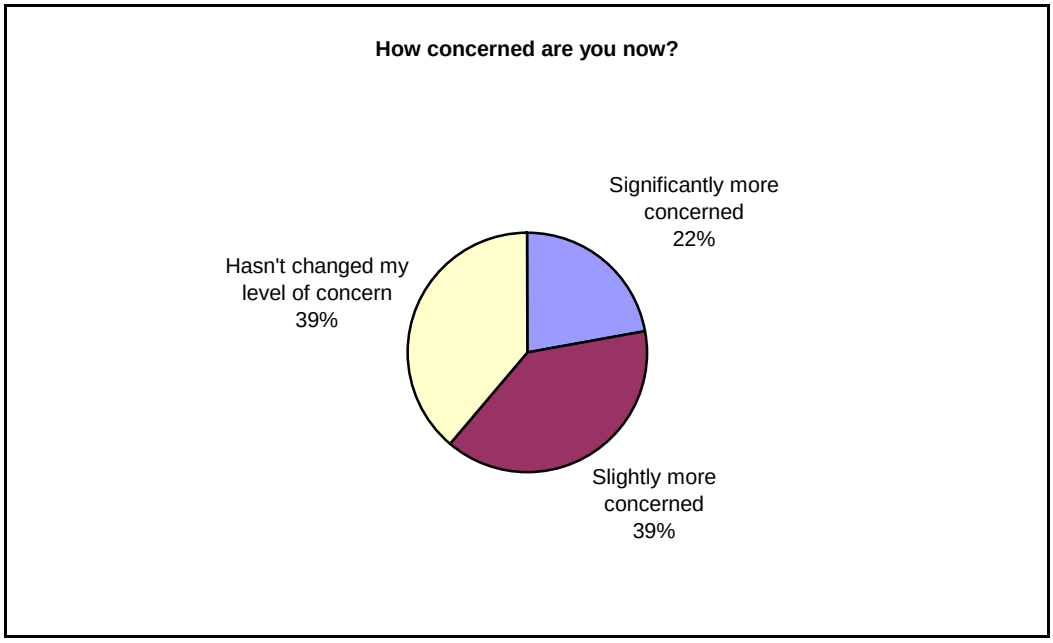

Figure 20 Patient Concerns

6.8 Unique Identifier

Lastly, patients were asked a question to establish their opinion of unique identifiers. The question was '*A **unique identifier** is a personal identification number (like your PPS number), which can be used to link medical records on computer networks by different health care providers. These unique identifiers could be used to make it easier for doctors to find your personal medical records and expedite care, but it could also make it easier for people not involved in your health care to get access to your information. Do you support the use of such unique identifiers?'*

As can be seen in figure 21, 46% (50) of patients supported the use and 54% did not support the use of unique identifiers.

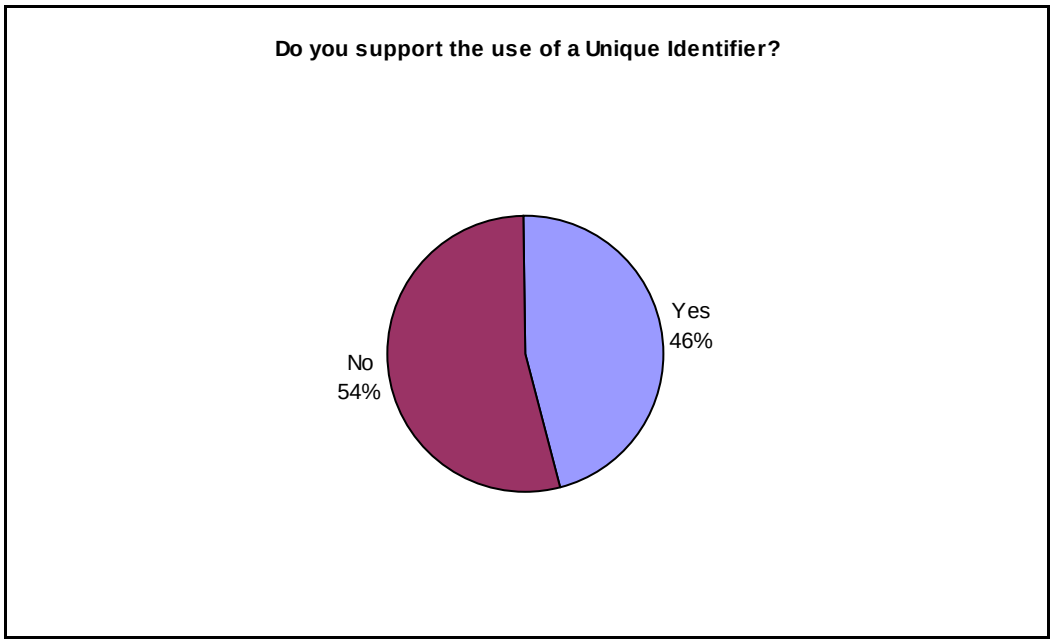

Figure 21 Support for the Unique Identifier

The Wilcoxon Two-Sample and the Kruskal-Wallis tests were both used to test the null hypothesis; H_0: there is no difference in the answers between gender against H_A: there is a difference in their median. In this case the P-values received is 0.018 (wilcoxon), and KW-test which is 0.0373 < 0.05 so therefore we can reject the null hypothesis that the gender values received are equal. The wilcoxon scores test found that males were more likely to agree with the concept of the unique

patient identifier. The author did not identify any reason why the majority rejected the use of unique identifiers.

The patient survey revealed that although the majority of patients do not claim to be concerned regarding the privacy of their medical records, a small number of them practice privacy protecting behaviour, and a large number of patients were not aware of their rights in relation to privacy of their medical records.

7 DISCUSSION

The vision of the EHR is one of a complete longitudinal medical record to which all disciplines involved in patients care would have appropriate access. In keeping with that vision, the author has been encouraged by the findings in her research, to discover that in the majority of organisations surveyed, all disciplines involved in patient care had access to that patient's record. This is a positive finding, indicating that where EHR's are implemented, the facility is there to treat the patient in an all-encompassing manner, with all disciplines being allowed access. However, these effective implementations of EHR with large numbers of health care professionals having access, brings with them increased risks for the integrity of the data contained therein.

All users of the EHR do not necessarily need access to all parts of the record, and the author believes that it is important that system wide access should not be given. Bacon, Moody & Yao (2002) suggest a method of reducing this risk by recommending a role based access control model as a realistic approach for defining access to the EHR, and Blobel et al (2006) also defines an access control model which is user role based. In the author's organisation, role based access is utilised, with only those directly involved in a patients care, having access. From the author's research, it is evident that most organisations have good procedures in place for defining and allocating user access, with most users receiving access according to their role. In very few cases were new rights added, or existing rights removed in the previous year, suggesting that the definition of user rights is accurate from the outset.

Defining role based access and allowing all professionals access to the EHR is seen positively by the author, once all users are hospital employees and are bound by their professional ethical duty and their employee contract to safeguard patient privacy and confidentiality. It is nevertheless a matter of concern that in a minority of organisations, general access is given to users who are not employees. This may allow them to see more than is necessary to care for the patient, which leads the author to question the control that these organisations exercise over the staff that have access to patient data. To address this potential problem, the

author would suggest the introduction of guidelines for staff not directly employed by the hospital. These might include restricted or supervised access and the signing of a confidentiality document, pertaining to information gleaned from patient records.

With regard to the management of user accounts, there were policies in place for setting up and deactivating accounts in most organisations. However, one organisation did not have any policy for removing users access when a user leaves the organisation or moves department, which in practice could mean that a user account is never made inactive. Although this represents a small percentage, this practice could potentially pose serious threats to the confidentiality of patient information, resulting in patient records being inappropriately accessed.

From the author's research, it would appear that privacy is considered an important issue in all organisations surveyed. All respondents replied that seminars on privacy, confidentiality, and data protection issues are held in their organisations. This is an encouraging finding, suggesting that organisations perceive the education of employees in the area confidentiality and privacy as a priority. It is also very positive to note that attendance is mandatory for staff in the majority of organisations. However, only 50% of organisations require users to sign a confidentiality document relating specifically to the EHR. This is most likely due to the fact that in many instances employees sign a confidentiality clause in relation to their contract of employment, and are also subject to global ethical considerations of their respective professions. With regard to confidentiality, the author would like to reiterate the need for confidentiality undertakings by temporary / casual staff.

Most organisations do not attribute a higher level of protection for specific patient groups such as staff members, but they do treat certain information, for example HIV tests, with a higher level of security. Although the author acknowledges that all patient information should be treated confidentially, it is the author's personal opinion that medical records pertaining to staff members and high profile persons should be given a higher level of security, in order to ensure that only those directly involved in the patients care have access. For example allocating a

pseudo name to these patients, that only those directly involved with the patient would know, and auditing access to these records, to recognise any attempts at inappropriate access may achieve this.

Audit trails record users who have accessed the EHR, and identify what functions those users have performed, so that instances of inappropriate access can be identified. The survey found that audit trails are maintained in most organisations, however, actions taken on foot of information extrapolated from audits appear unstructured and weak. Most organisations only investigate following a specific complaint, and although there were very few instances of inappropriate access from either within or outside organisations, some respondents were not aware of the statistics for their own organisation. In these instances, the author would question if there were more instances of inappropriate access than had been reported. Furthermore, where inappropriate access was known to have occurred, disciplinary procedures were not always followed. The author did not identify what disciplinary action different organisations had in place, but would recommend that audit trails are investigated regularly for discrepancies, and that each organisation have a definite policy relating to inappropriate access with defined actions and sanctions for those who contravene the policy.

The author's research demonstrates that most organisations distribute patient information to outside organisations and that this information is often traceable to the patient. Regarding the sharing of personal health information, patients are informed about 'whom' information is shared with, but not about 'what' information is shared. Research has shown that the more sensitive the information, the more sensitive patients are regarding its distribution (NHS, 2002; Flynn et al, 2003; Harris Interactive inc, 2005). The author would also question the legality of this practice, as international data protection legislation examined indicates that patients should be informed about who is collecting their data, the purpose for retaining it, and whom it is distributed to (Data Protection Act, 2003; HIPPA, 2006; Privacy Commissioner, Canada, 2002). Moreover, research has shown that patients will agree to their information being shared once they know what information is shared and whom it is shared with (2004 Willison et al, 2003;

Robling et al). In addition, the author suggests the anoymisation of all data where possible.

None of the organisations surveyed distributed information to patients' employers. This is seen as positive, but the author believes that this is an area that will need monitoring on an ongoing basis. As the EHR develops, information such as the patient's family medical history, and the patients' DNA profile will be recorded. It needs to be appreciated that genetic information is a very powerful tool that could allow an employer to preclude an otherwise qualified individual from getting or keeping a job, on the basis of information gleaned from the DNA profile. Rothstein & Talbot (2006) warn about the effects of compelled disclosures to patients' employers and insurance companies, indicating that disclosure of sensitive health information may result in the inability to obtain employment or insurance and recommend contextual access criteria for disclosures for non-medical purposes. Therefore only information relevant to the employer should be released, following consultation with the patient.

The author also wishes to point out that it is pertinent for organisations to be aware that once data leave their organisation they no longer have control over it. For example, problems have been encountered where pharmaceutical companies have solicited patients promoting alternative medications (Carter, 2000).

In the author's opinion, the most shocking finding from her research was patient's lack of awareness and lack of concern regarding privacy and confidentiality of their medical records. Patients who participated in the survey, were predominately unaware of their rights concerning their personal health records. This was apparent as:

- 75% of those who answered the questionnaire were not aware of any laws which existed to protect the privacy and confidentiality of medical information.
- 32% weren't sure or thought that they did not have the right to see their medical records.
- 53% did not know, or thought that insurance companies or other healthcare organisations could access their personal health information without their knowledge or permission.

In the EHR questionnaire, this lack of concern was evident as most organisations reported that no patient had requested access to their electronic patient record, nor had many patients expressed concern over who had access to their medical records. This finding is supported by findings in the patient questionnaire where more than half the respondents answered that they were not concerned about the privacy of their medical records, and only 3 out of 109 respondents had sought a copy of their medical records. Nevertheless, the majority of patients believe that doctors should ask for patients' permission before sharing information about them with another person. This finding concurs with Wilson et al (2003), who found that patients believe that they should be asked prior to their information being shared this author believes that her finding also portrays the confusion and ambivalence that exists, and highlights a pressing need for appropriate measures to be taken to inform and educate patients.

Having said that, other results appear to indicate patient awareness under certain circumstances, or among specific groups of patients who have been made aware of privacy and confidentiality issues due to life events. For example, there is a level of privacy protecting behaviour practiced, especially among patients in the 18 – 24 year age group, although this is to a lesser extent than in international studies (Cheng et al 1993; Sankar et al 2003; Ilene & Goldberg 2002). This may be due to the fact that younger age groups may have a heightened level of awareness of confidentiality breaches as they have be brought up in the information age and therefore are more alert to technology and the security risks that it imposes. Furthermore, patients who were aware of an instance where another's privacy was compromised, are more likely themselves to be concerned about the privacy of their own health records.

In the author's opinion, the lack of patient awareness and concern can be attributed to a number of reasons. The absence of documented examples of breaches of confidentiality in Ireland has resulted in issues of privacy and confidentiality of medical records not receiving any media attention, with no health organisation yet receiving penalties for being in breach of the Data Protection Acts (Data Protection Commissioner, 2006). All examples found are from international

literature. For example, an incident was reported in the Canadian media recently, where a patient's request that her personal health information be kept private was not met and information regarding her treatment had become known. Following investigation, it was found that her electronic record had been accessed a number of times by a nurse who was not involved in her care (Lake, 2006). The story was published in a Sunday newspaper, and correspondence with the author has revealed that publication of the article had generated immense interest in health privacy and confidentiality. Should a comparable story be covered in the Irish media, the author believes that it would generate a similar result, and patients would certainly become more aware, and possibly more concerned about the privacy and confidentiality of their personal health records.

Additionally, patients have traditionally had an innate trust and sense of comfort in the knowledge that their doctor, health professional or organisation will respect their privacy and will keep their secrets secret. This view is substantiated by the fact that patients believe their medical records to be secure regardless of whether the records are stored on paper or on computer.

Lack of awareness and concern may also be attributed to the fact that health organisations do not make patients aware of information sharing, nor is patient consent sought to share personal health information, thus the patient is not aware of the potential there is to misuse their medical information. As health organisations and professionals collect, store, and share patient health information they are in an ideal position to inform and educate patients regarding their privacy and confidentiality rights. This could be done through the health organisation's patient information booklet, the hospital website, or by displaying information posters in prominent positions such as waiting rooms and clinics throughout the hospital. Consideration could also be given to obtaining patient consent to share information as part of the admission procedure. As well as highlighting patient rights, this would serve to encourage patients to participate in their management and accept responsibility and thereby:

- Encourage patients to take ownership for their own records, and therefore be more involved in their own healthcare.

- Make electronic health records more accurate as patients would be in a position to point out inaccuracies and ensure that corrections were made.

Another interesting finding was that 54% of patients rejected the use of unique identifiers, which are a necessary precursor to EHR implementation. The author was somewhat surprised by this finding, considering the fact that the majority of respondents had replied that they were not concerned about the confidentiality of their records, they believed their records to be secure regardless of whether they stored on paper or computer and although privacy- protecting behaviour was practiced, it was not widespread. There was no further evidence in the research to indicate why this was the case, and the author might only speculate, that replying to the questionnaire had prompted patients to question the power of electronic records and unique identifiers, or perhaps it is just a facet of the Irish personality which resists any attempts by the state to label them.

8 CONCLUSION

The proliferation ICT in healthcare will ultimately mean the transition from paper to electronic records. The arrival of the EHR will without doubt offer many benefits to the clinician, the patient and the public in general. However, implementation of the EHR will also pose many challenges, particularly in the area of privacy and confidentiality, and it is important that the patients' trust is both attained and maintained in order to ensure its success.

The arrival of ICT has lead individual governments to implement laws to protect patient privacy and confidentiality, in the form of data protection and patient privacy legislation. Guidelines have also been developed by European and International initiatives, such as the EU Directive on Data Protection (95/46/EC), and the Organisation for Economic Co-operation & Development's (OECD), as well as organisations such as CEN and ISO.

However, while governments and organisations have taken a proactive role in safeguarding confidentiality and privacy, breaches to patients' confidentiality do still occur. It is also surprising that many patients are so unaware of their privacy rights. These findings highlight the need to monitor access in order to minimise the incidences of confidentiality breaches, and to develop processes to ensure that patients are more aware of their rights.

The challenges are therefore, to limit the scope of disclosures to unauthorised personnel and for non - medical purposes, and to educate patients.

Globally, large sums of money are being spent on ICT in Healthcare. Last year the Health Service Executive (HSE) agreed on a €56m contract, intended to implement an EHR nationally, across all HSE hospitals, clinics and GP surgeries. Considering the information that is already available, and a world of health information and technology which is rapidly changing, the Irish health sector is in a unique situation, where it can address the challenges presented by privacy and confidentiality, and consider them as essential factors to be considered during the implementation of the EHR.

REFERENCES

Adams et al. (2004) Lessons from the Central Hampshire electronic health record pilot project: issues of data protection and consent. **British Medical Journal.** 328 (7444) April, pp.871–874.

Agranoff, M. H. (1991) Controlling the threat to individual privacy. **Journal of Information Systems Management**. 8 (3) Summer, pp.48-52.

An Bord Altranais. (2000) Code of Professional Conduct. 2nd ed. Dublin, An Bord Altranais.

Anderson, J. G. (2000) Security of the distributed electronic patient record: a case-based approach to identifying policy issues. International Journal of Medical Informatics. 60 (2) November, pp.111-118.

Anderson, J. G. (2001) Undermining data privacy in health information. British Medical Journal. 332 (7284) February, pp.442-443.

Bacon, J., Moody. K., Yao, W. (2002) A model of OASIS Role Based Access Control and its Support for Active Security. ACM Transactions on Information and System Security. 5 (4) November, pp492 – 450.

Bakker et al. (1998) Overall Conclusions and recommendations. **International Journal of Medical Informatics.** 49 (1) March, pp135-137.

Barlow-Stewart, K., Keays, D. (2001) Genetic discrimination in Australia. **Journal of Law and Medicine.** 8 February, pp.250-262.

Barrett, M. J. (2000) The Evolving Computerised Medical Record. **Healthcare Informatics.** 17 (5) May, pp.85-88.

Barrows, R. C., Clayton, P. D. (1996) Privacy, Confidentiality, and Electronic Medical Records. **Journal of the American Medical Informatics Association.** 3(2) March / April, pp.139-148.

Basu R, & Sriskandabalan P. (1996) NHS computer network will breach venereal disease regulations. **British Medical Journal.** 311 (7007) September, pp.754.

Berner, E. S., Detmer, D. E., Simborg, D. (2005) Will the Wave Finally Break? A Brief View of the Adoption of Electronic Medical Records in the United States. **Journal of the American Medical Informatics Association.** 12 (1) January / February, pp.3-7.

Billings et al (1992) Discrimination as a result of Genetic Screening, **American Journal of Human Genetics.** 50 (3) March, pp.476-482.

Blobel et al (2006) Modelling privilege management and access control. **International Journal of Medical Informatics.** 75 () August, pp.597-623.

Bourque, L., & Fielder, P. (1995) **How to conduct self-administrated and mail surveys**. 1st ed. London, Sage.

Bowling, A. (1997) **Research Methods in Health.** Philadelphia, Open University Press.

Braunack-Mayer, A. J., Mulligan, Ea. C. (2003) Sharing patient information between professionals: confidentiality and ethics. **Medical Journal of Australia.** 178 (6) March, pp.277-297.

Calcutt, D (1990). **Report of the Committee on Privacy and Related Matters.** London, HMSO.

Carlisle et al (2006) Concerns over confidentiality may deter adolescents from consulting their doctors. A qualitative exploration. **Journal of Medical Ethics.** 32 (3) March, pp133-137.

Carman, D., Britten, N. (1995) Confidentiality of medical records: the patient's perspective. **British Journal of General Practice.** 45 (398), pp. 485-488.

Carter, M. (2000) Integrated electronic health records and patient privacy: possible benefits but real dangers. **Medical Journal of Australia.** 172 (1) January, pp.28-30.

CEN Health Informatics (2006) [Internet], CEN. Available from: <http://www.centc251.org> [Accessed 20th March, 2006].

Cheng T. L. et al. (1993) Confidentiality in health care: a survey of knowledge, perceptions, and attitudes among high school students. **Journal of the American Medical Association**. 269 (11) March, pp.1404-7.

Chhanabhai, P., Holt, A. & Hunter, I. (2006) Health Care Consumers, Security and Electronic Health Records. **Health Care & Informatics Review Online** [Internet], March. Available from: < http://hcro.enigma.co.nz/website/index.cfm > [Accessed 14th August, 2006].

Clamp, S., Felton, D., Heathfield, H (2001) **South Staffordshire EHR Project.** Interim Evaluation Report

Clarke, R (2006) **Data Surveillance and Information Privacy**. [Internet], Australia, Xanax Consultancy Pty. Ltd. Available from: <http://www.anu.edu.au/people/Roger.Clarke/> [Accessed 4th May, 2006].

Data Protection Acts 1998 & 2003. [Internet] Available from: <http://www.dataprotection.ie> [Access 18th August, 2006].

Data Protection Commissioner (2003) **Fifteenth Annual Report of the Data Protection Commissioner**. [Internet] 2003, Available from: <http://www.dataprotection.ie> [Access 18th August, 2006].

Data Protection Commissioner (2004) **Sixteenth Annual Report of the Data Protection Commissioner**. [Internet] 2004, Available from: <http://www.dataprotection.ie> [Access 18th August, 2006].

Data Protection Commissioner (2005) **Seventeenth Annual Report of the Data Protection Commissioner**. [Internet] 2005, Available from: <http://www.dataprotection.ie > [Access 18th August, 2006].

Department of Health and Children. (2004) **Health Information: A National Strategy.** Dublin, Stationary Office.

Electronic Frontiers Australia (2006) **Data Protection Laws / Privacy Acts** [Internet], Australia, Electronic Frontiers Australia. Available from: <http://www.efa.org.au/Issues/Privacy/privacy.html> [Accessed 5th March, 2006]

FIRP (2003) Press Release — **NHS Systems Fail to Protect Patient Confidentiality** [Internet], UK, Foundation for Information Policy Research. Available from: <http://www.fipr.org/press/030205NHS.html> [Accessed 25th April, 2006].

Flynn et al (2003) Patients' concerns about and Perceptions of Electronic Psychiatric Records. **Psychiatry Online** [Internet], November, 54 (11), pp.1539 – 1541. Available from: < http://www.ps.psychiatryonline.org/> [Accessed 14th August, 2006].

Forrester Research Inc. (2005) **National Consumer Health Privacy Survey 2005: Executive Summary.** California HealthCare Foundation [Internet], Available from: <http://www.chcf.org/topics/view.cfm?itemID=115694> [Accessed 14th August, 2006].

Gorlin, R. A. (1999) ed. **Codes of Professional Responsibility: Standards in Business, Health and Law**. 4th ed. Washington, D.C. Bureau of National Affairs.

Gorman, C (1996) Who's looking at your files? Prying eyes find computerised health records an increasingly tempting target. **Time Archive** [Internet] May 6th 1996. Available from: <www.time.com/time/archv/printout/> [Accessed 23rd July, 2006].

Gostin, O. (1993) Law and Medicine. **Journal of the American Medical Association**. 270 (2) July, pp.225-226.

Gregory Dawes, B. S. (2001) Patient Confidentiality takes on a new meaning. **AORN Journal.** 73 (3) March, pp.596-600.

Grimson, J., Grimson, W. & Hasselbring, W. (2000) The SI Challenge in Health Care. **Communications of the ACM** [Internet], June, 43 (6), pp.49-55. Available from: < http://doi.acm.org/10.1145/336460.336474 > [Accessed 14th August, 2006].

Harris Interactive inc. (2005) How the public sees Health Records and an EMR programme. **Programme on Information Technology, Health Records and an EMR programme.** February 16th.

Hassol et al (2004) Nursing constraint models for electronic health records: A vision for domain knowledge governance. **Journal of the American Medical Association** 11 (6) November – December, pp.505-513.

Hodge, J.G., Gostin, L.O., Jacobson, P.D. (1999) Legal Issues Concerning Electronic Health Information. **Journal of the American Medical Association.** 282 (15) October, pp.1466–1471.

Holahan, C. J. & Slaikeu, K. A (1977) Effects of contrasting degrees of privacy on client self-disclosure in a counselling setting. **Journal of Counselling Psychology.** 24 (1) January, pp.55-59.

Ilene, V., Goldberg, J.D. (2000) Electronic Medical Records and Patient Privacy. **The Health Care Manager.** 18 (3) March, pp.63-69.

International Organisation for Standardisation (2005) [Internet], ISO. Available from: <http://www.iso.org/> [Accessed 5th March, 2006].

Jenkins, G., Merz. J.F., & Sankar, P. (2005) A qualitative study of women's views on medical confidentiality. **Journal of Medical Ethics.** 31 (9) September, pp.499–504.

Jones, C. (2003) The utilitarian argument for medical confidentiality: a pilot study of patients' views. **Journal of Medical Ethics.** 29 (6) December, pp. 348-352.

Kane, E & O' Reilly-de-Brun, M. (2001) **Doing your own Research.** London, Boyars.

Kane, E. (1990) **Doing your own Research.** 5th ed. London, Boyars.

Kerr, K., (2004) The Electronic Health record in New Zealand. **Health Care & Informatics Review Online.** [Internet], March. Available from < http://hcro.enigma.co.nz/> [Accessed 14th August, 2006].

Kumar, R. (2005) **Research Methodology: A Step-by-Step Guide for Beginners.** 2nd ed. London, Sage.

Lake, H. (2006) Her Life was an open Book **Ottowa Sun.** [Internet] Available from: <http://ottsun.canoe.ca/News/OttawaAndRegion/2006/08/13/1752102-sun.html> [Accessed 19th August, 2006].

Law Reform Commission (1998) **Report on Privacy: Surveillance and the Interception of Communications.** Dublin, Law Reform Commission,

Layman, E. (2003) Health Informatics Ethical Issues. **The Health Care Manager.** 22 (2) January - March, pp.2-15.

Low, L King, S.; Wilkie, T. (1998) Genetic discrimination in life insurance: empirical evidence from a cross sectional survey of genetic support groups in the United Kingdom. **British Medical Journal** 317(7173):December, pp.1632–1635.

Madden, D. (2002) **Empowering Health Information: Medico-Legal issues.** Medico Legal Journal of Ireland. 8 pp.7-13.

Marks et al, (1995) The Prevalence of Patient Disclosure of HIV Infection to Doctors. **American Journal of Public Health.** 85 (7) July, pp.1018-1019.

McColl et al (2001) Design and use of questionnaires: a review of best practice applicable to surveys of health service staff and patients. **Health Technology Assessment** [Internet] 5 (31). Available from: <http://www.ncchta.org/execsumm/summ531.htm> [Accessed 26th July, 2006).

McKinney et al, (2005) A feasibility study of signed consent for the collection of patient identifiable information for the national paediatric audit database. **British Medical Journal,** 330 (7496) April, pp.877-879.

Meade, B. (2002) **A Data Privacy Code of Practice for Irish General Practice**. MSc thesis, Trinity College, Dublin.

Meadows, K. (2003) So you want to do Research? 5: Questionnaire Design. **British Journal of Community Nursing** 8 (12), pp.562-570

Mechanic, D. & Meyer, S. (2000) Concepts of trust among patients with serious illness. **Social Science & Medicine.** 51 (5) September, pp.657-658.

Meijden et al. (2001) Development and Implementation of an EHR: How to encourage the user. **International Journal of Medical Informatics.** 64 (2-3) December, pp.173-185.

Miller, P. S. (1998) Genetic Discrimination in the workplace **Journal of Law, Medicine & Ethics** 26 (3) Fall, pp189-198.

Moneyham et al (1996) Perceptions of stigma in women infected with HIV. **Aids, Patient Care and STD's.** 10 (3) June, pp.162-167.

Mulligan, E., Paterson, M. (2003) Patients rarely detect breaches of confidence. **Australian Health Review.** 26 (3) December, pp.73-78.

Mulligans, E. A., Braunack-Mayer, A. (2004) Why protect confidentiality in health records? A review of research evidence. **Australian Health Review.** 28 (1) September, pp. 48-55.

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

Network Research Group (1999) **The AIM SEISMEID Project.** [Internet], UK, Network Research Group. Available from: < http://www.ishtar.org.uk/> [Accessed 14th August, 2006].

NHS (2001) Defining **Electronic Records** [Internet], Department of Health. Available from: < http://www.connectingforhealth.nhs.uk/> [Accessed 1st March, 2006].

NHS Information Authority in conjunction with the Consumers Association and Health Which? (2002) **Share with Care: Peoples Views on Consent and Confidentiality of Patient Information.** Final Report October 2002. Birmingham, NHSIA, Information Authority.

Nolan, L. (2005) **Probe into who looked at files on Dolores**. Sunday Independent 4th December 2005.

O'Brien, J., Chantier, C. (2003) Confidentiality and the duty of care. **Journal of Medical Ethics.** 29 (1) February, pp.36-40.

Office of the Information Commissioner (2003) **Guide to the FOI Act.** [Internet] Available at: < http://www.oic.gov.ie> [Accessed 14th August, 2006].

Officer of the Privacy Commissioner of Canada (2002) **The Personal Information Protection and Electronic Documents Act.** [Internet], Canada, Officer of the Privacy Commissioner of Canada. Available from: <http://www.privcom.gc.ca/> [Accessed 14th August, 2006].

Ohno-Machado, L., Silveira, P.S.P., Vinterbo, S. (2004) Protecting patient privacy by quantifiable control of disclosures in disseminated databases. **International Journal of Medical Informatics.** 73 (7-8) August, pp.599-603.

Public Broadcasting Service (PBS) (2001) **Hippocratic Oath – Classical Version.** [Internet], US, PBS. Available from:<http://www.pbs.org/> [Accessed 15th August, 2006].

Pyper et al. (2004) Patients' experiences when accessing their on-line electronic patient records in primary care. **British Journal of General Practice.** 54 (498) January, pp.38-43.

Rindfleisch, T. C. (1997) Privacy, Information Technology, and Health Care. **Communications of the ACM** [Internet], August, 40 (8), pp.94-100. Available from: <http://doi.acm.org/10.1145/257874.257896> [Accessed on 14th August, 2006].

Robling et al 2004 Public Attitudes towards the use of primary care patient record data in medical research without consent: a qualitative study. **Journal of Medical Ethics.** 30 (1) February, pp.104-109.

Rothstein, M. A. & Talbott, M, K (2006) Compelled Disclosure of Health Information: Protecting against the greatest potential threat to Privacy. **Journal of the American Medical Association,** 295(24) June, pp. 2882 – 2885.

Saba, V. K., & McCormick K. A., (2001) **Essentials of Computers for Nurses.** 3rd ed, New York, McGraw-Hill

Schloeffel, P. (2004) Current EHR Developments: an Australian and International Perspective. **Health Care & Informatics Review Online.** [Internet] September Available from < http://hcro.enigma.co.nz/> [Accessed 14th August, 2006].

Schoenberg, R., Safran, C. (2000) Internet based repository of medical records that retains patient confidentiality. **British Medical Journal.** 321 (7270) November, pp.1199-1203.

Shalala, D. (1997) **Protecting Privacy of Health Information.** Address to National Press Club, Washington, D.C.

Terry, N. P. (2004) Electronic health records: International. Structural and legal perspective. **Journal of Law & Medicine.** 12, pp. 26-39.

The Oxford English Dictionary. (1989) vol. 5 2nd ed. Oxford, Oxford University Press.

Centre for Health Informatics (2005) **EHR** [Internet], Dublin, Trinity College. Available from: <http://www.cs.tcd.ie/chi/projects/ehrmeta.html> [Accessed 13th April, 2006].

University of Miami (2005) **Privacy / Data Protection Project** [Internet], USA, University of Miami. Available from: <http://www.privacy.med.miami.edu/index.htm> [Accessed 10th March, 2006].

Veronesi, J. F. (1999) Ethic Issues in Computerised Medical Records. **Critical Care Nursing Quarterly.** 22 (3) November, pp.75-80.

Waegemann, C. P (2003) EHR vs. CRP vs. EMR. **Healthcare Informatics Online** [Internet] May, pp.1-4. Available from: <http://www.healthcare-informatics.com> [Last Accessed 14th August, 2006].

Waegemann, C. P. (1996) IT Security: developing a response to increasing risks. **International Journal of Bio-Medical Computing.** 43 August, pp. 5-8.

Whiddett et al. (2006) Patients' attitudes towards sharing their health information. **International Journal of Medical Informatics.** 75 (7) July, pp.530-541.

Wilson et al. (2003) Patients' consent preferences for research uses of information in electronic medical records: interview and survey data. **British Medical Journal.** 326 (7386) February, pp.373-377.

Woods, K. M & McNamara, J.R (1980) Confidentiality: its effect on interviewee behaviour. **Professional Psychology** 11 (5) October, pp.714-721.

Appendix 1: Covering Email (Hospital Survey)

Thank you for agreeing to participate in my research.

As previously discussed I am undertaking an MSc in Health Informatics in Trinity College Dublin. I have chosen patient privacy and confidentiality in Electronic Healthcare Records (EHR) as my area of research for my dissertation, my research question being 'Is Patient Privacy and Confidentiality Adversely Affected when an Electronic Health Record is Introduced?

Attached please find my questionnaire, which should take no more than 10 minutes to complete.

The ISO defines an Electronic Health Record as 'a repository of information regarding the health of a subject of care, in computer processable 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 my study I will use this definition.

Please note that an EHR does not need to be implemented hospital wide for you to complete the questionnaire. The fact that an EHR is implemented in a particular area or for a particular specialty will suffice.

Any information or results gained from the completed questionnaire will be used solely for the purpose of this dissertation and will remain completely anonymous.

The closing date for return is Friday 14th of April. To complete:

1. Please save the completed questionnaire by selecting 'SAVE AS' in the 'FILE' menu and select the location to save it.
2. Compose a new e-mail, addressing it to flanagak@cs.tcd.ie or by replying to this e-mail
3. Attach the saved questionnaire to the newly composed mail.
4. Click 'SEND'

If you would like a copy of the results of this questionnaire please mail me and let me know - as soon as I have completed my analysis I will do so!

Kind Regards,
Katherine Flanagan

Appendix 2: Hospital Questionnaire

Survey of Organisations with an Electronic Health Record (EHR)

This questionnaire is intended to ascertain the level of patient privacy and confidentiality attributed to patient data where an EHR has been implemented. The questionnaire is divided into 4 sections. All questions should be answered, and require a tick in one or more boxes. Some answers require you to specify further details. It should take no longer than 10 minutes to complete, and can be returned by email. I wish to thank you in advance for your participation.

Section 1 – General Information

1.1 How long has your organisation been using an EHR?

☐ < One year ☐ 1 - 5 years

☐ > 5 years ☐ In Development

If '*In development'*, when do you plan to implement?

1.2 The EHR was:

☐ Purchased from a vendor, i.e. 'off the shelf'

☐ Developed specifically by a vendor, i.e. 'bespoke'

☐ Developed 'in-house'

☐ Other Please specify:

1.3 How many patient records are held on the EHR's database? (approx)

1.4 Which department do you work in?

☐ IT Department ☐ Clinical Department

☐ Medical Records

☐ Other Please specify:

1.5 Do all disciplines that deal with patients, have access to those patients EHR's?

☐ Yes ☐ No

☐ If you answered 'no' please specify what discipline does not have access and why?

Section 2 – Data Protection

2.1 *Patient information (demographic and/or clinical) recorded in the EHR is distributed to:*

- ☐ Government Agencies and Departments
- ☐ Commercial Organisations
- ☐ Voluntary Organisations e.g. Cancer Research
- ☐ Employers
- ☐ None of the above

2.2 *Is data distributed to outside organisations, traceable to the patient?*

- ☐ Always
- ☐ Sometimes
- ☐ Never
- ☐ Not Applicable

2.3 *Training seminars on privacy, confidentiality, and data protection are held in the organisation:*

- ☐ Once a year
- ☐ Less than once a year
- ☐ Whenever deemed necessary
- ☐ Never

2.4 *Is it mandatory for users to attend these seminars?*

- ☐ Yes, prior to user access being granted
- ☐ Yes, within a given period of joining the organisation
- ☐ No, seminars are not mandatory

2.5 *Do users sign a confidentiality document specifically relating to the EHR?*

☐ Yes ☐ No

2.6 Are audit trails maintained to monitor for inappropriate user access?

☐ Yes, but only investigated when there is a specific complaint

☐ Yes, and regularly reviewed for breaches of patient privacy/confidentiality

☐ No, audit trails are not maintained

2.7 *Are 'Staff' or 'VIP' records granted a higher level of protection than other records?*

☐ Yes

☐ No

2.8 In the past 12 months how many incidences of inappropriate access to patient information (by someone from within the organisation) have occurred?

☐ None ☐ Not Known

☐ < 10 ☐ 10 - 50

☐ 50 – 100 ☐ >100

2.9 In the past 12 months how many incidences of inappropriate access to patient information (by someone from outside the organisation) have occurred?

☐ None ☐ Not Known

☐ < 10 ☐ 10 - 50

☐ 50 – 100 ☐ >100

2.10 In how many instances has disciplinary procedures been followed?

☐ In all instances

☐ In some instances

☐ Never

2.11 Is all information recorded on a patient given the same level of security, for example are HIV test results (or similar) available as freely as a Full Blood Count result?

☐ Yes, the same level of security applies

☐ No, a higher level of security exists

☐ Other Please specify:

Section 3 – User Access

3.1 Who is responsible for defining user access to the EHR?

☐ IT Manager

☐ Database Manager

☐ Systems Administrator

☐ Clinical Director or person nominated by him / her

☐ Sub-Committee (or similar) developed to define user roles

☐ Other Please specify:

3.2 How are users granted access to the EHR?

☐ The user requests access him/herself

☐ The users manager requests access for him / her

☐ As per hospital policy, a user enrolment document (or similar) is completed and passed to the person responsible for creating new user accounts

☐ Other Please specify:

3.3 How are user account's made inactive when they leave or move to another role within the organisation?

☐ As per hospital policy, the IT department is notified and access is terminated

☐ Access is terminated when the user account has been inactive for a specific time period

☐ User accounts are never made inactive

☐ Other Please specify:

3.4 What level of access is assigned to users who are not members of the organisation e.g. agency nurses, locum's?

☐ Access is not given

☐ General access is given, which may allow them to see more than necessary to carry out their role in caring for the patient

☐ Basic access is given, which may prevent them from seeing all that they require to carry out their role in caring for the patient

☐ Access is given according to their role?

3.5 How are access levels managed?

☐ Role based according to the users role in the organisation

☐ Discipline based according to discipline

☐ Speciality based according to speciality

☐ All users have full access to the EHR

☐ Other Please specify:

3.6 Are all levels of a discipline allocated the same access, e.g. all nurses regardless of grade, all doctors, regardless of whether consultant or intern?

☐ Yes, all grades have the same access

☐ No, more senior grades have more access

☐ Other Please specify:

3.7 Approximately how often do users request increased user rights so that they can see more patient information?

☐ Once per month

☐ Once every 6 months

☐ Once every year

☐ This has never happened

3.8 How many times in the last 12 months have access rights been removed from users on the grounds that they could view more patient information than was deemed necessary?

☐ *Never*

☐ *1 – 5 times*

☐ *>5 times*

Section 4 – Patient Information and Consent

4.1 Are patients informed of the organisations that information about them might be distributed to?

☐ Yes
☐ No
☐ Information is not distributed to outside organisations

4.2 Are patients informed about what information recorded about them might be shared with other health professionals or passed to outside organisations?

☐ Yes
☐ No
☐ Information is not distributed to outside organisations

4.3 Do patients give written consent to information about them being shared?

☐ *Yes* ☐ *No*

4.4 Is there an 'opt out' clause whereby patients can choose not to have their information shared or certain information not shared?

☐ Yes ☐ No

4.5 In the last 12 months how many patients have requested access to their electronic patient record

☐ None ☐ < 10
☐ 10 - 50 ☐ > 50

4.6 In the last 12 months how many patients have expressed concern over who has access to their medical records?

☐ None ☐ < 10
☐ 10 – 50 ☐ > 50

4.7 Is there a procedure where by the patient can request that information can be corrected and/or removed?

☐ Yes ☐ No

Please feel free to enter any additional comments here:

Instructions for Returning Completed Questionnaire

- Please save the completed questionnaire by selecting **'SAVE AS**' in the '**FILE'** menu and select the location to save it.
- Compose a new e-mail, addressing it to flanagak@cs.tcd.ie or by replying to my first e-mail
- Attach the saved questionnaire to the newly composed mail.
- Click '**SEND'**

Disclaimer: *Any information or results gained from the completed questionnaire will be used solely for the purpose of this dissertation and will remain completely anonymous.*

Appendix 3: Covering Letter (Patient Survey)

11 Oakmount
Tower
Blarney
Co Cork
21st May 2006

RE: MSC Health Informatics

Dear Participant,

I am studying for a Masters in Science (Health Informatics) in Trinity College Dublin. In part fulfilment of the MSc, I am undertaking research in the area of Patient Privacy and Confidentiality with respect to Electronic Health Records.

As a user or potential user of the health service I am interested in your views on the privacy and confidentiality of your personal health information. A questionnaire has also been sent to hospitals where Electronic Health Records are in use, the intention being to compare the expectations of the public, with the actual practices in these hospitals.

The questionnaire should take no more than 5 minutes of your time to complete and can be returned to me, sealed, in the envelope provided. Any information or results gained from the completed questionnaire will be used solely for the purpose of my research and will remain completely anonymous.

Your participation in this survey is very important for my research.

Thank you for your time and contribution,

Yours Sincerely,

_____

Katherine Flanagan

Appendix 4: Patient Questionnaire

Please tick (✔) the appropriate box:

1. My age in completed years is:

   <18years☐ 18 – 24☐ 25 – 40☐ 41 – 60☐ >60☐

2. I am: Male☐ Female☐

3. What type of information do you think is kept in your medical record?

   Your PPS Number ☐
   Your current medical condition ☐
   Previous medical conditions ☐
   Health insurance information ☐
   Information about where you work ☐
   Family health history ☐
   Your doctor's personal notes or observations ☐
   Procedures that have been done ☐
   Medications you currently take ☐
   Medications you have taken in the past ☐
   Past health expenses and payment information ☐
   Your risk of developing certain conditions in the future ☐

4. How concerned are you about the privacy of your medical health records?

   Very concerned ☐
   Concerned ☐
   Not very concerned ☐
   Not at all concerned ☐

5. As far as you know, do you have the right to see your medical records?

   Yes☐ No☐ Don't Know☐

6. Have you ever tried to see or get a copy of your medical records?

   Yes☐ No☐

7. If yes, were you successful is getting access to your medical records?
   Yes☐ No☐

8. Have you ever, withheld information from your doctor because you feared that the information might not be treated confidentially?
   Yes☐ No☐

9. Have you ever delayed going to your doctor because you feared that information might not be treated confidentially?
   Yes☐ No☐

10. Have you ever visited a doctor who is not your own doctor, with a complaint that you did not wish to be recorded in the medical notes at your own doctors?
    Yes☐ No☐

11. As far as you know, can insurance companies, other healthcare organisations, access your personal health information without your knowledge or permission?
    Yes☐ No☐ Don't Know☐

12. Do you think your doctor should ask for your permission before disclosing information about you to another person?
    Yes☐ No☐ Don't Know☐

13. Have you ever decided not to be tested for a medical condition because you were concerned that others might find out the results?
    Yes☐ No☐

14. Have you ever asked your doctor not to write down your health problem in your medical records, or asked the doctor to put a less serious or less embarrassing condition into the record than was actually the condition?
    Yes☐ No☐

15. How secure do you think your medical records are when they are stored on paper?

Very secure	☐	Secure	☐
Slightly Secure	☐	Not Secure	☐

16. How secure do you think your medical records are when they are stored on computer?

Very secure	☐	Not very secure	☐
Slightly Secure	☐	Not Secure	☐

17. Are you aware of any instances where the privacy of a person's personal information was compromised?

Yes☐ No☐

18. If you answered **yes** to question 17, how have these instances affected your concern over the privacy of your medical records?

I am significantly more concerned ☐
I am slightly more concerned ☐
It hasn't change my level of concern ☐
I am slightly less concerned ☐
I am significantly less concerned ☐

19. Are you aware of any Laws, which exist to protect the privacy and confidentiality of medical information?

Yes☐ No☐

20. A **unique identifier** is a personal identification number (like your PPS number), which can be used to link medical records on computer networks by different health care providers. These unique identifiers could be used to make it easier for doctors to find your personal medical records and expedite care, but it could also make it easier for people not involved in your health care to get access to your information. Do you support the use of such unique identifiers?

Yes☐ No☐