A PRIVACY FRAMEWORK AND GUIDELINES FOR PSYCHIATRIC BEHAVIOURAL MONITORING SYSTEM

RUSYAIZILA RAMLI

UNIVERSITI SAINS MALAYSIA
2016

A PRIVACY FRAMEWORK AND GUIDELINES FOR PSYCHIATRIC BEHAVIOURAL MONITORING SYSTEM

by

RUSYAIZILA RAMLI

**Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy**

March 2016

ACKNOWLEDGEMENTS

Foremost, I would like to thank Allah SWT for the given chance to complete and submit this thesis. My heartiest appreciation goes to my parents and siblings for all the spirit, support and assistance throughout these tough years. To my beloved husband Nasrul Naim, thank you for supporting me. To my son and daughter Malique and Lisa, the pillars of my strength, which made me realised that achieving the highest level of education is something that I can be proud of. Not to forget my in-laws and my fellow colleagues and friends, you know who you are; I could not express how grateful I am to have such wonderful people around me, providing ideas and comments in ensuring this thesis a success. They kept me going whenever I was feeling down or having second thought of completing the most challenging part of my studies.

Million thanks to Dr. Nasriah Zakaria and Dr. Putra Sumari as my supervisors. It is an honour to carry out this research under the guidance of a true advocate and prolific researcher in the field of Information System.

I would like also to take this opportunity to express my deepest gratitude to all participants who were the key player in this research. Without them, this write up would almost be impossible.

To my sponsor, specifically Ministry of Higher Education, Malaysia, I am truly grateful for their financial support over the last five years for my post-graduate studies. Finally, a great thanks to Nursakirah who helped me a lot for the submission process as I am away from Malaysia, I do really appreciate her kind help that had been a major part of the success in completing this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BP	Blood Pressure
ECG	Electrocardiogram
CCTV	Closed-Circuit Television
EHR	Electronic Health Record
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
IRB	International Review Board
IS	Information System
ISD	Information System Development
JEPeM	Jawatankuasa Etika Penyelidikan (Manusia) of USM
MIS	Medical Information System
NHS	National Health Services
OCD	Obsessive-Compulsive Disorder
PBMS	Psychiatric Behaviour Monitoring System
PDP	Personal Data Protection
PHI	Protected Health Information
PHS	Patient-Centred Health IT Services
PPG	Photoplethysmography
PTSD	Post-Traumatic Stress Disorder
P3HR	Privacy-Aware Patient-Controlled Personal Health Record
SDLC	System Development Life Cycle
WHO	World Health Organisation

LIST OF PUBLICATIONS

1) Ramli, R. & Zakaria, N. (2013) Privacy Issues in a Psychiatric Context: Applying the ISD Privacy Framework to a Psychiatric Behavioural Monitoring System. Journal of AI & Society.

2) Ramli, R., Zakaria, N. & Mustaffa, N. (2013) The Methodology of Interviewing Psychiatric Patients: to Know Patient's Privacy Concern in Behaviour Monitoring System. The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013). Xianggang, Hong Kong, SDIWC Digital Library.

3) Ramli, R., Zakaria, N., Sultan, N. A. H., Mustaffa, N. & Sumari, P. (2012) Privacy Issues in a Psychiatric Context: Applying the Information Systems Development Privacy Framework to a Psychiatric Behaviour Monitoring System. International Stability and Systems Engineering Conference. Ireland.

4) Ramli, R., Zakaria, N., Muton, N. A. R., Talib, N. A., Abdullah, N. A. & Sultan, N. A. H. (2010) Qualitative Data Analysis Training for Graduate Students: Lessons Learned. IN LIM, J. (Ed.) International Workshop on Computer Aided Qualitative Research Asia 2010. Kuala Lumpur, Malaysia, Merlien Institute.

5) Ramli, R., Zakaria, N. & Sumari, P. (2010) Privacy Sensitive Architecture for Psychiatric Behaviour Monitoring System. Service Science and Innovation Doctoral Colloquium. Staffordshire University, UK.

6) Ramli, R., Zakaria, N. & Sumari, P. (2010) Privacy Issues in Pervasive Healthcare Monitoring System: A Review. International Conference on Computer, Electrical, and Systems Science, and Engineering, Singapore. ICCESSE 2010. Singapore.

7) Ramli, H., Saran, N. A. A., Sharif, M. R., Zakaria, N. & Ramli, R. (2010). A Study on Privacy Settings in Social Networking Sites among College Students. International Conference on Science & Technology. Penang.

KERANGKA KERJA PRIVASI DAN GARIS PANDUAN UNTUK SISTEM PEMANTAUAN PERLAKUAN PESAKIT PSIKIATRI

ABSTRAK

Isu-isu berkaitan dengan privasi seringkali menjadi topik perbincangan di kalangan mereka yang terbabit secara langsung atau tidak di dalam bidang perubatan dan juga pesakit-pesakit apabila isu-isu ini dikaitkan dengan sistem pemantauan perlakuan pesakit mental. Melalui kaijan-kajian terdahulu dan berdasarkan Akta Perlindungan Data Peribadi (2010), kami telah mengenalpasti beberapa perkara yang menimbulkan kebimbangan di kalangan pesakit-pesakit berkaitan dengan isu ini apabila kajian dilakukan di sebuah hospital universiti A. Kajian ini menggunakan teori konstruktivisme sosial di mana setiap pesakit yang terbabit ditemuramah dan data yang diperolehi melalui temuramah dan pemerhatian dikajiselidik menggunakan kaedah analisis kualitatif. Kerangka kerja pada permulaan kajian terdiri daripada lima faktor iaitu Fizikal, Sosial, Informasional, Psikologikal dan Global yang mana setiap satunya mempunyai aspek masing-masing. Bagaimanapun, kerangka kerja awal tersebut telah dimodifikasi berdasarkan keputusan dari analisis yang telah dilakukan. Ciri-ciri Akses Fizikal dan Had Batasan (Badan) yang menjadi aspek-aspek di dalam Faktor Fizikal di dalam kerangka kerja awal ternyata mempunyai kesamaan yang ketara maka kedua-duanya disatukan menjadi Had Batasan (Badan). Aspek-aspek Intimasi (Luaran) dan Intimasi (Dalaman) yang menjadi sebahagian daripada Faktor Sosial didapati mempunyai ciri-ciri yang hampir serupa dan dijadikan di bawah satu aspek iaitu Intimasi. Aspek Autonomi yang menjadi sebahagian daripada Faktor Psikologikal di dalam kerangka kerja awal didapati sebenarnya merupakan aspek ulangan di dalam Faktor Sosial, maka aspek ini dikeluarkan dari Faktor Psikologikal. Di bawah Faktor Psikologikal, kajian mendapati aspek Keintiman Emosi dan Kreativiti tidak menepati ciri-ciri yang dikehendaki. Keorganisasian dan Karakter-karakter Personal dan Keperluan Keadaan juga didapati tidak bersesuaian. Garis panduan privasi dihasilkan untuk membantu pembangun sistem memahami kerangka kerja yang berkaitan dan seterusnya mengaplikasikannya dengan lebih tepat di dalam membangunkan sistem pemantauan pesakit. Kajian ini telah menyatukan garis-panduan privasi dengan System Pembangunan Kitar Hidup untuk membolehkan pembangun aplikasi membina system pemantauan pesakit yang sensitif terhadap privasi.

A PRIVACY FRAMEWORK AND GUIDELINES FOR PSYCHIATRIC BEHAVIOURAL MONITORING SYSTEM

ABSTRACT

Privacy issues are frequently discussed among healthcare providers and end-users of healthcare applications as these sensitive issues are related to the use of a psychiatric behavioural monitoring system. We systematically reviewed literature on privacy issues and the Personal Data Protection Act (PDP) 2010 Malaysia to identify privacy concerns among Malaysian patients admitted to the Psychiatric Ward at a Teaching Hospital A. This study uses the social constructivism paradigm, through case study strategy of inquiry and the data was collected through interviews and observations. The study adapted privacy framework that consisted of five factors which are Physical, Social, Informational, Psychological and Global. It is found that two aspects under Physical which are Physical Access and Territoriality (Body) measured the same aspect and they were combined as one aspect called Territoriality (Body). Intimacy (External) and Intimacy (Internal), two sub-aspects under Social were also found to be very much alike and were combined into Intimacy. Autonomy, part of the Psychological, was found to be repeated in Social and was removed from the privacy framework. Under Psychological, our findings showed that Confiding and Creativity were not supported by the data. Organisational and Personal Characteristics and Circumstance were also not supported by the data. The end product is a privacy guidelines produced to help system developers better understand the framework and thus apply it more accurately to the design of psychiatric patients' monitoring systems. This study also has integrated the privacy guidelines with system development life cycle (SDLC) to allow developers build privacy-sensitive-PBMS.

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter gives a brief introduction on the background of the problem, statement of the problem, research questions, and research objectives, significance of the research and finally the structure of the thesis for better view of the overall thesis.

Wireless technology is becoming more and more reliable and better able to support various types of applications and its applications are growing rapidly. From ubiquitous wireless computing arose the pervasive healthcare field. Pervasive healthcare combines computing and healthcare to develop applications that can assist patients in their daily life. Pervasive healthcare include home healthcare monitoring systems, intelligent emergency management systems, online healthcare data access, and mobile telemedicine.

Even though all these technologies sound promising and are likely to be beneficial to patients, they pose a new risk of privacy leaks. When a hospital adopts a new medical technology such as an integrated Hospital Information System (HIS), which makes patient health records available anywhere and anytime, it opens the door to a number of privacy risks to its patients. Patient health records may include both data and multimedia, such as video. By making health data easily available and accessible to healthcare providers, the hospital creates opportunities for data theft. In addition, medical sales personnel might attempt to buy patient data from irresponsible healthcare providers, in order to know what types of products they could sell to patients, hence disrupting patient privacy. Another privacy risk is recorded video. Patients with mental health issues are often monitored by staff through behavioural monitoring system so that they can monitor if the patient needs help, such as medication or calming. Behavioural monitoring system “collects images, which are transferred to a monitor- recording device of some sort, where they are available to be watched, reviewed and/or stored” (Gill and Spriggs, 2005). This recorded video creates another privacy risk as patients can easily be identified through the video. The risk is heightened if the patient is a celebrity or well-known figure, since the media may seek to create more profit by selling details of their story. Another risk is that if the video is later accessible to potential employers, patients may lose job opportunities even though they are fully recovered (Laudon and Laudon, 2013).

Privacy law generally defines an individual’s privacy as personal information that represents an individual as a whole, which consequently uniquely describes that individual. To protect their privacy, patients have the right to control what data should be collected, and by/to whom it can be used or disclosed (El Emam and Kosseim, 2009). Without consent from the individual, his or her information should remain private; if any unauthorised person accesses or uses it, it is illegal.

1.2 Background of the Problem

Monitoring system was chosen for this study because they deal more with data transactions, such as audio, video or clinical data (e.g., blood pressure, heartbeat, and electrocardiograph). A monitoring system is a system that can observe or record a patient on a daily basis without intruding on the patient’s routine. It may involve multiple parameters simultaneously; for example, it could include reading the patient’s ECG every few minutes or taking their blood pressure twice a day, and sending this data to their healthcare provider, or transmitting live video and audio of a dementia patient, thus allowing family or healthcare professionals to watch their behaviour and assess their current condition. Most of the components of such a system are wireless, therefore vulnerable to electronic eavesdropping and data theft, which raises privacy issues.

Expanded research and development projects in pervasive healthcare give rise to many privacy issues and challenges; for that reason, it is important to understand the current issues and challenges in this field. Patients have the right to choose whether or not, and to whom, to disclose their information and individuals are becoming increasingly aware of privacy issues. Stronger privacy measures in such a system would result in better privacy protection for patients.

In this study, participants need to visualise having a Psychiatric Behaviour Monitoring System (PBMS) in the ward. As there is no behaviour monitoring system applied to the psychiatric ward, the participants were given scenarios on PBMS and they need to visualise as there is a monitoring system in the ward in order to answer the questions during the interview. Therefore, this study assesses the perceived privacy among psychiatric patients instead of actual privacy experience.

1.3 Statement of the Problem

Privacy issues in healthcare behavioural monitoring systems have not been identified and investigated adequately in the literature. Different patients have different perceptions on what the privacy issues are. Thus, such behaviour monitoring systems which have been developed for hospitals without identification of the privacy issues may in turn compromise patient’s privacy and also healthcare processes.

Previous work has been done to address privacy issues which generally looked at ubiquitous computing applications only such as Friend finder applications and mobile tour guides (Benisch et al., 2009; Cornwell et al., 2007; Hong and Landay, 2004). Few have addressed pervasive healthcare privacy issues. Ahamed et al. (2007)

discussed possible privacy issues in pervasive healthcare monitoring systems focusing on data leakage. They addressed issues about leakage of patients' private information by proposing a healthcare framework for intelligent medical data acquisition. However, they did not mention how patients could manage their privacy settings on their own. Hong and Landay (2004) developed architecture for privacy sensitive ubiquitous computing applications in general which could be used for applications.

1.4 Research Questions

The key problem is how to protect patient privacy in a healthcare environment in such a way that it does not interrupt the healthcare process. This study addresses four main research questions:

1) What are patients' privacy perceptions towards PBMS in the psychiatric ward?
2) What is the most suitable privacy framework for psychiatric behavioural monitoring system to address psychiatric patients' privacy concerns?
3) What are the guidelines that can assist system developers to develop behaviour monitoring system that is privacy-sensitive?
4) How can we map privacy guidelines onto system development life cycle (SDLC) to allow developers to build privacy-sensitive application?

1.5 Research Objectives

Currently, no research efforts have looked at privacy management embedded in a psychiatric monitoring system in Malaysia. Thus, the research objectives are the following:

1) To identify patients' perception on privacy issues towards psychiatric behavioural monitoring system (PBMS).

2) To apply privacy framework used by information systems developers in developing in PBMS.
3) To develop privacy guidelines based on the privacy framework to be used by information systems developers in developing for a patient behavioural monitoring system.
4) To integrate PBMS privacy guidelines into SDLC life cycle to be used by system developers for PBMS.

This work has implications for future monitoring system development since it will shed light on methods of embedding privacy aspects into such a system, thus protecting patient privacy while not interrupting the healthcare process.

1.6 Significance of the Research

The significance of this research is an increased understanding of the patient privacy for any behavioural monitoring system. Patient privacy is protected thus making a patient feel comfortable when the monitoring system is in use. It is important to make patients feel comfortable by knowing that their privacy is protected (Laudon and Laudon, 2013).

There are two types of contributions in this study which are the theoretical contributions and practical contributions.

The theoretical contributions are:

Carew and Stapleton (2005) privacy framework provides a comprehensive privacy factors for any information systems. In this study, we are able to apply privacy framework to explain why and how each of the factors influences the privacy perceptions of psychiatric patients towards PBMS. In addition, this privacy framework is able to fully describe the each of the complex privacy dimensions that influence the privacy concerns of psychiatric patients.

Bridge the gaps in the privacy field by applying framework in a unique and different context such as the medical institution and psychiatric patients.

The guidelines produced at the end of the study can be used by system developers to build any behaviour monitoring system with appropriate privacy principles.

The integration of PBMS privacy guidelines into SDLC waterfall lifecycle model is to help system developers in implementing PBMS privacy guidelines into the system.

The practical contributions from this study are:

The elicitation technique which is the interview method for psychiatric patients (the detailed process on the creating interview protocol, the do’s and don’ts during the interview, the inclusion and exclusion criteria, how to interview psychiatric patients, the data collection process, data analysis process and practical guidelines to handle psychiatric patients) can help future researchers in this field to understand the methodology that works with sensitive issue.

Institutions could identify potential privacy risks among psychiatric patients to help them protect the confidentiality, identity, and personal information from being known or disclosed.

1.7 Structure of the Thesis

This dissertation has five chapters.

Chapter 1 is the introduction; it summarises the principle privacy issues along with motivations for the development of a privacy-sensitive framework for behaviour monitoring system for psychiatric patients.

Chapter 2 discusses existing work on privacy needs from three different three related fields: computing, law and privacy. In chapter two, it discusses current privacy issues in healthcare. Besides that there is a discussion on comparison of four types existing theoretical framework on privacy.

Chapter 3 discusses on the exploratory qualitative approach. The elements of inquiry in this research are constructivism, case study and interview then conceptualized into qualitative research which finally translated into practice. It explains in details the design processes of the research which involve questions, theoretical lens, data collection and finally the data analysis.

Chapter 4 details the data collection finding and analysis that were done throughout the research. All of the findings is to be discussed in this chapter and relates with the privacy framework. Later, the discussion is about the guidelines analysis to develop the privacy guidelines for psychiatric patient behaviour monitoring system.

Finally **Chapter 5** discusses the design of the privacy sensitive framework and the privacy guidelines based on the analysis presented in chapter 4. Besides that a discussion on integrating the privacy guidelines into SDLC waterfall model, the strength and limitations on this study.

The appendices provide supporting materials such as patient interview scripts and end user evaluation forms.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter will review on the literature related to this study. First it will discuss about the pervasive healthcare involving monitoring system followed by the types of monitoring systems available nowadays and the risk of applying monitoring systems. Then privacy issues related to monitoring system followed by international and local (Malaysia) laws to protect privacy are discussed. Finally this chapter reviews four major works on patient's privacy related to this study. This chapter begins with pervasive healthcare overview, followed by privacy definition, current privacy issues in pervasive healthcare, existing theoretical framework on privacy, overview of the privacy framework, and finally explanation on relationship between the privacy framework and this study.

2.2 Pervasive Healthcare

Varshney (2007) defines pervasive healthcare as "*healthcare to anyone, anytime and anywhere by removing location, time and other restraints while increasing both the coverage and the quality of healthcare.*" This means, for instance, that a patient with heart problems can stay in the comfort of his or her own home while being monitored by healthcare providers, instead of having to stay at the hospital.

Other than Varshney (2007), there is no broad definition for pervasive healthcare in the literature (Orwat et al., 2008). Most of the literatures define pervasive healthcare from their own particular perspective, based on the system that they have developed. For example, Andre and Teller (2005) stated that pervasive healthcare should be inexpensive, accurate and easy to use while still being able to perform the desired task. This means that it must be able to collect current information from a patient, and the system must be practical for the patient to use. If a system can deliver perfect measurements and data, but is too huge or unpleasant for the patient to use, the system is considered a failure. Therefore, the researchers created a SenseWear system, Andre and Teller (2005) that is both wearable and provides useful information to healthcare providers.

In sum, pervasive healthcare can be defined as an application that applies wireless networking technology to objects that can be used for medical treatment purposes (Kim et al., 2007; Kim et al., 2006; Korhonen and Bardram, 2004; Sneha and Varshney, 2006). The application must be embedded into wearable devices because pervasive healthcare needs to deal with real data in real time. Managing data in a pervasive healthcare context is more crucial than other forms of ubiquitous computing as it involves human life.

Pervasive healthcare is in more and more demand since it can help caregivers manage their patients even at a distance and can reduce the need for direct interference. As a result, pervasive healthcare can reduce labour costs hence reducing the cost of medical care. Pervasive healthcare can be applied to many types of services. We did a literature review to find out the types of services that have been offered from the beginning of pervasive healthcare to date Ramli et al. (2010), given that different researchers define different types of services based on their understandings, perceptions and research goals. The details on types of pervasive healthcare can be found in Appendix A.

To summarise, different studies have presented different views of pervasive healthcare services, but one thing they all have in common is the interrelationship between patient, medical services and patient data management in delivering pervasive healthcare. However, privacy must be aggressively supported in every pervasive healthcare technology in order to attain widespread acceptance. If pervasive healthcare development puts human concerns with privacy aside, eventually there is a possibility that people will absolutely reject the applications.

This section has discussed pervasive healthcare in general and the type of services that are available or currently being studied. We now have a better understanding of what pervasive healthcare is, its applications in general, and how it might be applied to patients. In addition, the reader should have at least a basic grasp of how pervasive healthcare could interfere with a patient's privacy if it is not carefully applied and managed. This provides a solid foundation for the next section, which discusses in details the question "What is a monitoring system?" specifically in the context of this study.

2.2.1 Monitoring System

A monitoring system is one form of pervasive healthcare services. A monitoring system is used to monitor patients during their daily activities without interfering with their life. Patients with different types of health problems will require different types of monitoring systems depending on their needs with regard to assistance, capability and medication. A pervasive healthcare monitoring system can be used in any location, based on the patient's needs – indoor or outdoor, static or mobile, or at the patient's home, hospital, office or nursing home. Children and adolescents usually live at home or at child nursery. Children's movements are generally faster than those of older patients; the monitoring system should be able to follow their movements. Another consideration is that children are smaller than adults, thus the monitoring device should be small enough not to burden them yet not reachable by the child as they might eat, or remove or damage the device. For adults, they may fear rejection or ridicule; they may feel like the wearable device is destroying their appearance. Therefore, the device should be small and able to be worn under their garment so as not to be visible to others. For geriatric patients, the monitoring system device should be lightweight as they are sometimes not strong enough to hold a device. In addition, some elderly patients are technology resistant because it looks or feels intrusive to them. Thus there is a need to create a device that is not too intrusive from their perspective. Table 2.1 shows the diversity of patients by age and monitoring needs (Varshney, 2009a).

Table 2.1: Patient Monitoring Needs, by Age and Health Problem (Varshney, 2009a)

Age	**Possible Monitoring Location**	**Health Problem**	**What Needs to be Monitored**
Child and adolescent	Home, hospital, child nursery or while moving about	Asthma	Oxygen saturation
		Cancer	Vital signs (BP, heart rate, temperature, glucose level, oxygen saturation, ECG)
		Mental or Neural Disorder	Behaviour
		Asthma	Oxygen saturation
Adult	Home, office, hospital or while moving about	Cancer Hypertension Diabetes Stroke Heart Disease	Vital signs (BP, heart rate, temperature, glucose level, ECG)
		Mental Disorders	Behaviour
Geriatric	Home, hospital, assisted living or nursing home, or while moving about	Cancer Hypertension Diabetes Stroke Heart disease Asthma	Vital signs (BP, heart rate, temperature, glucose level, oxygen saturation, ECG)
		Mental disorders	Behaviour
		Falls	Fall detection
		Forgetful	Reminders

Monitoring systems are chosen for this investigation because they deal more with data transactions, such as audio, video, or clinical data (e.g., blood pressure, heartbeat, electrocardiogram [ECG]). A monitoring system is a system that can monitor a patient constantly but without intruding on their daily routine. The system may involve multiple parameters simultaneously; for example, it could read the patient's ECG every few minutes, or take their blood pressure and send it to their healthcare providers. A monitoring system could also, for example, transmit live video and audio of a dementia patient to family or staff who wish to be aware of his or her current condition.

Based on Table 2.2, we can see that different health problems will require different measurements be taken, and therefore the monitoring system needs different types of wireless technology devices. For in home location, monitoring can be done indoors or outdoors. Indoor behaviour monitoring for mental disorders and other health problem can be done via wearable devices that plug into an outlet, while outdoor monitoring can be done via wearable devices that run on batteries. Typically, hospital monitoring is more intense than home monitoring because hospitals have in-house expertise in case of emergency. However, in-home monitoring systems are simpler, seeing that if the device detects any unusual data reading, it only sends notification to the healthcare provider for help.

There are several possible types of pervasive healthcare monitoring systems. The brief explanations of the primary types (Varshney, 2009a) that can be referred in Appendix B.

Table 2.2: Vital Sign Definitions and Monitoring Devices

Vital Sign	Definition	Monitoring Device
Heart Activity	An electrical recording of the heart used in the investigation of heart disease (Jenkins and Gerred, 2009)	ECG/EKG telemedicine device (Lucani et al., 2006)
Blood Pressure	Pressure of the blood on the arteries and other blood vessels ("Blood Pressure," 2008)	Blood pressure cuff Photoplethysmography (PPG)
Oxygen Saturation	Percentage of the oxygen in the blood	SNORESAT to monitor breathing abnormalities during sleeping (Mikati, 2010)

2.2.2 Mental Illness

Though there are many illnesses that might benefit from pervasive healthcare monitoring, as outlined in the preceding section, this study focuses on mental illness because mental illness issues can create negative attitudes towards patients Read (2006) thus leading to prejudice among family, friends and colleagues (Byrne, 2001). This prejudice may affect a person's career if an employer becomes aware of their illness, and may negatively affect their relationship with family and friends. There are numerous definitions of mental health; for this study we have chosen three definitions that best support our thesis. The first definition is *"[a person's] cognitive, and/or emotional wellbeing. It is all about how we think, feel and behave*" (Nordqvist, 2015). The second, from MediLexicon, defines mental health as

"*Emotional, behavioural, and social maturity or normality; the absence of a mental or behavioural disorder; a state of psychological well-being in which one has achieved a satisfactory integration of one's instinctual drives acceptable to both oneself and one's social milieu; an appropriate balance of love, work, and leisure pursuits*"("Mental Health," 2009).

The third is from the World Health Organisation, which defines mental health as "*Mental Health is the foundation for the well-being and effective functioning of individuals. It is more than the absence of a mental disorder. Mental health is the ability to think and learn, and the ability to understand and live with one's emotions and the reactions of others. It is a state of balance within a person and between a person and the environment. Physical, psychological, social, cultural, spiritual and other interrelated factors participate in producing this balance*" ("Mental Health," 2016).

In sum, mental health is a state or condition wherein a human being can act and think rationally in living their daily life. When a human being acts differently from what is considered normal human behaviour, it can be called a mental health problem. Mental illness also can be referred to as a mental health problem or mental disorder. Mental illness "*[can] refer to a wide range of mental disorders that can be diagnosed by a healthcare professional*" (Nordqvist, 2009). In this thesis, we use the phrase "mental illness" to represent a mental health problem or mental disorder. Sometimes patients with a mental illness can harm themselves (suicide) or others (homicide). Hence, mental health monitoring of such patients is a crucial tool for avoiding accidents or mishaps.

Some mental illness symptoms require patients to see a psychiatrist. Varshney (2009a) lists several types of symptoms, which include suicidal ideation with or without intent or plan, homicidal ideation with or without intent or plan, unstable or out of control behaviour due to mania, agitation, acute psychosis, dementia with severe behavioural problems such as resisting care, wandering away or being at risk for harming self or others, dementia with psychotic symptoms, delirium when medically stable, serious withdrawal for drugs and rapid, sudden and severe deterioration of functioning. Mental illness patients with these kinds of syndromes need monitoring to avoid harm to themselves or others. Only when the symptoms are known can the appropriate monitoring system be applied to monitor a mental illness patient. The patient's family and relatives should also know the symptoms in order to work together with healthcare providers.

Mental illness monitoring systems could address problems such as Alzheimer's Dementia, Post-Traumatic Stress Disorder, Obsessive-Compulsive Disorder (OCD), Panic Disorder, Eating Disorders and Autistic behaviour issues (Varshney, 2009b).

Different types of mental illness require different types of monitoring. Table 2.3 summarises common categories of mental illness and their symptoms together with the preferred type of monitoring (Varshney, 2009b).

Occasionally, individuals with severe mental illness will be admitted to hospital for intensive monitoring; individuals with less severe mental illness problems can stay at home under the supervision of a behaviour monitoring system. In Malaysia, only public hospitals are allowed to have wards for psychiatric patients, and some of them provide behaviour monitoring system. Mental illness behaviour monitoring can be applied in hospitals, or at home in the patient's own house or in an assisted living facility. However, since there is stigma attached to mental illness, privacy is a serious concern.

Table 2.3: Mental Illness, Symptoms, Type of Monitoring and Target Population (Varshney, 2009b)

Category of Mental Illnesses	**Example**	**Symptoms**	**Type of Monitoring**	**Target Population**
Mood Disorders	Major Depressive Disorder Bipolar Mood Disorder	Lack of energy, sleep and interests Suicidal ideations Manic phase followed by depressive phase	Video or picture of patient's behaviour	Young adults, adults and geriatric population Young adults, adults and geriatric population
Cognitive Disorders	Alzheimer's Dementia	Severe forgetfulness Screaming, physical abuse of others	Video or picture of patient's behaviour	Geriatric population

Table 2.3: Continued

Category of Mental Illnesses	**Example**	**Symptoms**	**Type of Monitoring**	**Target Population**
Personality Disorders	Obsessive-Compulsive Disorder (OCD)	Distress in job and family situations	Video or picture of patient's behaviour	Young adults, adults and geriatric population
	Schizophrenia	Hallucinations Delusions	Wearable type of device	Young adults, adults and geriatric population
Anxiety Disorders	Post-Traumatic Stress Disorder (PTSD) Panic Disorder	Excessive worrying Excessive alertness Lack of sleep Panic attacks	Video or picture of patient's behaviour Sleep monitoring ECG	Young adults, adults and geriatric population All age groups
Developmental Disorders	Attention Deficit and Hyperactivity Disorder Autism	Inability to focus Abnormal social interactions	Video or picture of patient's behaviour Wireless sensor to report abusive or aggressive actions	Children
Eating Disorders	Anorexia Nervosa	Loss of weight Abnormal heart rhythm	Wireless sensors placed around neck to monitor amount of swallowing and vomiting ECG	Primarily young and adult women

2.2.2.1 Mental Illness Behaviour Monitoring System

Although there are many types of behaviour monitoring systems (Refer: Appendix B), the focus here is on those that monitor a patient's behaviour by recording video or taking pictures. In this section we will discuss in depth how a mental illness behaviour monitoring system could be used.

This study is about collecting patient's perceived privacy, rather than actual experience. This does not affect the factors because all participants managed to clearly visualise the situation. This is because CCTV is currently being used in most of public places in Malaysia, therefore participants have experienced being monitored but in different concept. There are three other studies in the well-known journals that performed qualitative study for perceived data rather than actual data (Haarsma et al., 2014; Haein et al., 2013; Radcliffe and Lester, 2003). Beside these journals, Adams et al. (2001) and Beckwith (2003) also studied perceived privacy. The journals are the proved that perceived privacy is acceptable among scholars.

Figure 2.1 depicts a healthcare monitoring system as suggested in this research. There are three main stakeholders with privacy concerns in a healthcare monitoring system: the patient, the family and the healthcare provider(s).

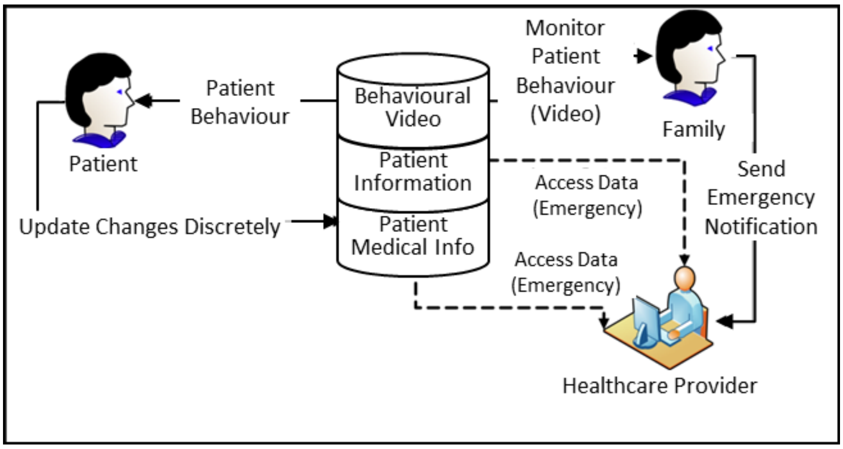

Figure 2.1: Healthcare Monitoring Overview

Thus far we have discussed pervasive healthcare and the various types of applications in general, and given examples of various possible monitoring systems in detail. In the next section, we will discuss privacy and privacy issues, and the relationship between privacy and computer science.

2.3 Privacy

Privacy is very important to human beings. A person wants to have their privacy to avoid embarrassment and shame Baker and Shapiro (2003), which is a particular dilemma for mental health patients, and it is a necessity for managing personal activities (Pedersen, 1997). Privacy does not mean blocking everyone from knowing anything about a person. It means the ability to control what other people know about you and when (Pedersen, 1997). Privacy has many definitions in the literature depending on the author's perspective, background, and research interests. As a result, there is no consensus on the term and no single definition. However, two studies have presented a collection of the different perspectives and views on privacy, including a list of privacy definitions from different scholars over a twenty year period, 1967 to 1984 (Margulis, 2003; Newell, 1995). In this section, we list several definitions of privacy from different perspectives, to give an understanding of what privacy is in relation to our study.

From the psychological viewpoint Pedersen (1997) defines privacy as "*behaviours [that] are engaged in to achieve a desired level of access to one's self or group.*" He identified six types of privacy (solitude, isolation, anonymity, reserve, intimacy with friends, and intimacy with family) and five privacy functions (anonymity, confiding, rejuvenation, contemplation and creativity). He created a privacy model that combines these two concepts of privacy type and privacy function to measure privacy level.

From a sociological perspective and a focus on consumer data privacy, "*the father of privacy*" Westin (1967) defines privacy as "*the claim of individuals, groups or institution to determine for themselves when, how and to what extent information about them is communicated to others.*" Altman (1977) defines privacy as "*selective* *control of access to the self or to one's group.*" He explains how a person's connections with others might affect their privacy preferences.

From the legal perspective, privacy law generally defines privacy in terms of personal information about an individual that can represent that individual as a whole, which consequently describes an individual. To protect their privacy, patients have the right to decide what data should be collected, and when and by/to whom can be used or disclosed (Kosseim and Emam, 2009). In addition, international human rights law recognises that privacy is "*clearly and unambiguously established as a fundamental right to be protected*" (Michael, 1994). Therefore, without consent from the individual, his or her information should remain private; if any unauthorised person takes it, it is an illegal action. People may have different privacy preferences depending on what they want at a particular moment, and what they want may change from time to time based on their physical environment and personal relationships (Werner et al., 1992). Related to this study, for example, a patient may define their privacy more openly at home while at the hospital they will define their privacy more strictly as that situation involves more strangers. In addition, patients may make their private data accessible or not accessible to others at different times (Altman and Chemers, 1986).

In this study, privacy is defined based on Altman's authoritative work on privacy. Altman's definition applies to this study in that patients might alter their privacy preferences depending on their illness and who they would like to share their private information with. Patients might want to define "openness" and "closeness" differently with different individuals.

2.3.1 Proposed and Existing Data Protection Laws on Privacy

This section gives an overview of existing privacy protection laws around the world, and then discusses privacy laws in Malaysia in depth. Figure 2.2 shows data protection laws around the world, indicating by colour whether a country has comprehensive privacy data protection laws (blue), pending efforts to enact such laws (red) or no laws at all (white). As can be seen, only a few countries have enacted comprehensive data protection (e.g., Japan, Korea, New Zealand, the Philippines, Israel, Canada, Russia, EU Countries and Australia). This map is based on data from 2007. As of by year 2011 more countries have enacted privacy protection laws, including Malaysia. The United States has legislation specific to health information, HIPAA, which will be discussed further in the next section. Most Middle Eastern and Asian countries have no privacy protection laws at all (e.g., Indonesia, Brunei, Vietnam, Laos and China). It can be inferred from this that citizens in developed countries have more privacy awareness than those in developing countries, perhaps because more data technologies are in use there, thus raising more privacy issues and increasing awareness among the citizens.

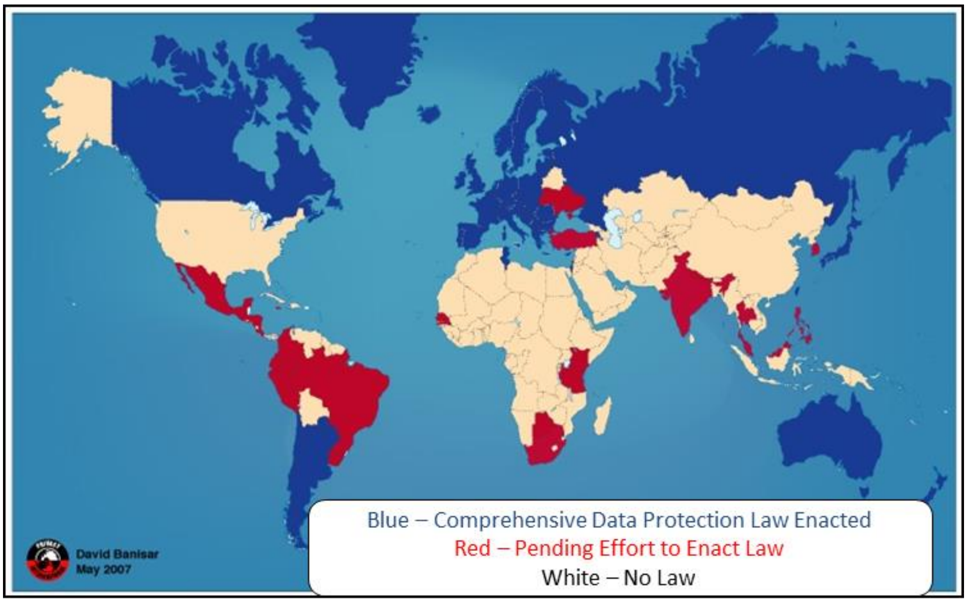
Blue – Comprehensive Data Protection Law Enacted
Red – Pending Effort to Enact Law
White – No Law
David Banisar
May 2007

Figure 2.2: Data Protection Laws around the World (Banisar, 2007)

2.3.2 Health Insurance Portability and Accountability Act (HIPAA)

HIPAA was the first comprehensive protection for the privacy of personal health information in the U.S. It has two sections, Title I: Healthcare Access, Portability and Renewability and Title II: Preventing Healthcare Fraud and Abuse; Administrative Simplification; Medical Liability Reform. This study will discuss more about Title I since it relates more to privacy issues.

Table 2.4 summarises the privacy components of HIPAA (*Summary of the HIPAA privacy rule*, 2003) that relate to this study. In HIPAA, individual health information is referred to as “protected health information” (PHI) and organisations subject to the privacy rule are referred to as “covered entities.” The full text of HIPAA is available at http://www.hhs.gov.ocr/hipaa.

Table 2.4: Summary of HIPAA Components Relating to Privacy (*Summary of the HIPAA Privacy Rule*, 2003)

Section	**Contents**
Goals (p.1)	To address the use and disclosure of protected health information. Lists individual's rights to understand and control how their health information is used. To assure that health information is properly protected without interrupting the healthcare process and while still protecting public health.
Statutory and Regulatory Background (p.1)	Standards for the privacy, security, and electronic exchange of health information.
Covered Entities (p.2)	All those who transmit health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA, including: • Health plans • Health clearinghouses (billing services, reprising companies, community health management information system) • Any healthcare provider
Protected Health Information (PHI) (p.3)	All individually identifiable health information (e.g., name, address, social security number, etc.) in any form or media, whether electronic, paper or oral, including demographic data, related to: • The individual's past, present or future physical or mental health or condition • The provision of healthcare to the individual • The past, present or future payment for the provision of healthcare to the individual
General Principles for Use and Disclosure (p.4)	Defines and limits the circumstances in which an individual's PHI may be used or disclosed by covered entities. A covered entity can only disclose PHI to: • Individuals authorised by the owner of the data HHS when it is undertaking a compliance investigation or review or enforcement action.

Table 2.4: Continued

Section	**Contents**
Permitted Uses and Disclosures (p.5)	A covered entity is permitted to disclose PHI without an individual's authorisation only: • To the individual • For treatment, payment and healthcare operations • Incident to an otherwise permitted use and disclosure • For public interest and benefit activities In the form of a limited data set for purposes of research, public health or healthcare operations.
Authorised Uses and Disclosures (p.9)	For any disclosure of PHI, the covered entity must have authorisation written in specific terms. The authorisation must include what information to be used, who is disclosing the information, which is the recipient, and the duration for the data disclosure.
Limiting Uses and Disclosures to the Minimum Necessary (p.10)	Only the minimum amount of PHI necessary for the intended purposes, disclosure or request should be disclosed. The covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. Minimum disclosure is not applicable in the following cases: • Disclosure to or a request by a healthcare provider for treatment of the individual • Disclosure to an individual who is the subject of the information, or the individual's personal representative • Disclosure to HHS for complaint investigation, compliance review or enforcement • Use or disclosure as required by law • Use or disclosure as required by HIPAA
Personal Representatives and Minors (p.16)	A personal representative is a person legally authorised to make healthcare decisions on an individual's behalf or to act for a deceased individual or his or her estate.

HIPAA applies only to medical records in the United States. However, many issues have been raised by many parties. As written by Annas (2003a), HIPAA regulations are very complex to understand and know how to apply, and makes managing health records difficult. From his point of view, HIPAA focuses more on how covered entities can access medical records rather than on protecting patient privacy. Annas (2003b) concluded that "*the implementation of the new HIPAA privacy regulations is likely to be costly, inconsistent and frustrating to both physicians and patients.*"

Creating the privacy architecture outlined in this study will help to protect patient privacy more easily and reduce costs. System developers can apply this privacy architecture to any behaviour monitoring system in the future.

2.3.3 Healthcare Data Protection in Malaysia

The preceding section discussed the protections available in other countries, such as the HIPAA regulation which is implemented in the U.S. but not in Malaysia. This section will discuss healthcare data protection in Malaysia, and describe the proposed laws and organisations that protect a patient's privacy in Malaysia.

Privacy preferences are likely to be different for each individual depending on family background, race, religion, culture, home country and what information is to be protected, such as personal information, medical information or shopping history (Rattanapongpaisan, 2001). In Malaysia, a majority of people are concerned about their privacy when it relates to money, and when it involves online banking and online shopping. Most Malaysians are still skeptical about online shopping because they are afraid their credit card information will be stolen. Besides online banking, now privacy awareness regarding their health information also are raising, thus a need for a better personal medical information management to protect their privacy is needed (Ismali, 2013). In addition, Malaysia lacks a comprehensive legislative framework for protecting this data (Sarabdeen and Ishak, 2008). Therefore, the greatest challenge in Malaysia is to provide protection for the privacy and confidentiality of medical data that is being stored electronically while delivering a good healthcare service.