

2016


# An Empirical Investigation of Privacy and Security Concerns on Doctors' and Nurses' Behavioral Intentions to Use RFID in Hospitals

Thomas George Winston

Nova Southeastern University, [thomwins@nova.edu](mailto:thomwins@nova.edu)

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: [http://nsuworks.nova.edu/gscis\\_etd](http://nsuworks.nova.edu/gscis_etd)

 Part of the [Computer Sciences Commons](#), [Equipment and Supplies Commons](#), and the [Health Information Technology Commons](#)

## Share Feedback About This Item

---

### NSUWorks Citation

Thomas George Winston. 2016. *An Empirical Investigation of Privacy and Security Concerns on Doctors' and Nurses' Behavioral Intentions to Use RFID in Hospitals*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (371)

[http://nsuworks.nova.edu/gscis\\_etd/371](http://nsuworks.nova.edu/gscis_etd/371).

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact [nsuworks@nova.edu](mailto:nsuworks@nova.edu).

An Empirical Investigation of Privacy and Security Concerns on Doctors'  
and Nurses' Behavioral Intentions to Use RFID in Hospitals

By

Thomas G. Winston

A dissertation submitted in partial fulfillment of the requirements  
For the degree of Doctor of Philosophy  
In  
Information Systems

Graduate School of Computer and Information Sciences  
Nova Southeastern University

2015

We hereby certify that this dissertation, submitted by Thomas Winston, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

---

Souren Paul, Ph.D.  
Chairperson of Dissertation Committee

---

Date

---

Lakshmi Iyer, Ph.D.  
Dissertation Committee Member

---

Date

---

Ling Wang, Ph.D.  
Dissertation Committee Member

---

Date

Approved:

---

Amon B. Seagull, Ph.D.  
Interim Dean, College of Engineering and Computing

---

Date

College of Engineering and  
Computing Nova Southeastern  
University

2015

An Abstract of a Dissertation Submitted to Nova Southeastern University  
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy  
An Empirical Investigation of Privacy and Security Concerns on Doctors'  
and Nurses' Behavioral Intentions to Use RFID in Hospitals

by

Thomas G. Winston

December 2015

Radio frequency identification (RFID) technology is a useful technology that has myriad applications in technology, retail, manufacturing, and healthcare settings. Not dependent upon line-of-sight, RFID can scan devices in their proximity and report the information to connected (wired or other wireless) information systems. Once touted as the panacea for home healthcare, RFID devices can add benefit to patients in remote settings. RFID devices have been used to optimize systems in areas such as manufacturing and healthcare to expose inefficiencies in a system or process. Unlike manufacturing, however, RFID in healthcare settings presents security and privacy concerns to the people being tracked by the devices – particularly healthcare workers including nurses and doctors. This research presented a theoretical model that assessed the effect of five independent variables, namely, cognitive factors, of privacy concerns regarding surveillance and RFID devices and trust in the electronic medium, subjective norm, existence of security policy, and persistence of data on a dependent variable - intention to use RFID. The theoretical model presented in this research is based on the technology acceptance model and the extended theory of planned behavior. The research showed significant relationships between the cognitive factors of privacy concerns regarding surveillance and RFID devices, and trust and the electronic medium and perception of external control on intention to use. The theoretical model used in this research can be refined to better understand intention to use RFID in hospital environments.

## **Acknowledgements**

I dedicate this work to my lovely wife and daughter – Moira and Elana. I would like to thank both of them profusely for being there for me throughout this process.

Finally, I would like to acknowledge the hard work and patience of my committee members (Dr. Ling Wang, and Dr. Lakshmi Iyer) and especially my chair (Dr. Souren Paul) for guiding me through this process, and I would like to thank Nova Southeastern University for giving me the opportunity to realize a life-long dream.

## Table of Contents

**Abstract** iii

**List of Tables** vii

**List of Figures** viii

### **Chapters**

#### **1. Introduction 1**

Background 1  
Problem Statement 2  
Dissertation Goal 3  
Research Questions 4  
Relevance and Significance 5  
Barriers and Issues 6  
Assumptions, Limitations and Delimitations 7  
Definition of Terms 7  
Summary 9

#### **2. Review of the Literature 11**

Introduction 11  
Technology Acceptance Overview 12  
Technology Acceptance Research Models 13  
Security as Privacy 22  
Proposed Research Model 23  
Perceived Usefulness and its Determinants 34  
Intention to Use and its Determinants 38  
Summary of What We Know and do not Know about the Topic 46

#### **3. Methodology 47**

Research Setting 47  
Sample Characteristics 48  
Sample Size 50  
Instrumentation 52  
Instrument Validation 53  
Operationalization of the Variables 54  
Validity and Reliability Assessment 57  
Data Collection 60  
Data Analysis 60  
Format for Presentation of Results 63  
Resources Used 63  
Summary 64

#### **4. Results 65**

Data Collection and Analysis 65  
Measurement Model Analyses 68  
Common Method / Common Variance Test 69  
Latent Variable Definitions 71  
Evaluation of Outer Model Loadings 72  
Internal Consistency Reliability 74  
Structural Model Analyses 76

**5. Conclusions, Implications, Recommendations and Summary 80**

Conclusions 80  
Implications 87  
Recommendations 88  
Summary 88

**Appendices**

A. Survey Invitation 94  
B. Survey 96

**References 101**

## **List of Tables**

### **Tables**

1. A Summary of Constructs, Definitions and References 25
2. Summary of Results 78



## **List of Figures**

### **Figures**

1. Technology Acceptance Model 15
2. Theory of Planned Behavior 16
3. Conceptual Model Developed by Anderson and Agarwal 20
4. Conceptual Model Proposed in this Research 24
5. G-Power Results 51
6. Descriptive Statistics of the Demographic Data 67
7. Descriptive Statistics of the Constructs 69
8. Common Variance Test 70
9. Definitions of Latent Variables 71
10. Correlations among the Constructs 73
11. Outer Model Path Loadings 73
12. Convergent and Discriminant Validity of Latent Variables 74
13. Cross-Loadings 75
14. Heterotrait Monotrait Ratio Criterion 75
15. Significance of the Path Coefficients Indicated by T-Test Statistics 76
16. Summary of Important Measures on Structural Model 77
17. Regression results using list-wise replacement for missing values 80
18. Further Testing with Dependent and Independent Variables 81
19. Inner Path Coefficients with Further Testing 82

# Chapter 1

## Introduction

### Background

Hospitals, manufacturing facilities construction, retail and even educational institutions are using Radio Frequency Identification (RFID) to track patients, parts, supplies, and items of clothing for inventory tracking and theft control (Akpinar & Kaptan, 2010); Littman, 2008; O'Connor, 2009b; Yin, Tserng, Wang & Tsai, 2009). Medical facilities use RFID technology to cut health care costs, automate and streamline patient identification processes in and outside of hospitals (Huan, Horng & Jong, 2008; Raad, 2010).

RFID usage in hospitals requires implicit acceptance of the technology, with consideration of inherent security and privacy concerns, specifically to healthcare providers using RFID devices. Fisher and Monahan (2008) discovered hospital staff members' unwillingness to use RFID technology due to the sense of "big brother" watching over their movements and activities in the work context. In this context RFID was used to track nurses movements, time spent with patients, and time spent off the floor. However, the RFID tags would also monitor time spent in the bathroom, for example. Raad (2010) determined that security concerns negatively affect willingness of patients to utilize RFID technology. Muller-Seitz, Dautzenberg, Creusen, and Stromereder (2009) stated data security concerns affect overall attitude of users toward

novel technologies such as RFID, in a German electronic retail corporation. Using TAM, Muller-Seitz, et al. (2009) an empirical study of 206 customers determined customer acceptance depends on perceived use. Muller-Seitz, et al. (2009) based their paper on the notion that commonly perceived risks of using novel technology may dissipate over time presented by Dickerson, And Gentry (1983) and Korgaonkar, and Moschis (1987). Over time the adopted technology becomes part of the workplace, and ordinary to its users.

### **Problem Statement**

In Littman (2008), Fisher and Monahan (2008) positively correlated RFID technology to both uncovering inefficiencies in a hospital system, and to ensuring the health and safety of hospital personnel and patients. Muller-Seitz, et al. (2009), using a modified TAM determined patients data security concerns regarding perceived use of information captured from RFID transponders, based on the patients' perception of privacy and security. This investigation did not focus on the patients, due to privacy concerns, but instead on the doctors and nurses, however, the methodology employed by Muller-Seitz, et al. can be used in determining security and privacy perceptions. Raad (2010) stated RFID technology could be employed for not only cutting down health care costs, but also for automating and streamlining patient identification processes in and outside hospitals. RFID technology plays an increasingly important role in hospitals, but suffers from negative perceptions of security and privacy issues associated with the technology. The widely tested technology acceptance model (TAM) shows how users accept and use a given technology in a variety of contexts (Davis, 1989). The extended theory of planned behavior (ETPB) an extension of the theory of reasoned action links attitudes to actions and has been successfully applied to technology acceptance and use questions in

healthcare settings (Baek, 2007). Privacy issues regarding RFID technologies have been extensively researched in the past 5 years (Bischoff, 2007; Consumers Against Supermarket Privacy Invasion and Numbering, Privacy Rights Clearinghouse, American Civil Liberties Union, and the Electronic Frontier Foundation, the Electronic Privacy Information Center, 2003; Junkbusterset, 2003; Ohkubo, Suzuki, & Kinoshita, 2005; Reid, 2007; Sade, 2007). In 2011 Norton investigated nurses' acceptance of RFID usage in a mandatory use environment. Since then in spite of concerns discovered by this research, more hospitals have required RFID usage among their medical staffs. This research expanded upon extant literature regarding acceptance of RFID technology as well as research describing privacy issues encountered with location based technology and focus on how security concerns and trust in the technology influence perceptions, and thus intention to use RFID technology in the workplace.

### **Dissertation Goal**

The primary goal of this study was to investigate security and privacy concerns on behavioral intentions to use RFID in hospitals among doctors and nurses. This research better framed the issues regarding security and privacy concerns in RFID usage, and those parameters in the context of RFID acceptance, furthering research conducted by Anderson, and Agarwal (2011), which considered privacy boundary calculus of the same problem. The model developed for this research was based on extant literature of TAM and extended TAM (Venkatesh & Davis, 2000; Venkatesh & Bala, 2008) as well as the ETPB (Anderson & Agarwal, 2011; Cammock et al., 2009; Hossain & Prybutok, 2008; Muller-Seitz et al., 2009; Xu & Gupta, 2009).

The researcher added the construct of “security” (Lee, 2009). The proposed model provided a theoretical framework for the constructs (variables), which according to the planned research would affect RFID acceptance in US hospitals.

The researcher proposed first a meeting with a panel of experts to better focus the important variables, then a survey tool was distributed electronically to US hospitals, and used a quantitative research design, and the researcher used statistical analysis to validate the theoretical model. The researcher conducted a survey to collect data and analyzed it using quantitative statistical methods. The goal of this dissertation was to assess how security trust, security concerns and perceived security affect behavioral intention to use RFID in US hospital systems.

### **Research Questions**

The unstructured interviews comprised a panel of experts review, done before conducting formal survey research. This served to pare down and further focus the research questions presented below (Sekaran, 2003).

The primary research questions of the study are:

RQ1: How does the existence of a data security policy affect the intention to use RFID in US hospitals? (Grabner-Krauter & Kaluscha, 2003; Hernandez-Ortega, 2011; Lee, 2009; Schneider, 2000)

RQ2: How does persistence of data or data retention affect the intention to use RFID in US hospitals? (Juels, 2006; Kamra, et al., 2006; Konomi, 2004; Palen & Dourish, 2003)

RQ3: How does subjective norm affect the intention use RFID in US hospitals?(Chen, et al., 2007; Commock et al., 2009; Davis, 1989; Mather, et al. 2000)

RQ4: How does perception of external control affect the perceived usefulness of RFID in US hospitals? (Ajzen, 1985; Carr, et al., 2010; Hosaka, 2004; Lee, et al., 2009; Venkatesh, 2000; Xu, et al., 2009)

RQ5: How do the cognitive factors of privacy concerns regarding surveillance and RFID devices as well as trust in the electronic medium affect intention to use RFID in US hospitals? (Beresford, 2003; Chanen, 2008; Hong, et al., 2004; Malhotra, et al., 2004; Myles et al., 2003; Röcker, 2010; Xu, et al., 2009)

RQ6: What is the relative strength of the contribution of the five variables (i.e., persistence of data, cognitive factors, existence of data security policy, subjective norm, and perception of external control) in predicting behavioral intention of doctors and nurses to use RFID in US hospitals?

### **Relevance and Significance**

Security and privacy issues regarding technology use pose a paradox in most modern contexts where technology is used. A large body of literature covering over 25 years outlines the paradox of privacy vs. security in many contexts, with the primary tenant being “To increase security, one must give up some privacy.” US laws have considered this carefully, and ran ashore of this paradox when the USA PATRIOT act was promulgated in the fall of 2001 (Lee 2009). According to Rahimi and Jetter (2015) while most using existing theories has passed the test of time, there is a compelling need for new and more empirical theories regarding healthcare technology acceptance.

Combining the variables of attitude, intention to use from the TAM, with the variables of subjective norm, perception of external control and normative cognitive factors from the ETPB, the model addressed the issues of security, taking into consideration affectations

of privacy on the usage of RFID, and is thus relevant. Lee (2009) discovered that security concerns play a role in RFID acceptance. Anderson, and Agarwal (2011) found that privacy and security are always a concern with RFID usage in medical contexts, however they were dependent on the emotional state of the patient. Bischoff (2007), Reid (2007) and Sade (2007) determined that RFID usage in mandatory environments could violate a nurse's privacy rights, due to the surveillance capabilities the technology enables. Monahan (2010) expanded this notion by noting the ability to connect seemingly disparate pieces of information about a person (birth date, credit card number, medical records, etc.) by modern search engines capability to search terabytes of stored information.

This investigation extended the extant and well-documented research regarding technology acceptance embodied by the TAM, and its variants, and the Extended Theory of Planned Behavior, by adding the dimensions of privacy and security to it. The notion of technology acceptance, like the models used to describe it has evolved over the years, in an attempt to better capture the behavioral elements of security and privacy.

### **Barriers and Issues**

Survey sample size, survey response rate, and potential survey bias may prohibit comprehensive testing of variables. Hospitals may be unwilling to provide data or access to data perceived to be proprietary, such as confidential security policies or data retention policies. Since the focus of this research was on the five variables affecting behavioral intention of doctors and nurses to use RFID, the contents of the data (i.e.: personal health information) were not discovered or researched.

### **Assumptions, Limitations and Delimitations**

The research assumed that doctors and registered nurses took the time to answer the survey. Sekaran (2003) stated that some participants' responses might be biased by answering questions in a negative state of mind or by answering questions they do not fully understand. Sekaran (2003) further stated that web-based surveys require user computer literacy, and that respondents must be willing to complete the surveys (p. 251). Finally, Sekaran (2003) indicated that respondents might not answer truthfully or respond in a way that they considered the researcher expects.

### **Definition of Terms**

*Behavioral intention.* A measure of the power of an individual's intention to perform a certain behavior (Fishbein & Ajzen, 1975).

*Controllability.* Controllability is the extent of an individual's control over his or her behavior (Cammock et al., 2009).

*Health Insurance Portability and Accountability Act.* HIPAA was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum-Kennedy Act after two of its leading sponsors. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers (**HIPAA**; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996).



*Information system (IS)*. “A set of interrelated elements or components that collect (input), manipulate (process), store, and disseminate (output) data and information, and provide a corrective reaction (feedback mechanism) to meet an objective” (Stair, Reynolds, & Reynolds, 2010, p. 10).

*Perceived behavior control*. Perceived behavioral control concerns the relative ease or difficulty of a behavior as perceived by an individual (Cammock et al., 2009).

*Perceived ease of use*. The degree of effort needed to use a system as perceived by an individual (Davis, 1989).

*Perceived usefulness*. The degree to which a certain system is able to increase one’s performance at work as perceived by that individual (Davis, 1989).

*Privacy*. Privacy has been defined as “the right to be let alone” (Warren & Brandeis, 1890, p. 193) and is based on federal and state statutes, tort law judicial decisions, and the U.S. Constitution (Magid, Tatikonda, & Cochran, 2009).

*Persistence of Data*. Concerns over the storage of data that could be used at later time potentially violating a person’s privacy (Konomi, 2004).

*Radio Frequency Identification (RFID)*. RFID is an unobtrusive technology that facilitates electronic transmission of potentially sensitive data without line-of-site requirements and without the sender’s active participation or knowledge (CASPIAN et al., 2003; Ohkubo et al., 2005). RFID systems feature two components, namely, an RFID tag and a reader or interrogator (Littman, 2008).

*RFID tag.* An RFID tag or transponder is a small device consisting of an antenna and integrated chip or silicon chip that holds information concerning the item to which it is attached (Littman, 2008).

*Subjective norms.* These are the perceived social pressures to perform (or not) a certain behavior (Cammock et al., 2009).

*Technology acceptance model (TAM).* TAM is a classic IS model that focuses on an individual's perceptions and how these perceptions influence the individual's intentions (Liu & Chen, 2009). According to TAM, an individual's intentions to use a technology can be explained by his or her perceptions of the technology's usefulness and attitudes toward its ease of use (Liu & Chen, 2009).

*Theory of planned behavior (TPB).* This is a theoretical model that is based on TRA, defined below, and is founded on the idea "that only specific attitudes toward the behavior in question can be expected to predict that behavior" (Ajzen, 1991, p. 180). TPB includes the constructs of perceived behavioral control, attitudes, and subjective norms in regard to the acceptance of technology (Ajzen & Fishbein, 1980).

*Theory of reasoned action (TRA).* TRA posits that the intent of an individual to engage in a behavior is the major determinant of whether the individual engages in that behavior (Cammock et al., 2009).

## **Summary**

Chapter 1 presented the research problem of privacy and security concerns effects on behavioral intention to use RFID devices. Specifically, the goal of the research was to

discover the effects of perceived security, security concerns, and security trust on the behavioral intention of doctors and nurses to use RFID in US Hospital Systems. This investigation was based on the contribution of the independent variables of subjective norm, persistence of data, existence of security policy and cognitive factors of privacy and trust. The dependent variable is the intention to use RFID.

## **Chapter 2**

### **Review of the Literature**

#### **Introduction**

According to Sarma, Weis, and Engels (2003) RFID systems serve as ubiquitous, low-cost solutions for many applications involving tracking, inventory management and healthcare. However as the information on the reader becomes more valuable it is necessary to think through security and privacy issues inherent to the devices. RFID use in healthcare has great potential to reduce healthcare costs and improve outcomes (Fichman, Kohli & Krishnan, 2011). Davis (1989) states IT only benefits its users if they are willing to accept it and adopt it. Researchers during the past 20 years have assessed technology acceptance using various iterations of TAM and the TPB (Chao & Lin, 2009; Hossain & Prybutok, 2008; Lee, 2009; Muller-Seitz et al., 2009). In 2002, Ajzen proposed the ETPB as an expansion on earlier work to the TPB further explaining the construct of perceived behavioral control. In 2011, Anderson and Agarwal proposed a theoretical model, which focused on privacy calculus as a determining factor in technology acceptance. This research considered privacy and security issues in the context of RFID acceptance, adding security dimensions to the theoretical privacy research conducted by Anderson and Agarwal (2011). Furthermore, this work extended research conducted by Norten (2011) by adding a security dimension and testing against acceptance by doctors and nurses of the technology in the workplace, versus a

requirement for nursing staff only in RFID required hospitals. The goal of the research was to validate, using a survey tool the theoretical model presented later in this chapter.

### **Technology Acceptance Overview**

The theoretical model developed in this research covers extant literature on technology acceptance, and related models. The next section considers these models, and how they shaped the theoretical model used for this investigation. The proposed model combined attitude toward usage variables of TAM3, and behavioral variables ETPB and the privacy dimension of the model proposed by Anderson & Agarwal to further explain security and privacy calculus in RFID acceptance. Literature from technology acceptance, as well as privacy and security issues in RFID implementations framed this research. TAM3 and its predecessors determined links between perceived usefulness, intention to use new technologies. Researchers have used the TAM3, and its predecessors TAM2 and TAM to determine whether or not a user population will accept a new technology. O’Leary and O’Leary (2001) stated: “the most important part of an information system is people (p.6).” People play a critical role in technology acceptance. Davis (1989) further described this idea in regarding the TAM by having stated: “if users are unwilling to accept and use IT, the benefits that the technology has to offer may be lost.” Hossain and Prybutok (2008) stated that TAM is a popular methodology for examining user acceptance of technology. Hung, Ku, and Chien (2010) used the theory of planned behavior model (TPB) to investigate the factors influencing physicians to accept the Medline System. Other researchers such as: Chao & Lin (2009); Hossain and Prybutok (2008); Lee (2009) and Muller-Seitz, Dautzenberg, Creusen & Stromereder

(2009) have used TPB and TAM to better understand attitudes toward and user acceptance of RFID technology in mixed context (mandatory or voluntary use) healthcare settings. Recent investigations of the literature surrounding information systems acceptance, and health informatics suggest that TAM is the predominant theory in use with only some adaptations emerging (Cockroft, 2015). This next section examines the literature regarding technology acceptance models used as underpinnings for the model presented in this research.

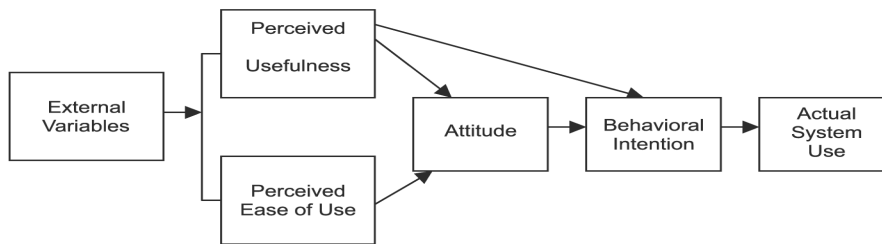
## **Technology Acceptance Research Models**

### *Technology Acceptance Model*

The research model presented in this investigation has foundations, in the Technology Acceptance Model as posited by Davis (1989), and Davis, Bagozzi, and Warshaw (1989), and measures attitude on the construct of perceived usefulness, one of the variables described in by TAM. While it has foundations in these models, this investigation focused on modifications made to the Anderson and Agarwal (2011) model for this research, presented later in this section. In order to understand how Anderson and Agarwal derived their model and how the model presented here fits into the broader scheme of technology acceptance models, the literature contextualizing each model was included in the next sections. This next section started the discussion by explaining how TAM, TAM 2 and TAM 3 as well as ETPB are supported by the literature as fundamental ways to explain technology acceptance. Many studies used the TAM to determine outcomes in information technology adoption (Adams, Nelson, & Todd, 1992; Bruner & Kumar, 2005; Davis, 1989; Davis et al., 1989; Heijden, Verhagen & Creemers

2003; Igbaria & Tan, 1997; Liao, Chen & Yen, 2007; Lin & Lu, 2000; Luarn & Lin, 2005; Mathieson, 1991; Moon & Kim, 2001; Taylor & Todd, 1995; Wu & Wang, 2005; Yang, 2005). In a like manner, TAM has been used in many health information technology acceptance assessments. Holden, and Karsh (2009) noted that not enough research has been conducted on how clinician end users react to an already implemented information technology. According to Liu, and Chen (2009), it is the perceptions of usefulness and the ease of use of a given technology that shape an individual's intention to use the technology. Carayon & Smith 1995; Laerum, Ellingsen, & Faxvaag, 2001; Lapointe & Rivard, 2005; Lorenzi & Riley, 2000; Markus, 1983; Zuboff, 1988; and showed how the fit between the clinical work system and the IT will lead intended end users to accept or reject the IT, to use or to misuse it, or to incorporate it in their routine or work around it. Hu, Chau & Sheng (1999) applied the TAM to explain end-user reactions to healthcare IT, according to Holden and Karsh (p.159). According to Holden and Karsh (2009), TAM is not a model developed specifically for technology acceptance research in healthcare, in that it does not capture some of the unique contextual characteristics of healthcare information technology such as privacy and its concomitant security concerns.

Moreover, along with technological, organizational, and environmental factors of RFID adoption also depends on the expectations and self-efficacy, and the process of continued usage intention involves satisfaction from current use and the degree of self-efficacy (Hossain & Quaddus, 2011). Lee (2009) used TAM to study employee RFID acceptance. Hossain and Prybutok and Muller-Seitz et al. (2009) used TAM to study RFID in consumer a context. The TAM is presented graphically in Figure 1.



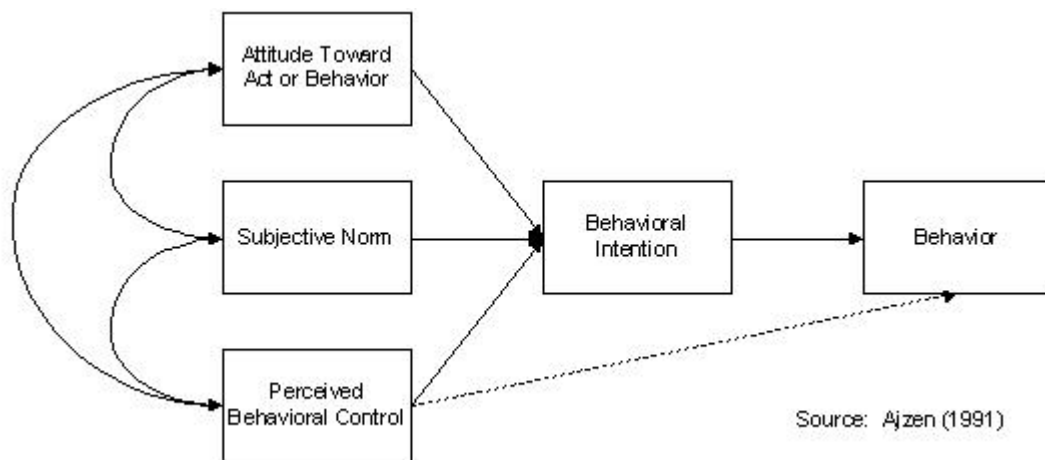
*Figure 1.* Technology acceptance model (Davis et al., 1989).

TAM underwent modifications, notably TAM 2 (2000) and TAM 3 (2008). Venkatesh, and Davis (2000), and Venkatesh (2000) extended TAM to TAM 2, to expand upon the construct of perceived ease of use to include control, intrinsic motivation and emotion. Venkatesh and Bala (2008) proposed TAM 3, which focused on interventions. This research drawing on Anderson and Agarwal (2011) draws the variable perceived usefulness from TAM (Holden & Karsh, 2009). It also applies the TAM2 variable subjective norm as well as the [behavioral] intention to use, from the Unified Theory of Acceptance and Use of Technology (UTAUT), as proposed by Venkatesh, et al., 2003). UTAUT explained 70% of the variance in the variable intention to use (Holden, & Karsh, 2009). The research presented here focused on the theoretical model provided by Anderson and Agarwal (2011), which although not stated may have had influences from UTAUT. UTAUT research conducted by Aldhaban, Daim, and Harmon (2015) on smartphone technology adoption in emerging regions noted that TAM could omit the role of important variables such as human and social factors in the adoption process. However incorporating and extensive explanation of UTAUT is beyond the scope of this paper. According to Holden and Karsh (2009) TAM and its three accepted variants, as well as TPB, are the most commonly used models when investigating technology acceptance (Holden & Karsh, 2009, p.160).



### *Theory of Planned Behavior*

Researchers use the TPB to better explain behavioral aspects of technology adaption. The Theory of Planned Behavior (TPB) model focuses on how an individual's external environment influences his or her intentions (Liu & Chen, 2009). Ajzen's (1985) first iteration of the TPB was an extension of the Theory of Reasoned Action, which added a new construct – perceived behavioral control (Armitage & Conner, 2001). Ajzen related the variables of intentions to perform a given activity to subjective norms, perceived behavioral control and attitude toward the behavior. Ajzen sums this stating: “only specific attitudes toward the behavior in question can predict that behavior” (Ajzen, 1991, p.180). Ajzen (1991) applied TPB to various social issues, such as condom use and problem drinking to determine which if any intervention in a given case was needed (Ajzen, 1991). TPB is presented in Figure 2. Dezhi, Lowry and Dongsong (2015) proposed and tested a research model using TPB and Rational Choice Theory (RCT) that investigated the compliance behavior of patients supported by a mobile healthcare system. The theory of planned behavior is presented in Figure 2.



*Figure 2.* Theory of planned behavior (Ajzen, 1991).

Subjective norm is defined as an individual's perception of whether people important to the individual think the behavior should be performed (Ajzen, 1991). Ajzen showed the constructs in TPB help researchers to better understand why individuals engage in certain behaviors. TPB is an effective tool in evaluating such decisions in healthcare settings. Norman, and Bennett (1998) used TPB to better understand binge drinking among young people; Bennett, and Bozionelos (2000) used TPB in determining condom use; Hagger, and Chatzisarantis (2002) used TPB to determine likelihood of physical activity. TPB is also useful in determining technology adoption in mixed (forced or voluntary) control contexts.

Brown, Massey, Montoya-Weiss, and Burkman (2002) discerned important differences between mandatory and voluntary use environments. Brown et al., defined voluntary-use environment as "one where users perceive the technology adoption or decision to use as a willful choice" (p. 284). While in mandatory-use environments, employees had to adopt a particular technology to keep their jobs, thereby eliminating the emphasis on prior beliefs and attitudes about the technology. Brown et al. (2002) continued by describing the deleterious effects mandatory-use environments can have on employee perception, possibly leading to delays in implementation, or possibly leading to alternative potentially destructive employee behavior (p. 284).

Lee (2008) investigated the factors influencing the adoption of Internet banking, by integrating TAM and TPB. Lee (2008) determined that intention to use online banking is adversely affected by security and privacy risks and that financial risk is positively affected by perceived benefit, attitude and perceived usefulness (p.1). Lee (2008) defined privacy risk as a loss of control over personal information, much like the privacy risk

associated with surreptitious RFID push and pull data. Lee continued by defining security risk as potential loss due to fraud, also relating to the research presented here. Lee's research diverges from the research presented here in that it considers perceived risks and perceived benefits on the dependent variables.

#### *Extended Theory of Planned Behavior*

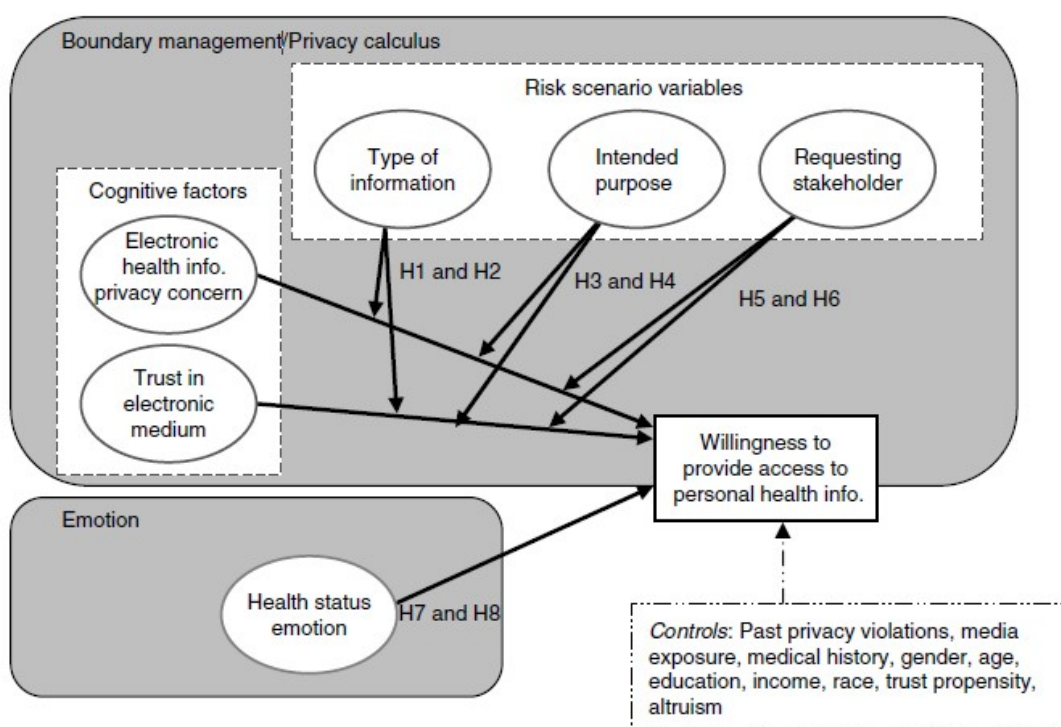
In 2002, Ajzen extended his earlier model of TPB by dividing out the construct of perceived behavioral control into two separate variables: self-efficacy and controllability. Cammock, Carragher, and Prentice (2009) used the extended TPB model to predict undergraduate intentions to apply to Northern Ireland civil service. Baker and White (2010) used the ETPB to understand influences on adolescent engagement with social networking technology. Baker and White (2010) discovered group norm was a more useful variable than subjective norm, in that it significantly predicted behavior intention by explaining 10% of the variance above and beyond standard TPM variable of subjective norm, and this finding was consistent with the research of Hogg, and Abrams (1988); Johnston, and White (2003), and finally Mason, and White (2008). The group norm variable as presented in Baker and White (2010) captured the constructs of adolescent perceptions of what their friends (peer group) are doing, as well as behaviors endorsed by the peer group (p. 1596). While these models represented baseline antecedent conditions for technology acceptance, none of them provided direct correlations between the variables investigated in this research. These models however fell short on explaining the inherent privacy calculus related to personal health information (PHI) exposure using RFID. The next section considered a model, and its

related literature that addresses many of the privacy in RFID research issues presented in this research.

*Conceptual model presented in Anderson, and Agarwal (2011)*

Anderson and Agarwal (2011) created a conceptual model to better understand the circumstances under which individuals will be willing to disclose personal health information to permit it to be digitized. Anderson and Agarwal consider how digitization of the healthcare industry has led to new and unintended consequences. Anderson and Agarwal (2011) proposed this model to explain the role of the type of information requested plays, the purpose for which it will be used and the requesting stakeholders in an individual's willingness to disclose personal health information, by applying privacy boundary theory and recent developments in literature related to "risk as feelings". The strength of this model over TAM3 and ETPB is in the way it further explicates not just reasons to accept or not to accept technology, but how antecedent conditions affect perceptions, which in turn affect the reasons for using a given technology. Anderson and Agarwal's usage of boundary management variables focused on a notion of "what is acceptable" and "what is not acceptable" in a given transaction where private information is exchanged. Communication theory, as posited by Petronio (1991) describes this as an activity that occurs during communication regarding private matters between marital couples. Anderson and Agarwal applied the well-established notions of boundary management and privacy calculus to information technology acceptance. The research presented in this paper applied a similar approach, in that it considered privacy and security concerns in the context of information being exchanged without necessarily telling any given participant when it is happening, and to which data points are being

shared. Metzger (2007) applied the same notions of communication privacy management (CPM) to the disclosure of private information in e-commerce relationships. Metzger (2007) noted applying CPM to online privacy management focuses on information that has not been publicly revealed to many people in the past. This research considered personal medical information being transmitted and possibly retained. Figure 3 represents the conceptual model Anderson, and Agarwal developed:



*Figure 3.* Conceptual model developed by Anderson, and Agarwal (2011).

The model in Figure 3 was particularly appropriate for the underpinning of the research presented here in the way it assessed privacy and security issues related to personal health information. According to Anderson and Agarwal (2011), a Harris poll conducted in 2006 showed that 25% of us adults have significant concerns about their personal healthcare information (PHI) and that 50% of US adults believe they have lost

control of this information. (p.469). Anderson and Agarwal's research considered how PHI exposure regardless of technological improvement, making the research presented in this investigation relevant regarding the burgeoning nature of RFID usage in healthcare settings. Therefore this next section presents the literature on how privacy rights interact with RFID, and how security is an extension of perceived privacy with RFID usage.

### *Privacy*

Privacy in the United States has its roots in the 1890 Supreme Court decision published by Samuel, D. Warren and Louis D. Brandeis, entitled the "The Right to Privacy." *Olmstead v. United States* (1928) Supreme Court just Brandeis defined this as the "right to be left alone." Common law (Tort Law) recognizes five rights to privacy – the most relevant to this research is "the common-right law to sue when information concerning a person's private life is disclosed to the public in a highly objectionable manner (<http://legal-dictionary.thefreedictionary.com/privacy>)." Another relevant outcome of this was protection of privacy from intrusion upon seclusion, which covered among other things, surreptitious electronic surveillance. For United States citizens, it follows then that privacy is at least protected by Constitutional law, and case-law disposition as well as Tort Law.

The Electronic Communications Privacy Act (ECPA) of 1986 does not adequately cover the ubiquity of personal computing devices seen today in society, however it did make the intentional disclosure or use of the contents of a knowingly intercepted communication a crime (<http://epic.org/privacy/ecpa/>). The definition focused on the transfer of data, or the time during which the packets of data are travelling between one point and another, which created an "on the wire" vs. "off the wire distinction which has

become complicated with the ubiquity of wireless transceivers (<http://epic.org/privacy/ecpa/>). The ECPA also protected against illegal access to stored transmission on electronic media, which in the case of the research presented here apply to persistence of data on RFID chips, and the privacy and security risks it poses (Stored Communications Act, 18 U.S.C. §§ 2701-12). Related to that, the next section considered how security issues are related to privacy issues.

### **Security as Privacy**

According to Henderson and Snyder (1999), and Westin (1967) privacy is the ability of an individual to control the terms under which personal information is acquired and used. Barkhi, Belanger, and Hicks (2008) and Pirim, James, Boswell, Reithel noted that privacy concerns have garnered much attention in recent years with the rise in identity theft and new capabilities to collect and process information. Pirim, et al. (2008) further note that less human contact and less opportunity for identification checks in e-commerce environments have exacerbated this concern (p.42). An online dictionary defines security as “freedom from danger, fear or anxiety” (<http://www.m-w.com/cgi-bin/dictionary/security>). It is further defined as measures taken to guard against espionage, crime, attack or escape. Garfinkel (2000) notes that privacy is the “right of people to control what details about their lives stay inside their own houses and what leaks to the outside.” Barnes (2006) further stated citizens and consumers should know who collects what information and how it is going to be used. In the case of RFID usage as a security problem, derived from its relationship to privacy – context is considered a key element. Concern over PHI exposure is bound by perceptions of what data is taken and how it is stored. The relationship between security as function of privacy is

explained in Barkhi, et al. (2008) where they state that an individual's perception of the importance of privacy and security on a personal level may impact their behaviors toward adoption and use of technologies in a wide variety of areas (p.44). Further, they discovered that a perceived need for privacy tended to be more important in situations where individuals did not feel comfortable with the possibilities of release of information to un-trusted parties or in other words – privacy may be something that an individual wishes to secure (p.49). Barnes (2006) notes the inherent privacy related security issues on social networks, as well as in various e-commerce paradigms that allow for user controlled privacy, but simultaneously collect and store personally identifiable information about the user. The literature here supports the notion of privacy and security concerns in a paradigm, where information is passively collected – such as that of RFID in healthcare. Considering the lack of literature regarding an intersection of privacy and security issues regarding RFID acceptance, the next sections explain how this investigation framed its hypotheses and the nature of the relationships between dependent and independent variables.

### **Proposed Research Model**

As the literature has defined certain parameters for assessing technology acceptance, across a wide-range of paradigms, this next section considers the literature underlying the creation of the theoretical model presented in this research. This investigation proposed a theoretical model that captures the behavioral aspects of Anderson and Agarwal's (2011), with modifications to combine privacy and security variables and to account for information discovered during the expert panel review. The researcher recognized that



there is the essence of TAMx and TPB represented herein and has thus explained them in the context of this investigation.

Security and Privacy Acceptance Conceptual Model (proposed)

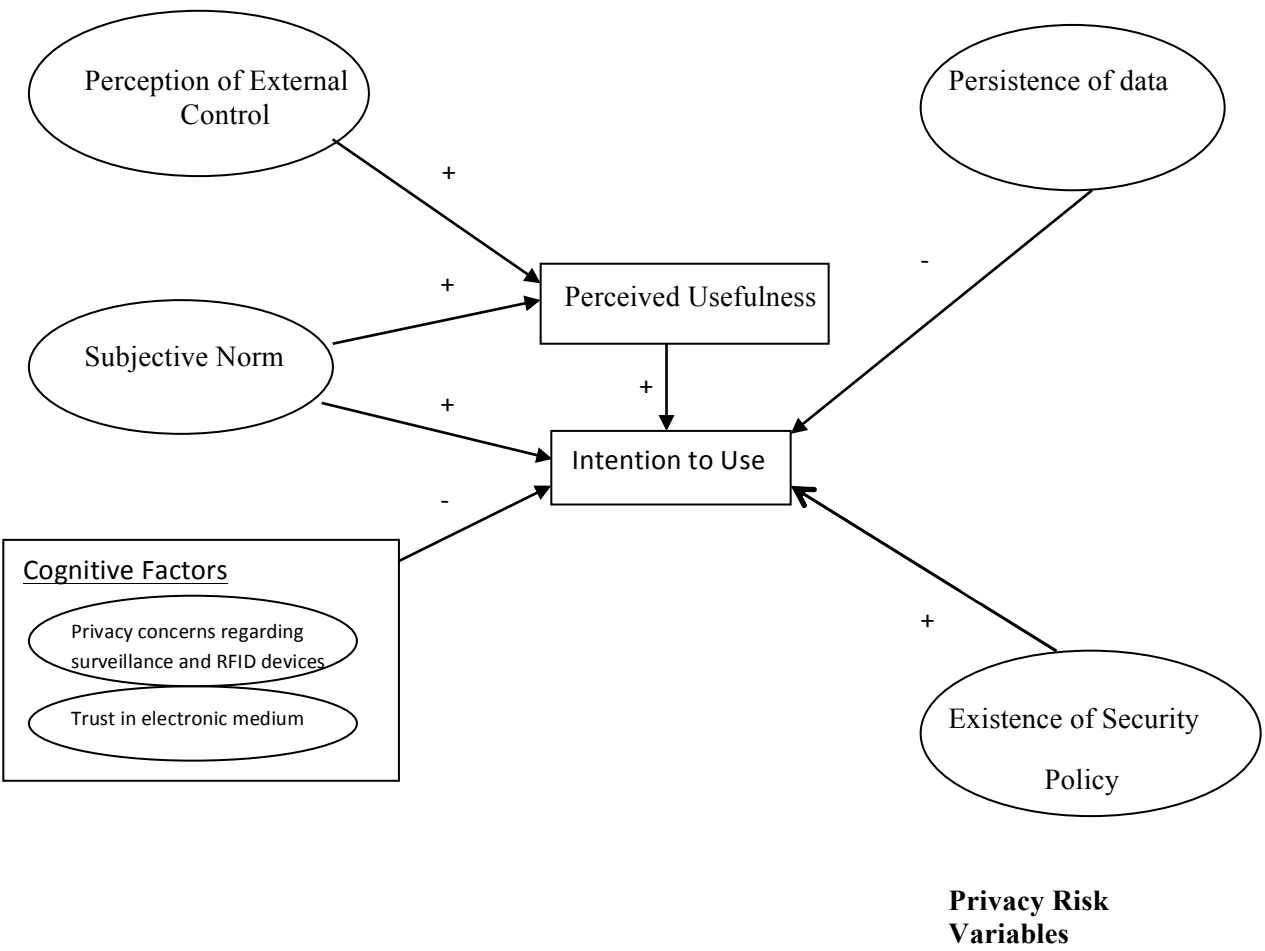


Figure 4. Conceptual Model proposed in this research

(+ denotes positive influence, - denotes negative influence)

A table matching constructs, definitions presented, and operationalized variables in this model follows.

**Table 1***A Summary of Constructs, Definitions and References*

<b><u>Construct</u></b>	<b><u>Definition</u></b>	<b><u>Operationalized</u></b>	<b><u>References</u></b>
1. Perceived usefulness	<p>The degree to which a person believes that using a particular system would enhance his or her job performance.</p> <p>Mandatory use environments, determined by internal policy sold required use as an enhancement to the nurse's job performance.</p> <p>Wireless system, and competent staff must be in place for health care information technology to function.</p> <p>No studies before 2008 regarding acceptance of information technology in health care settings captured notion that health IT might be useful for not only enhancing performance, but also making performance easier and more satisfying, increasing efficiency, lowering costs, and improving safety of care.</p>	How I perceive the control over the technology as well as those who influence my decisions will determine how useful I perceive the technology to be. (adapted from Davis (1989).	<p>Davis(1989)</p> <p>Norten(2011)</p> <p>Carr, Zhang, Klopping &amp; Hokey (2010)</p> <p>Holden &amp; Karsh (2009)</p>

<p>2. Perception of External Control</p>	<p>Feeling of control an individual has toward the use of computer based on the availability of knowledge, resources and opportunities required for its use.</p> <p>External control shapes intention and behavior in a variety of domains.</p> <p>External control can be defined as pull-based, location-based-systems (LBS), where the individual can choose thus giving user more security and privacy control.</p> <p>Push-based LBS allow services to geo-locate and send targeted messages to a user, without consent and or knowledge.</p> <p>Well managed, controlled wireless systems must exist for RFID environments.</p> <p>Comprehensive wireless, well-designed wireless networks under administrative control must exist for RFID to function.</p>	<p>Perception of external control will have a positive effect on perceived usefulness of RFID technology. (adapted from Hosaka, 2004).</p>	<p>Venkatesh(2000)</p> <p>Ajzen(1985)</p> <p>Xu, Gupta and Shi(2009)</p> <p>Lee and Shin(2009)</p> <p>Carr, Zhang, Klopping &amp; Hokey (2010)</p> <p>Hosaka (2004)</p>
--	--	--	---

<p>3. Subjective norm</p>	<p>Whether or not people important to the individual think the behavior should be performed.</p> <p>Used UTAUT to determine that social influence, and facilitating conditions showed positive return on improved performance using RFID devices in an emergency room environment.</p> <p>Theory of planned behavior provided moderate increase in the explanation of behavioral intention.</p>	<p>Subjective norm has a positive effect on perceived usefulness and intention to use.</p> <p>People Who influence my behavior would think that I should use RFID. People who are important to me think that I should use RFID (both adapted from Taylor and Todd, 1995).</p>	<p>Davis(1989);</p> <p>Chen, Wu &amp; Crandall (2007)</p> <p>Taylor &amp; Todd (1995)</p>
---------------------------	---	---	---

<p>4. Intention to use</p>	<p>Factors leading a person to use a particular technology.</p> <p>Positive correlation between subjective norm and intention to use.</p> <p>Context plays a significant role in healthcare IT acceptance.</p>	<p>If RFID devices are storing information and keeping it somewhere and if there is a security policy governing RFID usage in my hospital, it will affect my intention to use the technology. Also, how I perceive the technology as a device used for surveillance and how others I respect think about the technology will affect whether or not I want to use the RFID technology in the hospital (adapted from Venkatesh &amp; Davis (2000).</p>	<p>Venkatesh and Davis(2000)</p> <p>Adams, Nelson, &amp; Todd, (1992); Bruner &amp; Kumar, (2005); Davis (1989); Davis et al. (1989); Heijden et al. (2003); Igarria et al. (1997); Liao et al. (2007); Lin &amp; Lu (2000); Luarn &amp; Lin (2005); Mathieson (1991); Moon &amp; Kim (2001); Taylor &amp; Todd (1995); Wu &amp; Wang (2005); Yang (2005)</p> <p>Holden &amp; Karsh (2009)</p>
----------------------------	--	--	--

<p>5. Cog Factors: Privacy concerns regarding surveillance and RFID devices</p>	<p>Mandatory use of RFID constitutes a violation of privacy rights.</p> <p>Location based information poses a privacy and personal security risk.</p> <p>Willingness to disclose information as a condition for transacting [electronically] is an outcome variable that is consistent with prior privacy research.</p> <p>Users are reluctant to provide location information particularly when the data is automatically captured by the system.</p> <p>Location based services potential is obscured by privacy issues.</p> <p>Privacy is typically assumed in situations where customers are not aware that it can be violated.</p> <p>Privacy concerns differ, depending on the type of information involved.</p>	<p>When I think about privacy concerns and surveillance capabilities of RFID devices, they have a negative effect on my intention to use them. Privacy issues and surveillance will affect my intention to use the technology (adapted from Hossain &amp; Prybutok (2008); Beresford(2003); Myles and Friday(2003); Malhotra, et al.(2004); Hong, Ng, Lederer, and Landay(2004) Malhotra, et al.(2004).</p>	<p>Chanen(2008)</p> <p>Beresford(2003); Myles and Friday(2003); Malhotra, et al.(2004); Hong, Ng, Lederer, and Landay(2004)</p> <p>Malhotra, et al.(2004)</p> <p>Röcker(2010)</p> <p>Xu, Gupta, and Shi(2009)</p> <p>Hossain &amp; Prybutok (2008)</p> <p>Phelps, D'Souza, &amp; Nowak (2001); Culnan (1993)</p>
---	--	---	--

<p>6. Cog Factors: Trust in electronic medium</p>	<p>Trust and perceived risk are direct antecedents of intention to use.</p> <p>There is a paucity of Promulgated federal regulations protecting privacy on RFID devices.</p> <p>Definitions of privacy among consumers and customers likely differ.</p>	<p>I trust the electronic medium that RFID represents. Privacy issues and trust in the technology will affect my intention to use the technology (adapted from Pavlou, 2003).</p>	<p>Pavlou(2003)</p> <p>National Council of State Legislatures (2013)</p> <p>Xu, Gupta, and Shi(2009)</p>
---	---	---	--

<p>7. Persistence of data</p>	<p>Concerns over the collection of the data as well as concerns over the storage of the data collected will affect the intention to use (or be subjected to the use of) a certain technology.</p> <p>Discovered a correlation of persistence of data to privacy concerns in sensor networks.</p> <p>Described security concerns such as a lack of cryptographic capability, ability to detect duplicates, and how data retention of device information captured in a database affect intention to use.</p> <p>Privacy risk is classified into three categories: threats to spatial boundaries, threats to temporal boundaries due to persistence of data, and intersections between multiple spaces.</p>	<p>I am concerned about RFID data containing personally identifiable information being stored in a persistent device such as a database or a server. (adapted from Juels 2006, and Kamra et al. (2006).</p>	<p>Konomi(2004)</p> <p>Kamra, Feldman, Misra and Rubenstein(2006)</p> <p>Juels(2006)</p> <p>Palen &amp; Dourish (2003)</p>
-------------------------------	--	---	--



<p>8. Existence of Security Policy</p>	<p>Security policy defines execution, which for one reason or another has been deemed unacceptable.</p> <p>Extant security policy positively influences perceived usefulness, which in turn affects intention to use.</p> <p>Trust in the technology provider also increased intention to use.</p> <p>Positive relationship between security / trust and technology acceptance.</p> <p>Trust of the user's firm through security policies is key factor, and foments later successful acceptance.</p>	<p>A strong security policy will encourage me to use the technology.</p>	<p>Schneider (2000)</p> <p>Lee(2009)</p> <p>Hernandez-Ortega (2011), and Grabner-Krauter et al. 2003)</p> <p>Hernandez-Ortega (2011)</p> <p>Grabner-Krauter &amp; Kaluscha (2003); Yousafzai, Pallister &amp; Foxall (2003)</p>
--	---	--	---

Persistence of data and subjective norm were expected to affect intention to use as well. Another variable affecting intention to use was described by this model as existence of security policy. Perceived usefulness affects intention to use in a hospital setting. Kim, Kim and Chung (2015) state that information security is both a technical, and a social issue. The research model presented here tested several privacy and security concerns associated with RFID usage. The conceptual model presented in figure 4 is based on TAM 3, TPB and the model research conducted by Anderson & Agarwal (2011). The research questions presented here essentially consider acceptance of information technology in a specific context, based on the core of the TAM model (Davis, et al., 1989). Hossain, Prybutok, and Muller-Seitz et al. (2009) used TAM to study consumer RFID acceptance. Ajzen considered how intrusive technologies, which took control away from individuals affected their behaviors regarding usage (Ajzen, 1991; Cammock et al., 2009). This literature review focused on behavioral aspects to use technology, and considers research from the e-commerce, information systems acceptance and telemedicine fields.

Muller-Seitz, et al. (2009) remarked that drivers of customer acceptance of RFID technology remain unclear; and that RFID technology has primarily been analyzed in business-to-business settings. Anderson and Agarwal (2011) focused on behavioral constructs using and extended the theories of planned behavior and the TAM by focusing on privacy calculus to determine RFID accepting in mandatory use settings. The theoretical model presented here focused on security and privacy issues. The next section describes the variables used in the proposed theoretical model in the context of prior research.

### **Perceived Usefulness and its Determinants**

Perceived usefulness is defined as the degree to which a certain system is able to increase one's performance at work as perceived by that individual (Davis, 1989).

Venkatesh and Davis (2000) proposed TAM2 and defined the determinants of perceived usefulness are: subjective norm, image, output quality, job relevance and result demonstrability, and perceived ease of use (Venkatesh & Bala, 2008, p. 276-277). For the purposes of this research, the theoretical model presented only investigated two of these determinants – Perception of external control, defined as the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system (Venkatesh.com), and subjective norm, defined also by Venkatesh (2000) as a person's perception that most people who are important to the person think he/she should use the new system Venkatesh (2008). Venkatesh and Davis (2000) with TAM 2 stated that subjective norm, job relevance, image, output quality and results were determinants of perceived usefulness, and that experience was a moderator of relationship between subjective norm and intention to use (Carr, Zhang, Klopping & Hokey p. 28). Holden and Karsh (2009) considered studies published before 2008 regarding acceptance of information technology in health care settings and determined that none of the studies captured the idea that health IT might be useful for not only enhancing performance, but also making performance easier and more satisfying, increasing efficiency, lower costs, and improving safety of care (p. 162). In order for a hospital to implement RFID system, the hospital must have a wireless system in place and staff with competency to install and manage the system (Carr et al., 2010).

*Perception of External Control Influences Perceived Usefulness*

This model differed slightly from TAM3 in its presentation, because it assessed perception of external control as a direct determinant of perceived usefulness. In fact, Venkatesh (2000) demonstrated perception of external control as a determinant of “perceived ease of use”, and perceived ease of use as a determinant of perceived usefulness, thus perceived ease of use is a determinant of perceived usefulness. Holden, and Karsh (2009) defined “ease of use” as easy to learn, easy to operate, requiring low mental effort. In this research, the investigator focused on one of the determinants of perceived ease of use, and related it directly to perceived usefulness. Venkatesh (2000) defines perceived ease of use as effort expectancy, or the degree of ease associated with the use of the system. RFID devices are transponders and according to Carr et al. (2010) the devices require little or no user interaction, thus ease of use of RFID devices is assumed in this research. Carr, et al. (2010) noted that as healthcare organizations become more sophisticated in their use of information technology, they are likely to support more advanced information systems such as ones that use RFID. They state further that new systems have to be integrated with extant ones (p.29). Venkatesh (2000) defines perception of external control as the feeling of control an individual has toward the use of a computer based on the availability of knowledge, resources and opportunities required for its use. Conceptualization of external control (Ajzen, 1985) has an important role in shaping intention and behavior in a variety of domains. Perceived ease of use influences intention of use, indirectly through perceived usefulness. In addition, personal factors (perception of external control, anxiety towards computers, intrinsic motivation)

play an important role in the formation of perceived ease of use of virtual reality but do not have a direct impact on intention of use (Bertrand & Bouchard, 2008). An example of external control can be described as push vs. pull technology implementations, which require existing wireless infrastructure. According to Xu, Gupta & Shi (2009), pull-based location based systems (LBS) the individual can choose, and thus more security and privacy are realized. Push-based LBS on the other hand allows services to geo-locate and send targeted messages to the user, often without their consent or knowledge. RFID is a technology push and need pull system (Lee & Shim, 2009). Hosaka (2004) stated RFID implementations require comprehensive wireless networks. Carr et al. 2010 notes that adoption of RFID technology in the healthcare industry depends heavily upon the healthcare provider's ability to implement technological infrastructure, including hardware, software and middleware and that failing in any of these areas inhibits ability to implement an RFID solution.

A final example of how perception of external control affects RFID usage includes: Gunther and Spiekermann (2005) who investigated German retailers and discovered that most German consumers voiced concerns over losing privacy shopping at a retailer who used the devices over fear that the retailer would use the data for other purposes, and the consumers wanted the devices killed upon exiting the store.

Thus we proposed the following hypothesis:

H1: There is a positive relationship between perception of external control and perceived usefulness.

### *Subjective Norm Influences Perceived Usefulness*

Subjective norm is defined as an individual's perception of whether people important to the individual think the behavior should be performed (Davis, 1989). Holden and Karsh (2010) define it as social influence, and note that in healthcare IT settings it ignores other ways that social factors indirectly influence behavior, (p. 163). Chen, Wu and Crandall (2007) using the UTAUT considered how external performance acceptance among doctors in an emergency room was hampered because vital signs could not be managed or tracked in real-time on all patients. Their research considered how social influence and facilitating conditions showed a positive return on improved performance using RFID devices. Mather, Caputi and Jayasuriya (2000) noted differences in subjective norm influence technology acceptance in mandatory use environments. In mandatory use environments in hospitals, RFID devices are required to be used by management. This does not mean that compliance is at 100% however (Norten, 2011) and Davis (1989) defines perceived usefulness as the degree to which a person believes that using a particular system would enhance his or her job performance. Thus, in mandatory use environments, a policy decision determines that not only should the behavior be followed -wearing an RFID device in Norten, (2009), but also that the device will ultimately help their job performance. Norten's research concluded that mandatory use environments cause nurses to feel overly scrutinized for little gain. Hossain and Prybutok (2008) determined that in retail settings, consumers did not feel privacy was an important factor, because the end use of the RFID tags was for inventory control only. Subjective norm thus can be required policy or voluntary, but in either case it will affect

perceptions of the behavior on job performance. Thus we proposed the following hypothesis:

H2: There is a positive relationship between subjective norm and perceived usefulness.

### **Intention to Use and its Determinants**

Venkatesh and Davis (2000) noted the factors leading a person to use a particular technology, thus “intention to use” can be defined as the sum of those behavioral factors. *Cognitive factors of trust in electronic medium and privacy concerns regarding surveillance and RFID devices will have an effect on perceived usefulness of RFID.*

Norten (2011) investigated privacy issues concerning RFID usage among nurses in a mandatory use environment. According to an unidentified nurses union cited in Chanen (2008) mandatory usage of RFID tags on a nurse’s person constituted a violation of privacy rights. The cognitive factors of privacy concerns regarding surveillance as well as the trust in the electronic medium [technology] are based on perceptions of these issues. They are different from the privacy issues in the theoretical model of persistence of data and existence of security policy because they refer to either policy based decision – to store data, or to have a over-arching security policy in the hospital. They do not concern perceptions, as the cognitive factors noted in the theoretical model do. Privacy and security issues with devices providing location based information are mentioned in a body of literature that focuses on privacy issues considered the issue of providing location based information on an ongoing basis, as well as the privacy and security risks this poses (Beresford, 2003; Myles and Friday, 2003; Malhotra et al. 2004, Hong, Ng, Lederer, & Landay, 2004). Malhotra et al. (2004) discovered willingness to disclose

information as a condition for transacting is an outcome variable that is consistent with prior privacy research. These studies investigated ways to mitigate privacy concerns with the constant transmission of personal devices that showed location, using the global positioning system. Röcker (2010) found that users are reluctant to provide context (location) information, particularly when the data is automatically captured by the system. Röcker's study focused on cross-cultural differences regarding willingness to provide context information, and related cultural background, degree of computer knowledge to it. As with other similar research though, this study focused more on the perceived privacy risks, vice the security risks, and their effects on intention to engage in use of the technology. RFID transmission occur in open air, thus are vulnerable intercept, posing a privacy based risk with security ramifications, which will almost certainly negatively affect the user intention to engage in use of the technology.

Xu, Gupta, and Shi (2009) described how privacy issues such as location information security, and trust of electronic medium obscure the potential of location-based services (LBS). The literature defines LBS as network-based services that integrate a mobile device's location with other location based information to include: entertainment, dining and emergency services options. According to Xu, et al. (2009) LBS can also be used in asset tracking, such as in the case of RFID. Xu et al. describe this self-assessment of privacy as a sort of cost-benefit analysis that considers the risks associated with disclosing personal information. Anderson & Agarwal (2011) expand upon this stating personal information, in the case of health related information has gradations of importance, based on type of information, intended use for the information and finally the identity of the entity requesting the information. Xu and Gupta (2009) hypothesized that



such privacy concerns, here described as cognitive factors are negatively related to the intention to use LBS, such as RFID as presented in the research here.

Pavlou (2003) related trust in electronic medium to consumers' intention to use technology. Pavlou (2003) further concluded that trust and perceived risk are shown to be direct antecedents of intention to use [transact], suggesting that uncertainty reduction is a key component of acceptance (p. 123). Pavlou's research focused on intention to transact in an ecommerce environment, however the research proposed here follows the same behavioral constructs designed earlier – TRA, and TAM in determining intention to use a technology.

According to Cao, Jones, and Sheng (2014) patients don't usually like to be watched or monitored but in hospitals patients have different expectations of privacy. Privacy is typically assumed in situations where customers are not aware that it can be violated, according to Hossain and Prybutok (2008, p. 324). Also some consumers may have a different definition of privacy (Xu & Gupta, 2009). Privacy has state and federal legal definitions and scope, however there is no specific federal law that protects the privacy of individuals in regard to information gathered on an RFID chip. As of 2013, 14 states, which include Arkansas, California, Michigan, Minnesota, Nevada, New Hampshire, North Dakota, Oklahoma, Rhode Island, Texas, Vermont, Virginia, Washington, and Wisconsin have enacted legislation regarding RFID in the context of privacy (National Council of State Legislatures [NCSL], 2013). A lack of promulgated federal regulation combined with a similar lack of understanding regarding what and how data is captured cause trust and confidence issues in cases where RFID devices surreptitiously capture and possibly store information.

Phelps, D'Souza, and Novak (2000), and Culnan (1993) cited in Anderson and Agarwal (2011) note that “privacy concerns differ across types of information; for example, concerns regarding financial information are deeper as compared with demographic profiles or lifestyle interests” (p.470).

Thus we proposed the following hypothesis:

H3: The cognitive factors of privacy concerns, regarding surveillance and trust in the electronic medium have a negative relationship with intention to use.

#### *Persistence of Data Influences Intention to Use*

There is very little literature regarding the persistence of data influencing the intention to use in RFID acceptance. Most of the literature considers privacy risk as the key element in persistence of data research. Not to be confused with the Cognitive factors of privacy concerns regarding surveillance and trust in the [technology] electronic medium, persistence of data refers specifically to the persistent storage on a server or other storage mechanism of data collected from an RFID device during the course of its usage in a medical context. Cao, Jones and Sheng (2014) stated that RFID use healthcare has unique barriers to technology adoption, to include concern for security and privacy of patient data, and that widespread implementation of RFID technology has not occurred in healthcare environments. Palen and Dourish (2003), cited in Zhao, Lu and Gupta (2012) classified challenges to interpersonal privacy risk into three categories: threats to spatial boundaries, threats to temporal boundaries due to persistence of data and intersections between multiple spaces, but this research considered location based service network applications, not RFID. In a similar manner, Konomi's (2004) research considered the issues of privacy, and value of the data, in regards to context of the data collected. His

example of a customer not knowing who is monitoring his actions, or who will search records of the actions, if collected may be unwitting of the data collection and storage until weeks or months later the customer receives a marketing email (p.3).

Understanding of the usage of the data, and the security of the data collected relates to the customers understanding of the technology and their perceptions of how the technology adds value. Thus it appears that internalized notions of privacy, and understanding of data usage, storage or persistence would affect a users view on value add of a given technology. A recurring security concern about persistence of data in a sensor based network, such as RFID can both positively and negatively affects intention to use. Kamra, Feldman, Misra, and Rubenstein (2006) correlated the persistence of data to privacy concerns in sensor networks. Since push/pull networks such as those used in RFID networks can surreptitiously capture data, and potentially store the data, the perceptions and understanding of the RFID system parameters will affect whether or not an individual willfully uses the technology (Kamra et al., 2006).

Juels (2006) considered the security vulnerabilities of RFID technology, and focused on obvious issues such as a lack of cryptographic capability as well as less obvious ones like ability clone the device, detect duplicates, and how data retention either on the device or in a centralized database causes other security concerns, which would affect intention to use, and perceived usefulness. In this instance cloning a centralized database is necessary to compare current activity with device identification. Security concerns abound as to whether RFID device databases contain simply RFID specific information, or information received, recorded on the device and transmitted back to the others in the RFID network (Juels, 2006). Legislation protecting persistent data in applications is not

standard in the US. Idaho and Illinois included a provision for criminal prosecution under its identity theft legislation, which protects against the use of PII obtained from an RFID in any sort of criminal activity (NCSL, 2012).

Thus we proposed the following hypothesis:

H4: There is a negative relationship between persistence of data and intention to use.

#### *Subjective Norm Influences Intention to Use*

A body of literature regarding TAM, TAM2, UTAUT, and the TPB shows a positive correlation between subjective norm and intention to use (Adams, Nelson, & Todd, 1992; Bruner & Kumar, 2005; Davis, 1989; Davis et al., 1989; Heijden et al., 2003; Igbaria et al., 1997; Liao et al., 2007; Lin & Lu, 2000; Luarn & Lin, 2005; Mathieson, 1991; Moon & Kim, 2001; Taylor & Todd, 1995; Wu & Wang, 2005; Yang, 2005). As described earlier in this research, subjective norm as proposed in the research model presented herein influences both perceived usefulness and intention to use. The next section described how subjective norm affects intention to use. Subjective norm is defined as perceived social pressures to perform or not to perform a certain behavior (Cammock, et al., 2009). Norton showed that mandatory use environments while not allaying privacy concerns; strongly influence intention to use the devices. One of the goals of the TAM, TAM 2, TAM 3, and the TPB, as well as the EPTB was to describe which perceived social factors urge a person to perform or not to perform a certain behavior based on social pressure, or group behaviors (Cammock et al., 2009). According to Holden and Karsh (2009),

“...the direct route of social influence through others having an influential opinion about another’s health information system use was generally the same, but the source of social influence varied in specificity - e.g.: “important others” versus “important other pediatricians” and type – e.g.: “colleagues” versus “subordinates”(p. 164).”

Holden and Karsh (2009) continue by suggesting that context plays a significant role in healthcare IT acceptance, perhaps making the customary commercial context of extensive TAM validation less relevant to healthcare contexts (p. 169).

Thus we proposed the following hypothesis:

H5: There is a positive relationship between subjective norm and intention to use.

#### *Security Policy Influences Intention to Use*

Schneider (2000) stated, “...A security policy defines execution, which for one reason or another has been deemed unacceptable.” He continues by stating: “security policies restrict access, and restrict information flow (p.30).” This research considered how the latter restriction of “information flow” applies in RFID environments. The idea of security policy being a determinant of intention to use RFID is lacking in the literature, however there is some related literature in the areas of e-commerce and e-banking. For this research trust in the system based on either implied or de facto security policies can encourage intention to use a system or technology. According to Siponen,(2000) intention to use implies attitude towards use, which is divided into two elements, one of which has already been discussed: perceived usefulness, and perceived ease of use (p.36).

Hernandez-Ortega (2011) investigated acceptance of e-invoicing in a Spanish company, and determined a positive relationship between security and trust, and between both of those ideas and acceptance of the technology [use]. Further, she cites Grabner-Krauter and Kaluscha (2003) and Yousafzai, Pallister, and Foxall (2003) stating: “trust of the user’s firm is a key factor, which must appear after initial uses of a technology, and foments its later successful acceptance (p.523).”

Lee investigated the idea of security trust, related to existing security policies in a corporate setting. Lee (2009) conducted survey research on Korean companies using RFID and noted that security trust and extant security policy positively influence perceived usefulness [and perceived ease of use], but did not consider the effects of these two variables on [behavioral] intention to use. Lee (2009) noted corporate security policy plays a role in RFID acceptance. Lee (2009) conducted survey research on employees of public companies to test the variable security trust, represented in above as existence of a security policy. Security concern is captured by the variables persistence of data and willingness to provide GPS information. Lee’s research considered three categories of security trust, provider trust and employee knowledge. His research further showed that the most important factor affecting perceived usefulness and perceived ease of use was provider trust [security], and that this variable was based on past experiences with the IT service provider (p. 86).

Thus we proposed the following hypothesis:

H6: There is a positive relationship between the existence of security policies and intention to use.

### **Summary of What we Know and do not Know about the Topic**

Anderson and Agarwal (2011) note theory development regarding privacy and PHI has lagged behind. “Privacy theories have yet to incorporate emotion as a key construct, despite empirical evidence indicating that emotions have a profound influence on decisions (Anderson & Agarwal, 2011, p.270).” Norten (2011) investigated a specific use example of nurses’ RFID acceptance in a mandatory use environment. The investigation presented here extends this research by using a different model as its underpinning, proposing a new model for experimentation, and investigating different privacy and security aspects of RFID acceptance. Furthermore it considers the technology from the viewpoint of the doctors as well. Based on the lack of literature related to healthcare practitioners’ privacy and security concerns with RFID usage in hospital settings, the researcher conducted an investigation to test and validate a model for predicting behavioral intention to accept RFID technology.

## **Chapter 3**

### **Methodology**

#### **Research Setting**

Bhattacharya (2008) defines “research setting” as:

“... the physical, social, and cultural site in which the researcher conducts the study. In qualitative research, the focus is mainly on meaning-making, and the researcher studies the participants in their natural setting. The contrast with post-positivist, experimental, and quantitative research settings lies in the fact that here the investigator does not attempt to completely control the conditions of the study in a laboratory setting, instead focusing on situated activities that locate her or him in the context.

The research setting for this investigation was online, and considered effects of RFID (described below) in hospital settings in the US.

The study addressed the following research questions:

RQ1: How does the existence of a data security policy affect the intention to use RFID in US hospitals? (Grabner-Krauter & Kaluscha, 2003; Hernandez-Ortega, 2011; Lee, 2009; Schneider, 2000).

RQ2: How does persistence of data or data retention affect the intention to use RFID in US hospitals? (Juels, 2006; Kamra, et al., 2006; Konomi, 2004; Palen & Dourish, 2003).



RQ3: How does subjective norm affect the intention use RFID in US hospitals?(Chen, et al., 2007; Commock et al., 2009; Davis, 1989; Mather, et al. 2000).

RQ4: How does perception of external control affect the perceived usefulness of RFID in US hospitals? (Ajzen, 1985; Carr, et al., 2010; Hosaka, 2004; Lee, et al., 2009; Venkatesh, 2000; Xu, et al., 2009).

RQ5: How do the cognitive factors of privacy concerns regarding surveillance and RFID devices as well as trust in the electronic medium affect intention to use RFID in US hospitals? (Beresford, 2003; Chanen, 2008; Hong, et al., 2004; Malhotra, et al., 2004; Myles et al., 2003; Röcker, 2010; Xu, et al., 2009).

RQ6: What is the relative strength of the contribution of the five variables (i.e., persistence of data, cognitive factors, existence of data security policy, subjective norm, and perception of external control) in predicting behavioral intention of doctors and nurses to use RFID in US hospitals?

### **Sample Characteristics**

Yin (2009) stated that sample selection should be based on a set of criteria that deem the persons selected to be qualified. In this research, both doctors and nurses used RFID in different ways. The stratified sampling technique focused on a target population of male and female medical doctors and registered nurses aged 18 years and older. Sekaran (2003) states that the reasons for limiting a sample are self-evident. Carefully selected samples produce more reliable results (Sekaran, 2003, p. 267). The survey used Survey Monkey's<sup>TM</sup> Audience<sup>TM</sup> feature. Audience<sup>TM</sup> allows a researcher to distribute a survey instrument electronically to groups of people meeting certain demographic

characteristics. Using Survey Monkey's Audience<sup>TM</sup> feature, the researcher directed doctors and nurses to complete an online survey, which was designed to elicit information regarding the independent variables of perception of external control, subjective norms, and cognitive factors, persistence of data and existence of security policy impact on their intention to use RFID technology. The control questions at the beginning of the survey focused on eliciting information regarding the dependent variables of perceived usefulness, intention to use.

### *Population and Sample*

Social science research uses a p value of <less than or equal to> .05. Aczel & Sounderpandian (2006) noted that it is necessary to calculate a suitable significance level for rejecting the null hypothesis. The same authors stated that significance level standard values are 1%, 5% and 10%. Lipsey (1990) states that an alpha of .05 relates to the (1-alpha)=.95 probability of an accurate statistical determination when the null hypothesis is true. This study used the alpha value of .05, as it is the value commonly chosen in social science research (Lipsey, 1990).

“The null hypothesis is a proposition that states a definitive, exact relationship between two variables. It can be implied through the null hypothesis that any differences found between two sample groups or any relationship found between two variables based on our sample is simply due to random sampling fluctuation and not due to any “true” differences between the two population groups, or relationships between two variables (Sekaran, 2003, p. 105)”

According to Aczel and Sounderpandian (2006), it is necessary to calculate a suitable significance level for rejecting the null hypothesis. According to Lipsey (1990),

significance level standards are .01 (1%), .05 (5%) and .10 (10%). An alpha of .05 relates to the  $1 - \alpha = .95$  probability of an accurate statistical determination, when the null hypothesis is true. Cohen (1992b) notes that “the power of a statistical test of a null hypothesis is the probability that the null hypothesis will be rejected when it is false, in other words the probability of obtaining a statistically significant result” (p. 98). Cohen further states that an acceptable level of power is .80, making type II errors four times more probable than type I errors. A power level of .80 will be used for this investigation to calculate the sample size.

### **Sample Size**

Roscoe (1975), cited in Sekaran (2003) noted that sample size should be 30-500, and should be 10 times the number of variables in the study (p.295). This research has 5 independent and 2 dependent variables, making a very rough estimate of sample size, according to this method of 90. According to Cohen (1992b) it is important to determine the sample size that is needed for the statistical analysis in an investigation, taking into consideration level of significance, population effect size, and power. Cohen stated:

“Statistical power analysis exploits the relationships among the four variables involved in statistical inference: sample size (N), significance criterion ( $\alpha$ ), population effect size (ES), and statistical power. For any statistical model, these relationships are such that each is a function of the other three. For example, in power reviews, for any given statistical test, we can determine power of a given  $\alpha$ , N, and ES. For research planning, however, it is most useful to determine the N necessary to have a specified power for given  $\alpha$  and ES (p. 156).”

Cohen (1992a) notes that for regression, effect sizes are large if they are .35 or greater, medium if they are .15 - .34 and small if they are .02 - .15. A large sample size is needed for a small effect size and a small sample will result in a large effect size (Cohen, 1992a).

The study will use multiple linear regression analysis to determine the statistical significance of the attempted predictions, and determine the strength of association between the independent and dependent variables. The planned study used both multiple and linear regression and multiple linear regression analyses. The program G\*Power 3.1.9.2 was utilized for determining the minimum sample size of 100 using a medium effect size of 0.3, and a significance level of .05.

**t tests** - Correlation: Point biserial model

<b>Analysis:</b>	A priori: Compute required sample size	
<b>Input:</b>	Tail(s)	= One
	Effect size $ \rho $	= 0.3
	$\alpha$ err prob	= 0.05
	Power (1- $\beta$ err prob)	= 0.9303196
<b>Output:</b>	Noncentrality parameter $\delta$	= 3.1448545
	Critical t	= 1.6605512
	Df	= 98
	Total sample size	= 100
	Actual power	= 0.9303196

*Figure 5.* G-Power results

## **Instrumentation**

### *Survey Method*

In an effort to better understand the cause and effect between the independent variables and the dependent variable, the researcher conducted several unstructured interviews. Sekaran (2003) suggests that such interviews be conducted among various layers of the hierarchy in a given setting; and keeping with this suggestion, the researcher interviewed both nurses and doctors. A survey methodology was employed for conducting this research. Palvia, Leary, Mao, Midha, Pinjani, and Salam (2004) state survey methodologies have a high degree of external validity, and thus can be used to validate predictive models. The study's prediction of behavioral intention to use RFID in US hospital systems was based on the relative strengths of the contributions of the independent variables of persistence of data, willingness to provide GPS info, existence of data security policy, subjective norm, and perception of external control on the dependent variable behavioral intention to use RFID.

According to Straub (1989), a survey questionnaire is valid when it contains relevant questions, drawn from a larger body of questions in literature. Previously identified questions, taken from existing constructs are more easily verifiable (Kitchenham & Pfleeger, 2002). The author used already validated items to better assess the effects of perceived security, security concerns, and security trust on the behavioral intention to use RFID in US Hospital Systems. The author distributed survey links electronically using an appropriate the proprietary Audience tool on Survey Monkey website. The surveys were conducted using a web-based format, as they eliminate data entry errors, and

encourage greater participation due to their ease of use and relatively low cost (Levy, 2006; Rhodes, Bowie & Hergenrather, 2003). The survey used a Likert scale and was derived from previously validated questions such as those created by Xu and Gupta (2009), Cammock et al. (2009), and Taylor and Todd (1995).

The questionnaire used in this survey was based on pre-existing questions, previously validated for other research efforts. The analysis presented regarding the questions on the survey used well-known regression techniques; however the theoretical model presented herein uses a unique and different relationship and mix of dependent and independent variables. The survey was distributed through the Internet, using a Web-based questionnaire. Web-surveys facilitate an easily accessible medium through which to participate at little to no cost to the participants (Fleming, Bowden 2009; Rhodes, Bowie & Hergenrather, 2003). The questionnaire is located in Appendix A. Leidner and Jarvenpaa (1995) suggest using existing variables instead of creating new constructs, and this survey used questions validated by Cammock et al.(2009), Grabner-Krauter, et al. (2003), Hernandez-Ortega (2011), Lee (2009), Venkatesh et al.(2003), and Xu and Gupta (2009).Boudreau, Geffen and Straub (2001) stated that pre-existing survey items that related to constructs relevant to contemporary research have been used repeatedly in the literature.

## **Instrument Validation**

### *Expert Panel Review*

The researcher called on an expert panel in order to examine the proposed instrument. The expert panel included medical personnel. The researcher discussed open-ended

questions regarding the instrument with the expert panel. After discussion, the researcher determined that the tool was adequate, with a few exceptions:

1. Perception of external control does not matter.
2. Subjective norm does not matter.
3. Privacy concerns and trust in electronic medium are very important.
4. Persistence of data matters.

The researcher considered these discussions during the design of the instrument, and the expert panel and their comments regarding the proposed instrument further shaped and improved the proposed survey tool explicated in this research.

### **Operationalization of Variables**

#### *Measure of Subjective Norm (SN)*

The measures for SN in this survey were adapted from survey items developed and validated by Taylor and Todd (1995), as well as Venkatesh et al. (2012). Taylor and Todd had a Cronbach's alpha of .88 for the items. The research presented herein substituted RFID for the term computer resource center. Venkatesh (2012) had a Cronbach's alpha of .82 for the related items. In this research, RFID was substituted for the term mobile internet. The measures of Subjective Norm are numbers SN1-SN3 in the survey.

#### *Measures of Privacy (MP)*

The Measures of Privacy (MP) questions considered both variables: Persistence of Data and Existence of Security Policy. The two measures of privacy were based on a validated instrument created by Smith et al. (1996), Lee (2009), and finally Xu and Gupta

(2009). Smith et al. noted four dimensions with regard to privacy concerns: improper access, unauthorized secondary use, errors, and collection of information. Lee (2009) used the survey to evaluate the acceptance of RFID among Korean companies. Similarly, Xu and Gupta (2009) used a survey instrument for studying privacy concerns among cellular phone users in Singapore. The privacy concerns (MP) in this research to include: persistence of data and existence of security policy was measured using a modified form of the surveys mentioned here. The modifications to the questions changed Lee's 2009 "company" to "hospital." The first measure of privacy – existence of a security policy was based on Lee (2009). Lee's (2009) survey considered the acceptance of RFID among companies in Korea. Lee's survey, based on Shalhoub (2006) asked 3 questions specifically about personal privacy, possibility to leak information, and security policy existence in a company, so these questions were used to validate RQ1, RQ2 and RQ5. Lee's Cronbach's alpha scores on security trust questions scored .80 making them reliable.

Xu and Gupta used a survey developed by Smith et al. (1996) to study privacy concerns over location-based services among 176 cellular telephone users in Singapore. The results related to this collection dimension had a Cronbach's alpha of .832, indicating high reliability. Xu and Gupta's (2009) survey was based on Smith et al. (2006) survey, in which he identified four dimensions of information privacy concerns to include collection (persistence of data in this research), unauthorized secondary use (Cognitive factors of trust in electronic medium, and privacy concerns regarding surveillance and RFID devices in this research), errors and improper access (also the cognitive factor of trust in electronic medium in this research). The MP items are numbered MP1-MP6.



### *Measure of External Control (EC)*

Measures of external control for this survey were adapted from survey items developed and validated by Mohamed, and Ahmad (2012), Cammock et al. (2009), and Dinev and Hart (2004) as well as Woon, Tai and Low (2004). Mohamed and Ahmad (2009) using a tool created by Dinev and Hart (2004) and Woon, Tai and Low (2004) studied external control, defined as “perceived vulnerabilities” in their work among use of social networking sites in Malaysia. I applied this to the EC parameter, because Venkatesh (2000) stated that external control is: “Feeling of control an individual has toward the use of computer based on the availability of knowledge, resources and opportunities required for its use.” Cammock et al. studied the intentions of undergraduate students in Northern Ireland to apply for jobs with the Northern Ireland Civil Service. The questions from the various surveys comprising this section were adjusted to reflect this research by substituting “RFID” as the technology and “in hospitals” as the location. Finally, Mohamed and Ahmad (2012) investigated the privacy concerns in social networking usage in Malaysia. In these instances, the term “social network” was substituted with “RFID.” The EC items are numbered EC1-EC5.

### *Measures of Cognitive Factors*

Pavlou & Chellappa (2001) as cited in Grabner-Krauter & Kaluscha (2003) developed a research model to investigate how perceived privacy and trust affect trust in e-commerce transactions. Lee (2009) also created a survey that asked relevant questions about trust in the electronic medium. In this case, it will be “trust in RFID.” While not exactly that same as the research presented in this study, the regression analysis

techniques used to determine the hypothesized relationships among perceived privacy and perceived security dependent variables and intention to use (deemed consumer's trust in Pavlou, and Chellappa (2001)) was applied to this research (Pavlou, et al., 2001). The CF items are numbered CF1-CF6.

### **Validity and Reliability Assessment**

This research tested the validity and reliability of the survey tool to be used.

According to Tavakol & Dennick (2011), validity is concerned with the extent to which an instrument measures what it is intended to measure. Reliability is the ability of an instrument to measure consistently. An instrument cannot be valid unless it is reliable. Nunally (1978) recommends that instruments used in basic research have reliability of about .70 or better. He adds that increasing reliabilities much beyond .80 is a waste of time with instruments used for basic research. Nunally (1978) continues:

Nunnally (1978, p. 245) notes that increasing reliabilities much beyond .80 is a waste of time with instruments used for basic research. Leedy & Omrod (2005) noted that a survey's reliability and validity affect the amount of information that can be learned from a phenomenon upon which a research experiments. Sekaran (2003) states: "Cronbach's alpha is a reliability coefficient that indicates how well the items in a set are positively correlated to one another. Cronbach's alpha is computed in terms of the average intercorrelations among the items measuring the concept" (p. 307). It is expressed as a number between 0 and 1 (Cronbach, 1951). The following guidelines are used for evaluating Cronbach's alpha coefficients: coefficients of .49 or less are unacceptable, coefficients of .5 to .59 are poor, coefficients of .6 to .69 are questionable, coefficients of

.7 to .79 are acceptable, coefficients of .8 to .89 are good, and coefficients greater than .9 are excellent (George & Mallery, 2003). Internal consistency describes the extent to which all the items in a test measure the same concept or construct, and thus it is connected to the inter-relatedness of the items within the test (Tavakol & Dennick, 2011, p.53). Ellis and Levy (2009) stated that internal consistency concentrates on “level of agreement among the various parts of the instrument or process in assessing the characteristics being measured” (p.334). For this investigation, internal consistency and reliability of each variable was measured using composite reliability. Wong (2013) noted that “Traditionally, ‘Cronbach’s alpha’ is used to measure internal consistency reliability in social science research but it tends to provide a conservative measurement in PLS-SEM. Prior literature has suggested the use of Composite Reliability as a replacement.” Furthermore, Levy (2006) and Howell (2010) note importantly that before the examination of survey results the questionnaire items must be evaluated for directionality, and those with a reversed directionality were reverse scored to guarantee that all the items were scored in the same direction.

Validity is the ability of a researcher to draw valid and significant conclusions about a population, from a data sample collected (Creswell, 2005; Ellis & Levy, 2009). Sekaran (2003) defines the following categories of validity: content, face, criterion-related, concurrent, predictive, construct, convergent and discriminant validity (p.208). This study used: construct validity, factor analysis and hypothesis testing as part of its research methodology.

According to Cronbach, and Meehl (1955) construct validity is an issue of operationalization or measurement between constructs. The concern is that the

instrument items selected for a given construct are, considered together and compared to other latent constructs a reasonable operationalization of the construct (cited in Straub, et al., 2004, p 388). Put another way, construct validity is defined as the extent to which the results of a test are related to an underlying psychological construct (Salkind, 2006, p.116). Straub (1989) noted that construct validity determines whether or not measures used are true constructs describing the event (p.150). External validity focuses on how a given survey tool relates its findings outside of its context. Further, it determines whether or not the results of the test can be generalized enough to be used in other similar studies conducted in other contexts (Leedy and Ormrod, 2005).

Petter, Stacie, Straub and Rai (2007) caution against descriptions of differences between formative and reflective constructs. In this research, the constructs: are reflective, and thus should exhibit multicollinearity. Petter et al. (2007) further note than any model containing both reflective [or multidimensional] constructs and formative constructs is formative in nature (p. 627). This research is based on reflective constructs. This determination was made using Jarvis, MacKenzie and Podsakoff,P.; MacKenzie, Lee, and Podsakoff, N. (2003) four decision rules for determining whether or not a construct is formative or reflective: Theoretical direction of causality between each construct and its measures; Determine whether or not the measures are interchangeable or not (reflective measures are interchangeable); Do the measures covary with one another? With reflective constructs, the measures need to covary with one another; and finally ask whether or not the measures of the construct have the same antecedents and consequences. With reflective measures, it is necessary to have the same antecedents and consequences (Petter et al., 2007, p. 633-634).

Finally, after data collection according to Bollen and Lennox (1991) to assess construct validity it is necessary to validate the formative constructs by eliminating or keeping non-significant items, in the latter to preserve content validity, as cited by Petter et al. (2007, p. 642). Other steps include analysis of construct via Covariance-Based structural equation modeling, or via components-based structural equation modeling.

### **Data Collection**

The survey was made available to each participating US doctor and nurse using Survey Monkey's Audience technology. As noted above, the survey used both a 5-point Likert scale with 1 = strong disagree, 2 = disagree, 3 = neither disagree nor agree, 4 = agree, and 5 = strongly agree, and true/false type questions. The data was analyzed using SmartPLS, Partial Least Squares Structural Equation Modeling (PLS-SEM) software package, which is a robust statistical analysis program.

### **Data Analysis**

The research investigated five independent variables: perception of external control; subjective norm; cognitive factors of privacy concerns, and trust in electronic medium; persistence of data; and existence of security policy and their effect on doctors and nurses behavioral intention to use RFID technology in the workplace. The statistical technique chosen to test the stated hypotheses was partial least squares (PLS) path analysis, otherwise known as partial least squares structural equation modeling (PLS-SEM). PLS is an advanced statistical method that allows optimal empirical assessment of a structural (theoretical) model (Keil, Tan, Saarinen, Tuunanen and Wassenaar, 2000). We used the

framework specified by Chin (1998) and protocols described by Chin (2010) and Wong (2013) for constructing a PLS path model using SmartPLS software, specifically the computation and evaluation of (1) outer model loadings; (2) internal consistency reliability; (3) convergent validity; (4) discriminant validity; (5) inner model path coefficient sizes and significance; and (6) explanation of variance. Chin (2010, p. 656) and Wong (2013, p.5) emphasized that PLS applications “Do not use goodness-of-fit (GoF) Index” and similarly, Hair (2014) concluded that GoF indices are not universally applicable. Chin notes that GoF indices are not prominent in PLS models and that their absence in PLS analyses should not be considered a deficit (2010, p.656). Consequently no goodness of fit indices are provided. A path diagram, defining the hypothesized relationships between the variables, was drawn with the graphic user interface of SmartPLS. The following tests were conducted to validate the model as described by Wong (2013): (a) factorial validity, tested by evaluation of the outer model loading coefficients; (b) internal consistency reliability, tested by the composite reliability coefficient (not Cronbach’s alpha, which is not applicable for PLS-SEM); (c) convergent validity, tested by the average variance explained (AVE); and (d) discriminant validity, tested by the square root of AVE.

SmartPLS computed the path coefficients or standardized regression weights ( $\beta$ ) between the latent variables. Each path coefficient ranged in value from -1 to +1. The researcher conducted bootstrapping to test for the significance of the path coefficients. A path coefficient was declared to be significantly different from zero if  $p < .05$  for the  $t$ -test statistic. The  $R^2$  values computed by SmartPLS were recorded to reflect the effect

sizes in terms of the proportions of the variance explained according to Chin (2010), and Wong (2013).

### *Linear Regression*

Linear regression is the association between an independent variable and a single dependent variable. Using an F test, the researcher was able to determine if the independent variables predicted the dependent variable (Tabachnick & Fidell, 2006).

### *Regression Assumptions*

There are 5 regression assumptions: The predictor variables can be tested as fixed values; The relationship is linear, or approximately linear over the entirety of the sample; The variance is constant (homoscedasticity); The errors are independent; and finally the regression must exhibit a lack of multicollinearity in the predictors. Tabachnik & Fidell (2006) state that homoscedasticity or homogeneity of variance presumes the scores computed will be scattered around the regression line, and normality presumes that the scores are normally distributed, and linearity presumes any relationship between a criterion variable and a predictor variable is a straight line. Scatter plots can visually represent these three factors, and can help determine moderate to high inter-correlations among predictors (Stevens, 2002, p.91). Stevens deems this event “multicollinearity” and that it can be diagnosed by examining a “variance inflation factor” for each predictor variable. A variance inflation factor of 10 or more denotes multicollinearity (2002).

In order to determine the relationships between the independent variables and the dependent variables, multiple linear regression was used. Multiple linear regression analysis examines the relationship between multiple independent variables and a dependent variable. The multiple regression model used in this research will be:

Intention to Use =  $\beta_0 + \beta_{MP} * MP + \beta_{EC} * EC + \beta_{SN} * SN + \beta_{CF} * CF + e$ , where Intention to Use is the dependent variable, MP were the measures of privacy (persistence of data, and existence of security policy), EC is external control, SN is subjective norm and CF is cognitive factors. *F*-test will determine whether the groups of independent variables, taken as a whole, predict the dependent variable, and r-squared tests (coefficient of determination) will calculate the variance of the group of independent variables (Tabachnick & Fidell, 2006). Homoscedasticity, linearity will be evaluated by a perusal of the scatter plots. According to Stevens (2002), “When there are moderate to high intercorrelations among the predictors, as is the case when several cognitive measures are used as predictors, the problem is referred to as multicollinearity” (p.91).

### **Format for Presentation of Results**

The data were presented in figures and tables in the results section of the final dissertation report. The data in the tables and figures drew conclusions regarding the hypotheses presented in this dissertation report.

### **Resources Used**

The researcher created the Likert-scale, survey tool using Survey Monkey’s Audience program. The survey will be distributed by the Survey Monkey website using their proprietary demographic solutions tools, located at <http://www.Survey Monkey.com>. The researcher used the SmartPLS PLS-SEM software suite. The researcher also used SPSS version 22. Since the research will use human subjects, the researcher obtained IRB approval during summer 2014, and included the approval document in the appendix.



The researcher relied upon his advisor and his committee for advice, and guidance as well the resources made available online by the NSU digital library.

### **Summary**

In order to study doctors' and nurses' privacy and security concerns on behavioral intentions to adopt RFID in hospitals, the researcher developed a multi-item survey instrument. The questionnaire was delivered via a Web-based survey and items were answered using a Likert scale. The questionnaire was composed of pre-existing, validated scales from the literature. The questionnaire was distributed to US physicians and registered nurses concerning the privacy and security concerns with the intention to use RFID in their workspaces.

The data analysis technique used was linear regression – to assess the relationship between the independent variables, and multiple regression – to assess the relationships between the five independent variables and the dependent variable. The results of the survey were used to determine whether the theoretical model accurately portrays the effect of the five independent variables on the dependent variables. The results were used to provide guidance to medical staff looking to implement large-scale RFID usage in their hospitals. Also, the outcome of the research could be used to assess how well medical staffs understand security and privacy issues associated with RFID usage, and thus provide areas for further research and or education in those environments.

## **Chapter 4**

### **Results**

This chapter provides the results of statistical analyses of the survey data that was collected to validate the hypotheses of this research. The chapter begins with a presentation of the data collection and analysis including the findings for reliability and validity as well as the results of the multiple regression testing. The chapter concludes with a summary.

#### **Data Collection and Analysis**

##### *Data Collection*

The web-based survey instrument (Appendix A) was created and distributed using SurveyMonkey. Using SurveyMonkey's Audience™ the researcher distributed the survey instrument to US doctors and registered nurses aged 18 and older. The Audience™ tool mailed the surveys on November 30<sup>th</sup> and December 1<sup>st</sup>. All surveys were completed by December 3<sup>rd</sup>, 2014. A total of 115 doctors and nurses completed the survey, and this provided 101 usable surveys, which comprised the data set.

##### *Data Screening*

The researcher screened the data to ensure that conclusions were well founded. Levy (2006) states that the researcher has to identify problems or anomalies in the data, such as incorrectly coded questions, and missing responses. Levy (2006) further states that pre-

analysis screening of the data helps to maintain the accuracy of the collected data. The researcher transferred the data from the web-based questionnaire first to Excel, then to SPSS format, as SurveyMoneky allows these two types of export. The researcher ensured that all the Likert scales were keyed in the same direction, based on the content of the questions (Levy, 2006). The researcher also carefully analyzed the wording of the questions to determine if any items needed reverse coding.

Finally, and most importantly, the data the researcher collected and subsequently used for the perceived usefulness construct was discarded as it had substantial issues with face validity. Sekaran (2003) states that face validity is the extent to which a test is subjectively viewed as covering the concept it purports to measure. The item used to test perceived usefulness did not specifically address perceived usefulness in that the wording of the question was not concise enough, and thus did not yield appropriate responses. The researcher initially chose the question from one of the pre-existing questions in the survey: “People who are important to me think that I should use RFID.” This determination later proved to be in violation of face validity, and the researcher confirmed that this question had been used in prior research as a subjective norm item. As it turned out, it was removed from analysis on subjective norm due to weak a Cronbach’s alpha score during initial testing. Therefore, the perceived usefulness construct had to be removed from the data analyses presented in this chapter.

### *Sample Profile*

The researcher surveyed 115 U.S. registered nurses and doctors aged older than 18 years. The N values for the respondents varied between 76-99, depending on the

question. This was the result of some respondents not completing all questions on the survey. Chin (1998) notes that tradeoffs between measurement models and structural ones can be avoided by having a sample size of at least 10 times the number of independent constructs affecting a dependent construct. In this model, after modifications due to face validity issues, there were 5 independent constructs, indicating a minimum of 50 respondents. Even in the worst case (76) it was a sufficient sample according to Chin's stated criteria regarding sample sizes and the use of PLS-SEM. The levels of education among the respondents varied from 2 years to 8+ years, post secondary school. The survey respondents did not answer any questions regarding the number of years they have used RFID. Figure 6 shows descriptive statistics for the sample.

	N	Range	Minimum	Maximum	Mean	Std. Deviation	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Gender	99	1	0	1	.75	.437	.191	-1.157	.243	-.676	.481
Age	97	41	24	65	52.02	11.831	139.979	-.559	.245	-.566	.485
Household Income	79	132	18	150	105.85	38.864	1510.387	-.458	.271	-.962	.535
Educaton	98	9	11	20	17.10	2.797	7.825	-.263	.244	-1.246	.483
Valid N (listwise)	76										

Gender 0-female, 1-male; Age (absolute); household income in thousands of dollars per year; education 11- less than high school, 12 high school, 14- associates, 16- bachelors, 18- masters, 20 terminal degree.

*Figure 6.* Descriptive statistics of the demographic data. The researcher used SPSS , version 22 to generate this image.

The distribution of demographic statistics shows negatively skewed data, and a platykurtic distribution. The mean of the Kurtosis values is less than 3 and the mean of

the skewedness of the values is less than 0, making this slightly left-skewed population, with a platykurtic shaped curve, or one that is flatter than normal with a wider peak.

## **Measurement Model Analyses**

### *Test for Normality*

PLS-SEM makes no assumptions about the data distribution (Vinzi, Trinchera and Amato, 2010). Thus PLS-SEM is a good alternative to parametric tests, such as the Shapiro-Wilk test for normality when the sample size is small, and the predictive accuracy of the model is paramount. According to Wong (2013), PLS-SEM is very useful for structural equation modeling when there are limited participants, and when the data distribution is skewed.

The researcher ran the Shapiro-Wilk test for normality on the constructs and it indicated just about 0.000, or significant values for all items. This would indicate that the constructs did not receive equally distributed responses. The skew values and kurtosis values (Figure 7) corroborate this. The frequency distributions of the scores for the latent variables are illustrated in Figure 2. The frequency distributions did not approximate bell-shaped curves, reflecting deviations from normality. The descriptive statistics (mean, standard deviation, skewness) for the constructs are presented in Figure 7. All the variables were negatively skewed and deviated from normality ( $p < .05$ ).

Construct	N	Mean	Std. Dev	Skewness	Kurtosis
SN	98	2.598	0.831	-0.028	0.056
SP	95	3	0.963	-0.244	-0.57
DP	95	3.22	0.834	-0.49	0.786
CF	91	2.69	0.899	-0.079	0.003
EC	93	2.66	0.852	-0.003	0.011
IU	32	0.75	0.43994	-1.212	-0.57

CF – Cognitive Factors; DP – Data Persistence; EC – External Control; IU – Intention to Use; SP – Security Policy; SN – Subjective Norm

*Figure 7.* Descriptive statistics of the constructs

The frequency distributions for the latent variables are illustrated in Figure 7. The mean of the skewness values show that the data is slightly left skewed (-0.2785), meaning most values are concentrated on the right of the mean, with extreme values to the left. The mean of the Kurtosis values (0.056) is less than 3, making this a platykurtic distribution, which is flatter than a normal distribution with a wider peak. The probability for extreme values is less than for a normal distribution, and the values are spread wider around the mean.

### **Common Method / Common Variance Test**

According to Podsakov (2003) common-method variance (CMV) is the spurious variance that is attributable to the measurement method rather than to the constructs the measures are assumed to represent. For example, an electronic survey method might influence results for those who might be unfamiliar with an electronic survey interface differently than for those who might be familiar. If CMV affects the measures, the inter-correlations among them can be inflated or deflated depending upon several factors (Richards & Brown, 1994). Richardson, et al. (2009) note that when the results of this test show that one factor explains much less than 50% of the total variance, the method is

sound and well represents the constructs presented in the model. The researcher ran this common method / common variance test in SPSS and determined that one factor only explained 29% of the total variance, thus the method is sound and well represents the constructs presented in the model.

**Total Variance Explained**

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6.114	29.114	29.114	6.114	29.114	29.114
2	3.094	14.734	43.848			
3	2.151	10.241	54.089			
4	1.598	7.612	61.701			
5	1.503	7.159	68.860			
6	.985	4.692	73.551			
7	.870	4.145	77.696			
8	.771	3.670	81.366			
9	.601	2.861	84.227			
10	.535	2.549	86.776			
11	.515	2.454	89.230			
12	.443	2.111	91.341			
13	.389	1.854	93.195			
14	.319	1.517	94.712			
15	.276	1.316	96.028			
16	.208	.989	97.017			
17	.191	.909	97.925			
18	.172	.817	98.742			
19	.120	.571	99.313			
20	.088	.421	99.734			
21	.056	.266	100.000			

Extraction Method: Principal Component Analysis.

*Figure 8.* Common Variance Test. The value of one factor is much less than 50% of the total variance, therefore the method is sound and well represents the constructs presented in the model.

## Latent Variable Definitions

The latent variables, the indicators, and the measurement scales used to construct the PLS path model are defined in figure 9. After the researcher began initial reliability testing, the following items were removed from their respective latent variables: CF1, CF2R, CF3, CF4R, CF6R, DP1, EC1, EC5, SN1, due to their low alpha scores. In the analyses that follow these items were not included as Nunally (1978) states that is better to save time and money by using a model that has at least moderate reliability scores. Bollen and Lennox (1991) state that although reliability estimates (e.g.: Cronbach's alpha) of the set of indicators will be lower if fewer indicators are included in the measurement model, the construct validity will be unchanged when single indicators are removed from reflective models, because the remaining indicators should adequately represent all facets of the construct.

Latent Variable	Number of Indicators	Indicators	Measurement Scale
INTENTION TO USE	1	SN2 (People who influence my behavior think I should use RFID)	1 = Strongly Disagree to 5 = Strongly Agree
EXTERNAL CONTROL	5	EC1, EC2, EC3, EC4, EC5	1 = Strongly Disagree to 5 = Strongly Agree
SUBJECTIVE NORM	2	SN1, SN3	1 = Strongly Disagree to 5 = Strongly Agree
SECURITY POLICY	3	MP1, MP2, MP3	1 = Strongly Disagree to 5 = Strongly Agree
DATA PERSISTENCE	3	MP4, MP5, MP6	1 = Strongly Disagree to 5 = Strongly Agree
COGNITIVE FACTORS	6	CF1, CF2R, CF3, CF4R, CF5, CF6R	1 = Strongly Disagree to 5 = Strongly Agree

Note: Indicators suffixed with R (CF2R, CF4R, and CF6R) were reverse coded.

Figure 9. Definitions of Latent Variables



## Evaluation of Outer Model Loadings

Figure 10 presents both the composite reliability for and Cronbach's alpha values for the items. Figure 6 presents the outer model factor loadings for each item used in the analysis.

### *Reliability*

The researcher obtained high composite reliability scores for the survey items, and due to the reflective design of the model, the researcher could remove items that produced scores less than .7 on composite reliability tests, and less than .6 on Cronbach's alpha tests. As noted before, the following items were removed from the analyses that follow, due to their low alpha scores: CF1, CF2R, CF3, CF4R, CF6R, DP1, EC1, EC5, SN1. Alpha scores less than .7 on composite reliability tests and less than .6 on Cronbach's alpha tests indicate low reliability and Nunally (1978) notes that it is best to work with instruments that have at least modest reliability of .7 or greater. With reflective models, it is possible to remove items, and removing items produced overall higher reliability values for each construct. The researcher also crosschecked the alpha values using SmartPLS and SPSS and found no significant differences. Figure 10 presents the composite reliability coefficients and Cronbach's alpha values for the latent variables with multiple indicators. Composite reliability does not assume tau equivalency among the measures with its assumption that all indicators are equally weighted (Chin, 2010, p. 671). The composite reliability of the constructs with multiple items was good (>.8) for DP and EC, and excellent (>.9) for SN and SP.

Construct	CR	<u>Cronbach's</u>	AVE
<b>CF</b>	1	1	1
<b>DP</b>	0.855	0.664	0.746
<b>EC</b>	0.865	0.795	0.617
<b>IU</b>	1	1	1
<b>SN</b>	0.919	0.907	0.851
<b>SP</b>	0.942	0.909	0.844

**CR: Composite Reliability**

*Figure 10.* Correlations among the constructs

Figure 11 presents a copy the outer model path loadings. All of the outer model path loadings were strong ( $\geq .7$ ). Again, the table below shows which items were kept in each construct to obtain the best factor loadings. The high proportion of strong factor loadings provided evidence to support the factorial validity of the model. The lack of cross-loadings of factors also corroborates the factorial validity of the items.

	CF	DP	EC	IU	SN	SP
CF5	1					
DP2		0.894				
DP3		0.832				
EC2			0.825			
EC3			0.758			
EC4			0.812			
IU1_R				1		
SN2					1	
SN3					0.838	
SP1						0.928
SP2						0.938
SP3						0.889

*Figure 11.* Outer model path loadings

## Internal Consistency Reliability

### *Convergent and Discriminant Validity*

Figure 12 presents the evidence for convergent validity indicated by the average variance explained (AVE) in the latent variables with multiple indicators. According to Fornell and Larcker (1981) convergent validity was strong with good AVE values (>.5) for all constructs tested, indicating convergent validity, or that the items are all correlated within the constructs.

Latent Variable	Convergent AVE	Discriminant $\sqrt{AVE}$
CF	1	1
DP	0.746	0.864
EC	0.617	0.785
IU	1	1
SN	0.851	0.922
SP	0.844	0.919

*Figure 12.* Convergent and discriminant validity of latent variables

The square root of AVE for each latent variable was computed to test for discriminant validity. The research confirmed discriminant validity because the square roots of AVE were larger than the corresponding inner model path coefficients (beta-values) associated with the latent variables as shown in Figure 15. The research conducted this analysis again with the pared down set of items described in the section on latent variables.

	CF	DP	EC	IU	SN	SP
CF5	1	0.297	0.091	-0.429	0.283	-0.006
DP2	0.279	0.894	0.072	-0.223	0.327	0.09
DP3	0.23	0.832	0.139	-0.18	0.322	0.304
EC2	0.178	0.213	0.825	0.211	0.274	0.432
EC3	-0.028	-0.087	0.758	0.169	-0.124	0.182
EC4	0.03	0.141	0.812	0.117	0.2	0.268
IU1_R	-0.429	-0.236	0.218	1	-0.245	0.167
SN2	0.285	0.378	0.148	-0.25	1	0.359
SN3	0.162	0.196	0.286	-0.006	0.838	0.402
SP1	-0.005	0.154	0.332	0.174	0.348	0.928
SP2	0.027	0.204	0.341	0.162	0.306	0.938
SP3	-0.054	0.255	0.415	0.111	0.35	0.889

Figure 13. Cross-loadings

Using the conditional formatting function on data derived from SmartPLS analysis, the researcher highlighted values greater than .5. As shown above there are no cross-loaded variables, thereby establishing discriminant validity once again.

	CF	DP	EC	IU	SN	SP
CF						
DP	0.361					
EC	0.134	0.31				
IU	0.429	0.286	0.22			
SN	0.245	0.388	0.421	0.14		
SP	0.033	0.304	0.589	0.17	0.441	

Figure 14. Heterotrait Monotrait Ratio Criterion

In order to present further evidence for discriminant validity, the researcher conducted the heterotrait-monotrait criterion test, using SmartPLS. Figure 14 shows all values, which according to Henseler, Ringle and Sarstedt (2015) prove discriminant validity using the Heterotrait Monotrait criterion. Henseler, et al. stated that a conservative estimate of the proof of discriminant validity is to have no values higher than 0.85.

Furthermore, they note that values further from 1.0 are preferable. Both the values lower than 0.85 and their relative distance from 1.0 further prove discriminant validity.

### **Structural Model Analyses**

This section explains the analysis of the hypotheses presented in chapter 3, and it is based on a modified version of the theoretical model presented in chapter 2. The theoretical model in chapter 2 had a dependent variable for perceived usefulness, which was removed to face validity issues. Those issues are further explained in chapter 5. The researcher used structural equation modeling with SmartPLS software to complete this analysis. Fornell and Bookstein (1982) note that SmartPLS is a good choice when the analysis is not contingent on multivariate normal distributions. They also stated that SmartPLS is appropriate for testing theories in the early stages of development.

#### *Inner Model Path Coefficients and Significance*

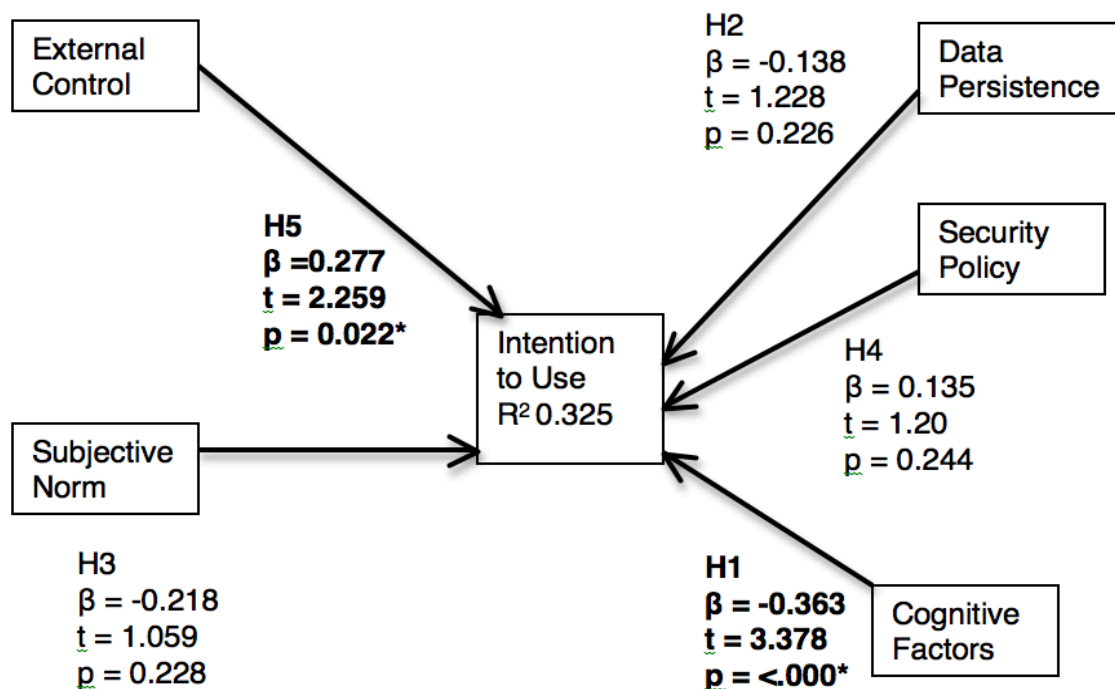
The inner model path coefficients or standardized PLS regression weights ( $\beta$ ) are presented in Figure 10. The t-test statistics indicating the significance of the path coefficients are also presented in Figure 9. The results of the significance tests with p-values are summarized in Figure 9, as well.

	$\beta$	$t$	$p$
CF → IU	-0.363	3.377	0
DP → IU	-0.138	1.228	0.226
EC → IU	0.277	2.259	0.022
SN → IU	-0.218	1.059	0.228
SP → IU	0.135	1.2	0.244

Figure 15. Significance of the path coefficients indicated by t-test statistics

*Explanation of Variance and Significance*

Chin (2010) and Hair, Ringle and Sarstedt (2014) suggested that the primary criterion for the assessment of a PLS path model is the coefficient of determination ( $R^2$ ), which represents the amount of explained variance in each endogenous latent variable. The  $R^2$  values take into account the fit of each regression equation in the inner model. Only about 1/3 of the variance in Intention to Use (32.5%) was explained by the dependent variables shown below in Figure 16.



\* Significant ( $p \leq .05$ ), Hypotheses in bold were supported.

Figure 16. Summary of important measures on structural model

The PLS path model provided the statistical evidence at the .05 level to indicate significant positive correlations between (a) perception of external control and intention to use; (b) cognitive factors and intention to use. The beta-value for CF->IU is negative indicating that for every 1-unit decrease in the independent variable, the dependent variable will increase by the beta coefficient value. The proportion of the variance explained in Intention to Use was  $R^2 = 32.5\%$ . Table one below shows the summary of the results for this research.

At first glance, the  $R^2$  value may seem low, however given this is the first experiment of this specific type, it is not known whether this value possesses better explanatory models than other similar ones. Of greatest concern is the lack of evidence supporting a significant relationship between intention to use and perceived usefulness.

Table 2

*Summary of Results*

	$\beta$	$t$	$p$	Hypothesis supported?
CF -> IU	-0.363	3.377	0	Yes
DP -> IU	-0.138	1.228	0.226	No
EC -> IU	0.277	2.259	0.022	Yes
SN -> IU	-0.218	1.059	0.228	No
SP -> IU	0.135	1.2	0.244	No

The summary of results in Table 2 above shows the regression coefficients, the  $t$ -values, and their significance, as well as whether or not the predicted hypotheses were supported by the research. The data collected supported only two of the proposed hypotheses, one of which (CF) that had not been tested in this way prior to this research. The researcher was unable to conclude why more of the hypotheses were not supported

by the data, but has made some potentially significant suggestions in chapter 5 regarding this.



## **Chapter 5**

### **Conclusions, Implications, Recommendations and Summary**

#### **Conclusions**

The study examined whether doctors or nurses in US hospitals had privacy or security concerns when using RFID, or when dealing with technology that contains RFID chips. The primary goal of this study was to examine relationships between measures of privacy, and security trust in the context of intention to use. To accomplish this, the study proposed a theoretical model that considered relationships between the independent variables of perception of external control and subjective norm, persistence of data, existence of security policy, subjective norm and cognitive factors on the dependent variable intention to use. The researcher developed a multi-item questionnaire, and utilized pre-existing Likert and binary scales. The researcher electronically distributed the surveys using a web-based survey provider. The survey was distributed to 100 U.S. doctors and registered nurses, and there were 96 valid responses out of 100 total respondents, yielding a response rate of 96%. Finally, the researcher conducted a common method variance test on the data set to show there was no bias in this survey, based on its electronic distribution approach.

The researcher conducted additional statistical analysis using the linear regression in the parametric testing tool, SPSS to further investigate relationships between demographic independent variables of Gender, Age, Household Income and Education.

The researcher did not discover any significant relationships between these variables and Intention to Use.

*Regression results excluding cases list-wise for missing values (SPSS)*

Coefficients <sup>a</sup>						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.286	.399		-.717	.475
	Gender	.162	.112	.145	1.441	.152
	Age	.008	.004	.184	1.925	.057
	Household Income	.001	.001	.070	.717	.475
	Educaton	-.003	.018	-.019	-.190	.850

a. Dependent Variable: AU1

*Figure 17.* Regression results excluding cases list-wise for missing values copied from SPSS.

The researcher experimented further with other structural models in SmartPLS, adding in the construct of “actual use”, for which the researcher had already collected data. Some of the results were very interesting (see Figure 18).

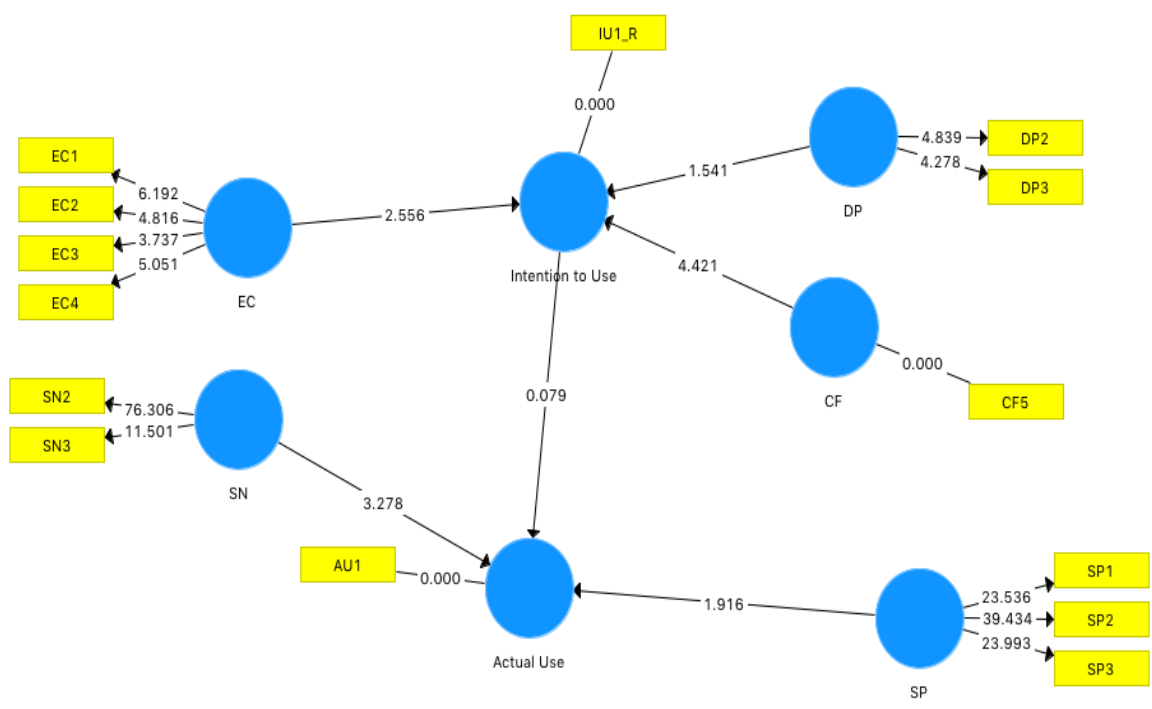


Figure 18. Further testing with dependent and independent variables (Copy of SmartPLS output).

The SmartPLS diagram above shows significant relationships (t-values greater than 1.96) between EC, CF and Intention to Use as well as weakly strong significance between DP and Intention to Use. It also shows a significant relationship between SN and Actual Use, and a weakly significant relationship between SP and Actual Use. More experimenting should be done to further explicate why this model produces stronger relationships than the proposed model.

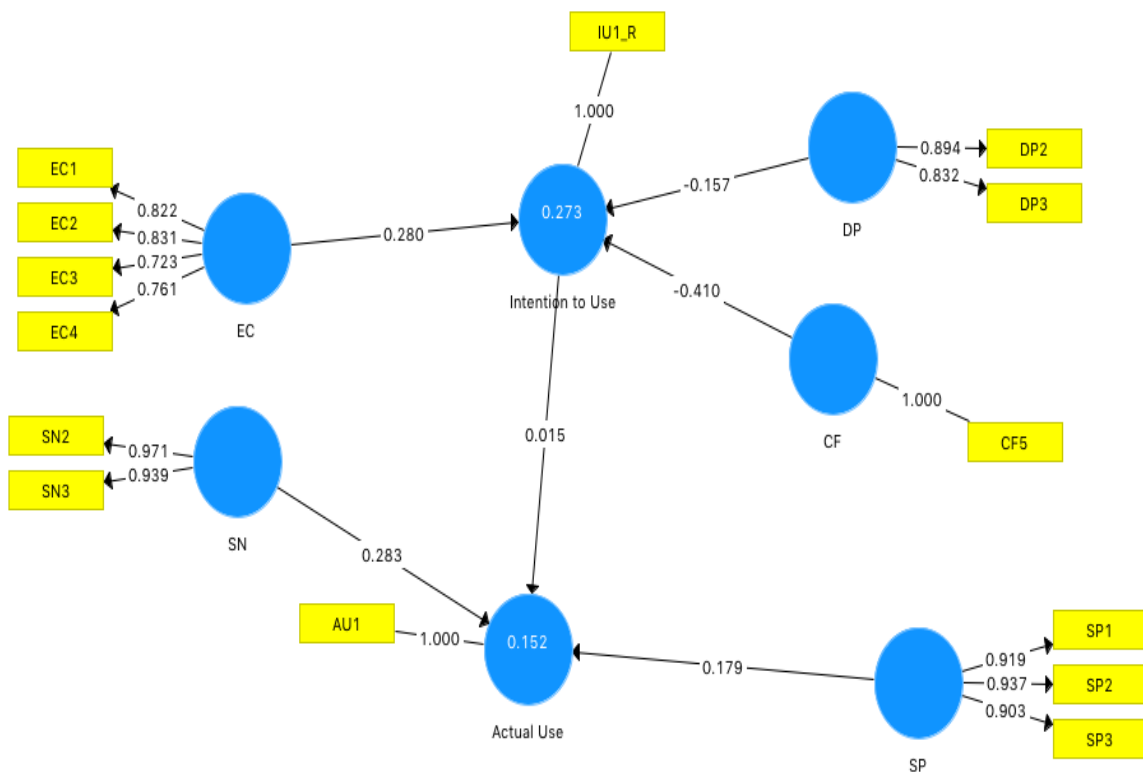


Figure 19. Inner path coefficients with further testing (Copy of SmartPLS output)

The findings shown in Figure 19 above are interesting in that the results better match the predictions presented in the theoretical model (chapter 1), and that there were many more significant relationships between the IVs and the DVs. As predicted in the theoretical model, the relationship between CF, EC, and DP did not change from the predicted values (CF is negative relationship, EC and DP are positive relationships). SN in the actual tested model did not bear out its relationship as it was predicted to be a positive relationship, and in the actual results it was negative. Also of note is that in this

model SP and to a lesser extent DP have significant relationships with their dependent variables.

The researcher recognizes that the lack of significant relationship between IU and AU is counter-intuitive to what is shown in the literature. While it is not immediately apparent, the researcher will investigate this further to see what the reasons might be. One of the previously untested variables - cognitive factors of privacy concerns regarding surveillance and trust in the electronic medium supported its hypothesis with a t-value 3.378. Data persistence and the existence of security policies did not support their hypotheses. The existence of security policy (SP) and data persistence (DP) did not support their hypotheses with t-values of 1.20, and 1.228, respectively. The t-test values in these three cases were less than 1.96, failing to reject their null hypotheses. A failure to reject the null hypothesis means that the null hypothesis is possible. This finding is not supported by the literature. A Further developments to the survey tool regarding trust issues, and RFID usage education could provide a better understanding of how these three variables influence intention to use.

A limitation of this research was the face validity issue with the survey question used to test perceived usefulness. Another limitation of this research was with the wording of the question used to test Intention to Use: If RFID is implemented at your facility would you want to a way to bypass or avoid using it at your facility? A positive response to this (yes) would mean you would not want to use this technology, it also means we would not intend to use this technology. The semantic difference between want to use and "use" is very small. And unfortunately, the way the question is worded "would you want a way to bypass" -- this is more "intention to use" (the act of bypassing equates to

avoiding, but it is slightly different b/c others may be using it and not bypassing it, and if they were thinking about the actual usage, they would make a judgment (based on behavioral traits) about whether or not they "wanted to use it all", which is how I derived this as "intention to use." The wording: "would you avoid using it" - this is more "actual use" - The researcher notes that technology evasion is different from avoidance. So evading the technology is a behavioral choice, whereas avoiding it altogether is strictly speaking "whether or not you use".

The first research question was: How does the existence of a data security policy (under the rubric of "Privacy Risk Variables" in the theoretical model) affect the intention to use RFID in US hospitals? The findings of the PLS analysis demonstrated that the measures of privacy: data persistence and security policy were not significant factors affecting intention to use RFID in US hospitals. These factors had not been previously applied in the context of RFID usage among doctors and nurses. These results validated the research of Hossain and Prybutok(2008), who also found measures of privacy were not a significant factor affecting consumer acceptance of RFID, and of Xu and Gupta (2009) who determined that users of a cellular telephone auto-location service were not deterred from using the technology due to privacy concerns. Finally, using the approach adopted by Anderson and Agarwal (2011) where they included specific moderating variables in their theoretical model may have also improved my significance testing, due to the fact that their moderating variables further parsed risk scenarios between the cognitive factors of electronic health information privacy and trust in the electronic medium.

The second research question under the rubric in the model of “Privacy Risk Variables” in the theoretical model was: How does persistence of data or data retention affect the intention to use RFID in US hospitals? The findings in this investigation supported those of Xu and Gupta (2009) who determined that users of a cellular telephone auto-location service were not deterred from using it due to extant privacy concerns. The findings in this research did not support Fisher and Monhan (2008) who determined that privacy had a significant impact on nurses’ acceptance of RFID technology, however the correlation between that research and the this investigation is not particularly strong due to the differing cross-sectional samples used.

The third research question was: How does subjective norm affect the intention to use RFID in US hospitals? The subjective norm construct results supported research conducted by Ajzen (1985, 1988, 1991) that determined subjective norm to be a significant construct affecting behavioral intention. The PLS analysis did not show

The fourth research question was: How does perception of external control affect intention to use RFID in US hospitals? The findings in this research showed a significant positive correlation between perception of external control and intention to use.

The fifth research question was: How do the cognitive factors of privacy concerns regarding surveillance and RFID devices as well as trust in the electronic medium affect intention to use RFID in US hospitals? The findings in this research did not show a significant positive correlation between the cognitive factors of privacy concerns regarding surveillance as well as trust in the electronic medium and intention to use. The results of this research showed significant positive correlations between these cognitive factors and intention to use.

The sixth research question was: What is the strength of the contribution of the five variables (i.e., persistence of data, cognitive factors, existence of data security policy, subjective norm, and perception of external control) in predicting behavioral intention to use RFID in US hospitals. The SmartPLS analysis showed external control, the cognitive factors to be strong predictors on intention to use behaviors. The SmartPLS analysis did not prove that data persistence, security policy, or subjective norm were strong predictors on intention to use.

### **Implications**

This research attempted to better correlate security and privacy factors as well as cognitive factors with perceived usefulness, and intention to use. The cognitive factors of privacy concerns regarding surveillance and trust in the electronic medium, as well as the existence of security policies, were found not to be significant predictors of the intention to use RFID. The t-test values in these three cases were less than 1.96, failing to reject their null hypotheses. " A failure to reject the null hypothesis means that the null hypothesis is possible. When  $H_0$  is true, it is likely that we will fail to reject it. When  $H_0$  is false, we may also fail to reject  $H_0$  due to low statistical power. In both cases, our conclusion is to fail to reject the null hypothesis (a null result). When we fail to reject the null hypothesis, it does not transmit any meaningful information about the viability of the null hypothesis, primarily because of the high probability of making a Type II error (Aberson, 2002, p.38).



## **Recommendations**

This research can pave the way for perhaps more exploratory research, with larger population samples and more better defined questions regarding security and privacy issues. Perhaps a better place to start would be with the structural models presented in Figures 3 and 4.

The theoretical model used in this research could be refined for further research (see Figure 3), to better reflect the measures of privacy elements: data persistence and security policy could be combined into one category “measures of privacy”, and tested with questions that focused more specifically on data breaches and data loss. The theoretical model shown here was tested several months before the Blue Cross Anthem data breach, and this alone could change outcomes to results regarding the theoretical model. A study that runs the same survey tool could in this case yield more strong correlations between security and privacy issues, and intention to use. Developing further lines of questioning that focus on personal data loss, as opposed to general data loss may elicit responses that better support H4 and H6. It is even possible given the greater media attention to data loss and data theft (hacking), that H3 would have been better supported by respondents. Finally, a larger population of respondents may provide better statistical power and thus increase the likelihood of rejecting the null hypothesis.

## **Summary**

This study focused on the behavioral intentions of U.S. doctors and registered nurses to use RFID in hospitals. To conduct this investigation, the researcher developed a theoretical model based on TAM Davis (1989), ETPB (Ajzen, 2002), and Anderson and

Agarwal (2011). Unlike Anderson and Agarwal however the researcher did not use influence variables in this investigation, and instead focused on the interactions between five independent variables and initially three dependent variables. The dependent variable perceived usefulness, had face validity issues, and was therefore discarded in the analysis section. The final results were based on five independent variables and two independent variables.

After conducting a review of the literature concerning RFID usage and acceptance, as well as TAM (Davis, 1989), ETPB (Ajzen, 2002), and the theoretical model presented by Anderson and Agarwal (2011), the researcher developed a theoretical model to calculate the effects of the independent variables external control, subjective norm subjective norm, data persistence, security policy and cognitive factors on the dependent variable intention to use. The goal of this study was to create a model as shown in Figure 4, based on the analysis of the effect of external control, subjective norm, data persistence, security policy and cognitive factors on intention to use RFID. The main research question considered the effects of these variables on perceived usefulness, and doctors and nurses intention to use RFID in US hospital setting. The investigation addressed these specific questions:

RQ1: How does the existence of a data security policy affect the intention to use RFID in US hospitals? (Grabner-Krauter & Kaluscha, 2003; Hernandez-Ortega, 2011; Lee, 2009; Schneider, 2000).

RQ2: How does persistence of data or data retention affect the intention to use RFID in US hospitals? (Juels, 2006; Kamra, et al., 2006; Konomi, 2004; Palen & Dourish, 2003)

RQ3: How does subjective norm affect the intention use RFID in US hospitals?(Chen, et al., 2007; Commock et al., 2009; Davis, 1989; Mather, et al. 2000).

RQ4: How does perception of external control affect the perceived usefulness of RFID in US hospitals? (Ajzen, 1985; Carr, et al., 2010; Hosaka, 2004; Lee, et al., 2009; Venkatesh, 2000; Xu, et al., 2009).

RQ5: How do the cognitive factors of privacy concerns regarding surveillance and RFID devices as well as trust in the electronic medium affect intention to use RFID in US hospitals? (Beresford, 2003; Chanen, 2008; Hong, et al., 2004; Malhotra, et al., 2004; Myles et al., 2003; Röcker, 2010; Xu, et al., 2009).

RQ6: What is the relative strength of the contribution of the five variables (i.e., persistence of data, cognitive factors, existence of data security policy, subjective norm, and perception of external control) in predicting behavioral intention of doctors and nurses to use RFID in US hospitals?

The researcher chose U.S. doctors and registered nurses for the focus of this research. For the investigation, the researcher developed a 20 item Web-based survey, based on existing validated scales that used Likert-scaled items as well as binary measures. SN1, and SN2 were adapted from survey items developed by Taylor and Todd (1995). EC1 to EC5 were adapted from items developed by Cammock et al. (2009). The measures of privacy were divided into two sections: SP1 to SP3 referred to security policy, and DP4 to DP6 referred to data persistence, and were based on survey items developed and validated by prior research from Grabner-Krauter et al. (2003); Hernandez-Ortega (2011); Lee (2009); Schneider (2000); and Yousafzai, et al. (2003). CF1 to CF6 were adapted from survey items developed and validated by Beresford et al. (2003); Chanen

(2008); Hossain and Prybutok (2008); Pavlou (2003), and Xu et al. (2009). There were three items designed for this research, which elicited responses for the dependent variables perceived usefulness (PU1), intention to use (IU1).

The research model presented in this investigation predicted that there would be positive relationship between external control, subjective norm and the dependent variable perceived usefulness. The values for the dependent variable perceived usefulness were not included, due to face validity issues outlined in chapter 4. The model also predicted positive relationships between the independent variables subjective norm and intention to use, as well as existence of a security policy on the dependent variable intention to use. It predicted negative relationships of the independent variables cognitive factors of privacy and trust in the electronic medium, and persistence of data on the dependent variable intention to use. The researcher used SmartPLS to provide statistical analysis of the survey items and the proposed hypotheses. The survey was distributed to 100 doctors and nurses in the U.S. and 96 responded, providing a response rate of 96%. The researcher used SurveyMonkey's audience tool to demographically select the cross-sectional study.

The PLS path model provided the statistical evidence at the .05 level to indicate significant positive correlations between (a) cognitive factors; (b) external control and intention to use. As a positive predictor of Intention to Use, Cognitive Factors ( $\beta = -0.363$ ) was more important than External Control ( $\beta = -0.277$ ). The beta-values for CF->IU and EC->IU are negative indicating that for every 1-unit decrease in the independent variable, the dependent variable will increase by the beta coefficient value. The proportion of the variance explained in Intention to Use was 32.5% ( $R^2 = 32.5\%$ ) and

in academic fields that attempt to predict human behavior R-squared values are typically lower than 50%.

The results showed significant relationships between External Control and Intention to Use as well as between Cognitive Factors and Intention to Use. The beta-values for these relationships were negative, indicating negative relationships between the variables. In practical terms for this research, this means that the more a person knows about surveillance capabilities and issues of trust in the electronic medium (cognitive factors) the less likely the person intends to use the technology. The research findings are consistent with the prediction presented in H1: The cognitive factors of privacy concerns regarding surveillance and trust in the electronic medium, have a negative relationship with intention to use. The same relationship exists between the perception of external control and intention to use, as presented in H5. The prediction shows that there should have been a positive relationship, in practical terms meaning: If there is a higher perception of external control, then a person will be more likely to intend to use the technology. The findings in the research showed were consistent with the prediction: the higher the perception of external control, the more likely a person will be to use the technology, based on the negative correlation coefficient between the values. The research showed that both of these relationships EC, CF -> IU were significant. The theoretical model predictions and the actual results are presented below in Table 1.

In chapter 5, the researcher concluded the study by experimenting further with the relationships between independent and dependent variables. The researcher discovered that there was a permutation of variables that produced the most significant relationships, and that those relationships would need further investigation. The relationships were:

EC-> IU,; DP-> IU; CF-> IU; SN->AU; and SP->AU, and IU->AU. Using SmartPLS the researcher found significant relationships between all except IU->AU, and DP->IU. The researcher noted that this is still unusual because the literature shows many examples of significant relationships between IU->AU.

The researcher presented the implications of this study, indicating that the theoretical model provided can be tested in future research. Additionally, the researcher's model re-validated longer standing hypotheses as described in H1, H2, and H5. The investigation's limits were number of respondents and potential for respondents to bias answers to survey questions, and overall goal of the study. Finally, the researcher provided suggestions for future research that could broaden the knowledge of the relationships between security/trust issues, and intention to use.

## Appendix A. Survey Invitation

Dear U.S. Doctor or Registered Nurse:

You are invited to participate in a survey concerning radio frequency identification technology (RFID). According to PC World magazine, RFID is defined as follows:

**(Radio Frequency Identification)** A data collection technology that uses electronic tags for storing data. The tag, also known as an "electronic label," "transponder" or "code plate," is made up of an RFID chip attached to an antenna. Transmitting in the kilohertz, megahertz and gigahertz ranges, tags may be battery-powered or derive their power from the RF waves coming from the reader. (PC World, 2010)

The US Food and Drug Administration in 2013 expanded upon this definition:

Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. Tags, which use radio waves to communicate their identity and other information to nearby readers, can be passive or active. Passive RFID tags are powered by the reader and do not have a battery. Batteries power active RFID tags. RFID tags can store a range of information from one serial number to several pages of data. Readers can be mobile so that they can be carried by hand, or they can be mounted on a post or overhead. Reader systems can also be built into the architecture of a cabinet, room, or building. Some uses include:

- Inventory control
- Equipment tracking
- Out-of-bed detection and fall detection
- Personnel tracking
- Ensuring that patients receive the correct medications and medical devices
- Preventing the distribution of counterfeit drugs and medical devices
- Monitoring patients
- Providing data for electronic medical records systems (US Food and Drug Administration, 2013 from <http://www.fda.gov/Radiation-EmittingProducts/RadiationSafety/ElectromagneticCompatibilityEMC/ucm116647.htm><http://www.fda.gov/Radiation-EmittingProducts/RadiationSafety/ElectromagneticCompatibilityEMC/ucm116647.htm>)

The purpose of this survey is to measure responses regarding security and privacy concerns in the context of RFID usage in a healthcare setting.

The survey should take approximately 10 minutes, and all responses will be kept confidential. The survey questions will ask for perceptions, thus there are no incorrect responses. Your participation in this survey is important, and very much appreciated. Thank you for your support!

Completing the survey indicates your voluntary participation in the study.

Sincerely,

Thomas G. Winston

Nova Southeastern University Doctoral Student

Graduate School of Computer & Information Sciences

[thomwins@nova.edu](mailto:thomwins@nova.edu)

References:

PC Magazine. (2014). *Definition of RFID*. Retrieved from <http://www.pcmag.com/encyclopedia/term/50512/rfid>

US Food and Drug Administration. (2013). *Radio Frequency Identification (RFID)*. Retrieved from <http://www.fda.gov/Radiation-EmittingProducts/RadiationSafety/ElectromagneticCompatibilityEMC/ucm116647.htm>



## Appendix B. Survey

---

The following questions will determine your eligibility to participate in this survey:

---

1. Does your facility currently use RFID? YES / NO

2. If RFID is implemented at your facility would you want to a way to bypass or avoid using it at your facility?

YES / NO

3. Does your facility mandate RFID usage in devices or in wearable devices on doctors and nurses?

YES / NO

---

The following is a list of statements related to your security and privacy concerns regarding RFID usage in your workplace at a hospital or clinic. Please read each item and rate the level of likelihood you attribute to each statement from: (1) Strongly Disagree to (5) Strongly Agree.

---

	Items	Strongly Disagree	Disagree	Neither Disagree nor Agree	Agree	Strongly Agree
SN1:	People who are important to me think that I should use RFID	1	2	3	4	5
SN2:	People who influence my behavior think I should use RFID	1	2	3	4	5
SN3:	People	1	2	3	4	5

	whose opinions I value prefer that I use RFID					
--	---	--	--	--	--	--

The following is a list of statements related to your security and privacy concerns regarding RFID usage in your workplace at a hospital or clinic. Please read each item and rate the level of likelihood you attribute to each statement from: (1) Strongly Disagree to (5) Strongly Agree.

	Items	Strong Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
MP1:	I trust that the hospital will safeguard information stored on RFID devices.	1	2	3	4	5
MP2:	I trust the security policy of the hospital.	1	2	3	4	5
MP3:	I trust that the hospital will not store and leak RFID information collected on me.	1	2	3	4	5
MP4:	Losing personal information through RFID devices would be a serious problem for me.	1	2	3	4	5

MP5:	My hospital may store private information on RFID	1	2	3	4	5
MP6:	The hospital keeps private RFID information related to me in a database.					

The following is a list of statements related to your security and privacy concerns regarding RFID usage in your workplace at a hospital or clinic. Please read each item and rate the level of likelihood you attribute to each statement from: (1) Strongly Disagree to (5) Strongly Agree.

	Item	Strongly Disagree	Disagree	Neither Disagree nor Agree	Agree	Strongly Agree
EC1:	I believe I have the ability to protect my personal information on RFID devices.	1	2	3	4	5
EC2:	It is easy for me to enable security and privacy measures on RFID devices.	1	2	3	4	5
EC3:	Whether or not I use RFID is entirely up to me.	1	2	3	4	5
EC4:	I feel that I have complete control over using RFID.	1	2	3	4	5
EC5:	I feel that I have no control over using RFID	1	2	3	4	5

The following is a list of statements related to your security and privacy concerns regarding RFID usage in your workplace at a hospital or clinic. Please read each item and rate the level of likelihood you attribute to each statement from: (1) Strongly Disagree to (5) Strongly Agree.

	Items	Strong Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
CF1:	I trust that the IT department knows how to manage RFID devices.	1	2	3	4	5
CF2:	The RFID device could be subjected to a malicious computer attack.	1	2	3	4	5
CF3:	I trust that RFID is safe	1	2	3	4	5
CF4:	I don't trust RFID usage.	1	2	3	4	5
CF5:	My hospital uses RFID for surveillance purposes	1	2	3	4	5
CF6:	I feel my personal information on RFID devices could be inappropriately used.	1	2	3	4	5

## References

- Aberson, C. (2002). Interpreting null results: Improving presentation and conclusions with confidence intervals. *Journal for Articles in Support of the Null Hypothesis*, 36-42.
- Aczel, A. D., & Sounderpandian, J. (2006). *Complete business statistics* (6th ed.). New York, NY: McGraw Hill.
- Adams, D.A., Nelson, R.R., & Todd, P.A. (1992). Perceived usefulness, ease of use and usage of information technology: A replication. *MIS Quarterly*, 16(2), 227-247
- Akpinar, S., & Kaptan, H. (2010). Computer aided school administration system using RFID technology. *Procedia – Social and Behavioral Sciences*, 2(2), 4392-4397.
- Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckman (Eds.), *Action control: From cognition to behavior* (11-39). New York, NY: Springer.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179-211.
- Aldhaban, F., Daim, T., Harmon, R. (2015). Proceedings in *Portland International Conference on Management of Engineering and Technology (PICMET)*. Portland, OR. IEEE. 2355-2370.
- Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, 32, 665-683.
- Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behavior: A meta-analytic review. *British Journal of Social Psychology*, 40, 471-499.
- Anderson, C. L., & Agarwal, R. (2011). The Digitization of Healthcare: Boundary risks, emotion and consumer willingness to disclose personal health information. *Information Systems Research*, 22(3), 469-490
- Baek, J-D. (2007). The Effects of Individual, Organizational, and Health Care System Factors on Physicians' Information Technology Use.
- Baker, Rosland K. & White, Katherine M. (2010). Predicting adolescents' use of social networking sites from an extended theory of planned behavior perspective. *Computers in Human Behavior*. 26(6), 1591-1597.

- Barkhi, R., Belanger, F. and Hicks, J. (2008), "A model of the determinants of purchasing from virtual stores", *Journal of Organizational Computing and Electronic Commerce*, Vol. 18 No. 3, p. 177.
- Bennett, P., & Bozionelos, G. (2000). The theory of planned behavior as predictor of condom use: A narrative review. *Psychology Health & Medicine*, 5, 307-326.
- Beresford, A. R. (2003). Location privacy in pervasive computing. *Pervasive Computing, IEEE*, 2(1), 46-55.
- Bertrand, M., & Bouchard, S. (2008). Applying the technology acceptance model to WR with people who are favorable to its use. *Journal of Cyber Therapy & Rehabilitation*. 1(2).
- Bischoff, G. (2007). RFID privacy issues loom large. *Mobile Radio Technology*, 25(5), 10.
- Bollen, K., and Lennox, R.(1991). Conventional wisdom on measurement: A structural equation perspective. *Psychological Bulletin*, 110 (2), 305–314.
- Boudreau, M., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly*, 25(1), 1-16.
- Brown, S., Massey, A., Montoya-Weiss, M., & Burkman, J. (2002). Do I really have to? User acceptance of mandated technology. *European Journal of Information Systems*. 11, 283-295.
- Bruner, G.C., Kumar, A. (2005). Explaining consumer acceptance of handheld Internet devices. *Journal of Business Research*, 58(5), 553-558.
- Cammock, T., Carragher, N., & Prentice, G. (2009). Undergraduate intentions to apply to the Northern Ireland civil service: The application of a theory of planned behavior model. *European Journal of Social Psychology*, 39, 401-414.
- Cao, Q., Jones, D., Sheng, H. (2014). Contained Nomadic information environments: Technology, organization and environment influences on adoption of hospital RFID patient tracking. *Information & Management*, 51,(2), 225-239.
- Carayon, P. & Smith, P. (1995). Implementation of an electronic health records system in a small clinic: The viewpoint of clinic staff. *Behaviour & Information Technology*, 28(1), 5-20.
- Carr, A.S., Zhang, M., Klopping I., & Hokey, M. (2010). RFID Technology: Implications for healthcare organizations. *American Journal of Business*, 25(2), 25-40.

- Chao, S.-L., & Lin, P.-S. (2009). Critical factors affecting the adoption of container security service: The shippers' perspective. *International Journal of Production Economics*, 122, 67-77.
- Chen, C.C., Wu, J., & Crandall, R.E. (2007). Obstacles to the adoption of radio frequency identification technology in the emergency rooms of hospitals. *International Journal of Electronic Healthcare*, 3(2), 193-207.
- Chin, W. (1998). The partial least squares approach for structural equation modeling. In , G. Marcoulides (ed) *Modern Methods for Business Research* 295-336.
- Chin, W. (2010). Chapter 28: How to write up and report PLS analyses. Springer Handbooks, 655-690.
- Cockroft, S. (2015). *Proceedings from 48<sup>th</sup> annual Hawaii Interantional Conference on Systems Sciences (HICSS)*. Kauai, HI. IEEE. 4938-4947.
- Consumers Against Supermarket Privacy Invasion and Numbering. (2005) *RFID Right to Know Act of 2003*. Retrieved from <http://www.nocards.org/rfid/rfidbill.shtml>
- Consumers Against Supermarket Privacy Invasion and Numbering, Privacy Rights Clearinghouse, American Civil Liberties Union, Electronic Frontier Foundation, Electronic Privacy Information Center, Junkbusters, . . . Privacy Activism. (2003). 109 *RFID position statement of consumer privacy and civil liberties organizations*. Retrieved from <http://www.privacyrights.org/ar/RFIDposition.htm>
- Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson.
- Culnan, M.J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, 17(3), 341-363.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 133, 319-339.
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35, 982-1003.
- Dillon, A., & Morris, M. G. (1996). User acceptance of information technology: Theories and models. *Annual Review of Information Science and Technology (ARIST)*, 31, 3-32.



- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.
- Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq. (1986).
- Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology*, 6, 323-337.
- Fichman, R., Kohli, R., & Krishnan, R. (2003). Editorial Overview – The role of information systems in healthcare: Current research and future trends. *Information Systems Research* 223(3), 419-428.
- Fleming, C and Bowden, M 2009, 'Web-based surveys as an alternative to traditional mail methods', *Journal of Environmental Management*, vol. 90, no. 1, 284-292.
- Fornell, C., and Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research*, 19, 440–452.
- Free Dictionary. (2008). Privacy. Retrieved from <http://legal-dictionary.thefreedictionary.com/privacy>
- Garfinkel, S. (2001). Database Nation: The death of privacy in the 21<sup>st</sup> century. Sebastopol, CA: O'Reilly Media.
- Gefen, D., & Straub, D. (2000). Managing trust in B2C e-services. *E-Service Journal*, 2(2), 7-24.
- George, G., & Mallery, P. (2003). *SPSS for windows step by step: A simple guide and reference, 11.0 update*. Boston, MA: Allyn & Bacon.
- Grabner-Krauter, S., & Kaluscha, E.A. (2003). Empirical research in on-line trust: A review and critical assessment. *International Journal of Human-Computer Studies*, 58(6), 783-812.
- Gunther, O., & Spiekermann, S. (2005). RFID and the perception of control: The consumer's view. *Communications of the ACM – Special Issue: RFID*, 48
- Hagger, M. S., & Chatzisarantis, N. L. D. (2005). First- and higher- order models of attitudes, normative influence, and perceived behavioural control in the theory of planned behaviour. *British Journal of Social Psychology*, 44, 513-535.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: Sage.

- Hair, J., Ringle, G., & Sarstedt, M. (2014). A primer on partial least squares structural equation modeling (PLS-SEM).
- Henderson, S.C., & Snyder, C.A. (1999). Personal information privacy: Implications for MIS managers. *Information & Management*, 36(4), 213-220.
- Henseler, J., Ringle, C., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*. 115-135
- Hernandez-Ortega, B. (2011). The role of post-use trust in the acceptance of a technology: Drivers and consequences. *Technovation*, 31,(10-11), 523-138. Doi 10.1016/j.technovation.2011.07.001
- Heijden, H., Verhagen, T., & Creemers, M. (2003). Understanding online purchase intentions: Contributions from technology and trust perspectives. *European Journal of Information Systems*, 12, 41-48. Doi 10.1057/palgrave.ejis.3000445
- Hogg, M. A., & Abrams, D. (1988). *Social identification: A social psychology of intergroup relations and group processes*. London: Routledge.
- Holden, R. J., & Karsh, B-T.(2009). The technology acceptance model: Its past, and its future in health care. *Journal of Biomedical Informatics*, 43, 159-172.
- Hong, J.I., Ng, J. D., Lederer, S., & Landay, J.A. (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques* (DIS '04). ACM, New York, NY, USA, 91-100
- Hosaka, R. (2004). Feasibility study of convenient automatic identification system of medical articles using LF-Band RFID in hospital. *Systems and Computers in Japan*, 35(10), 571-78.
- Hossain, M. M., & Prybutok, V. R. (2008). Consumer acceptance of RFID technology: An exploratory study. *IEEE Transactions on Engineering Management*, 55, 316-328.
- Hossain, M.M., & Quaddus, M. (2011). The adoption and continued usage intention of RFID: an integrated framework. *Information Technology & People*, 24(3),.236 – 256.
- Howell, D. (2011). *Fundamental Statistics for the Behavioral Sciences*. Belmont, CA: Wadsworth.

- Hu, P.J., Chau, P.Y.K., & Sheng, O.R.L. (1999). Examining the Technology acceptance model using physician acceptance of telemedicine technology. *Journal of Management Information Systems*, 16(2), 91-112.
- Hung, S. Y, Ku, Y. C, & Chien, J.C. (2012). Understanding physicians acceptance of the Medline system for practicing evidence-based medicine: A decomposed TPB model, *International Journal of Medical Informatics*, 81(2), 130-142.
- Igbaria, M., & Tan, M. (1997). The consequences of information technology acceptance on subsequent individual performance. *Information & Management*, 32(3), 113-121.
- Johnston, K. L., & White, K. M. (2003). Binge-drinking: A test of the role of group norms in the theory of planned behaviour. *Psychology and Health*, 18, 63-77.
- Juels, A. (2006). RFID security and privacy: A research survey. *Selected Areas in Communications, IEEE*, 24(2), 381-394
- Kamra, A., Feldman, J., Misra, V. & Rubenstein, D. (2006). Data persistence for zero-configuration sensor networks. *SIGCOMM Computers and Communications Review*,36(4), 255-266.
- Keil, M., Tan, B., Wei, W., Saarinen, T., Tuunanen, T., & Wassenaar, A. (2000). A cross-cultural study on escalation of commitment behavior in software projects. *MIS Quarterly*, 299-325.
- Kitchenham, A. B., & Pfleeger, L. S. (2002). Principles of survey research: Part 3:Constructing a survey instrument. *ACM SIGSOFT Software Engineering Notes*, 27(2), 20-24.
- Konomi, S. (2004). Personal privacy assistants for RFID users. *Paper presented at the International Workshop Series on RFID in Tokyo, Japan*. Retrieved from <http://www.slrc.kyushu-u.ac.jp/rfid-workshop/>
- Krippendorff, K. (2004). *Content analysis: An introduction to its methodology* (2<sup>nd</sup> ed.). Thousand Oaks, CA: Sage Publications.
- Laerum, H., Ellingsen, G., & Faxvaag, A. (2001). Doctors' use of electronic medical records systems in hospitals: Cross sectional survey. *BMJ*, 323,(1344). Doi 10.1136/bmj.323.7325.1344
- Lapointe, L., & Rivard, S. (2005). A multilevel model of resistance to information technology implementation. *MIS Quarterly*, 29(3), 461-491.

- Lee, C-P, & Shim, J. P. (2007). An exploratory study of radio frequency identification (RFID) adoption in the healthcare industry. *European Journal of Information Systems*, 16, 712–724.
- Lee, M-C. (2008). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, 8, 130-141.
- Lee, M. S. (2009). An empirical study about RFID acceptance—Focus on the employees in Korea. *International Journal of Business, Economics, Finance and Management Sciences*, 1, 78-87.
- Leedy, P. D., & Ormrod, J. E. (2005). *Practical research: Planning and design* (8th ed.). Upper Saddle River, NJ: Prentice Hall.
- Leidner, D.E., & Jarvenpaa, S.L. (1995). The use of information technology to enhance management school education: A theoretical view. *MIS Quarterly*, 19(3) 265-291.
- Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science.
- Liao, C., Chen, J-L., & Yen, D.C. (2007). Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: An integrated model. *Computers in Human Behavior*, 23(6), 2804-2822.
- Lin, C-C. L., & Lu, H. (2000). Towards an understanding of the behavioural intention to use a web site. *International Journal of Information Management*, 20(3), 197-208.
- Lipsey, M. W. (1990). *Statistical methods for psychology* (7th ed.). Belmont CA: Wadsworth Cengage Learning.
- Littman, M. K. (2008). Implementing RFID technology in hospital environments. In N. Wickramasinghe & E. Geisler (Eds.), *Encyclopedia of healthcare information systems* (Vol. 2, 705-710). Hershey, PA: Medical Information Science Reference.
- Liu, D.-S., & Chen, W. (2009). An empirical research on the determinants of user ecommerce acceptance. In R. Lee (Ed.), *Software engineering, artificial intelligence, networking and parallel/distributed computing* (Vol. 209, 93-104). Berlin, Germany: Springer.
- Lorenzi, N.M., & Riley, R.T. (2000). Managing change, an overview. *Journal of American Medical Informatics Association*, 7, 116-124. Doi 10.1136/jamia.2000.0070116

- Luarn, P., & Lin, H-H. (2005). Toward an understanding of the behavioral intention to use mobile banking. *Computers in Human Behavior*, 21(6), 873-891.
- Malhotra, N. K., Kim, S. S, and Agarwal, J. (2004). Internet users' Information Privacy concerns (IUIPC): The Construct, the Scale and a Casual Model. *Information Systems Research*, (15)4, 336-355.
- Mandel, N. (2003). Shifting selves and decision making: The effects of self-construal priming on consumer risk taking. *Journal of Consumer Research* 30(1), 30-40.
- Markus, M.L. (1983). Power, politics and MIS Implementation. *Communications of the ACM*, 26(6), 430-444.
- Mason, T. E., & White, K. M. (2008). Applying an extended model of the theory of planned behaviour to breast self-examination. *Journal of Health Psychology*, 13, 946-955.
- Mather, D., Caputi, P., & Jayasuriya, R. (2002). Is technology acceptance model a valid model of user satisfaction of information technology in environments where usage is mandatory? *Faculty of Health and Behavioural Sciences – Papers (Archive)*, 1241-1250.
- Mathieson, K. (1991). Predicting user intentions: Comparing the technology acceptance model and the theory of planned behavior. *Information Systems Research*, 2(3), 173-191.
- Metzger, M.J.(2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, 12(2).
- Mohamed, N., & Ahmad, I.H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28 2366-2375.
- Monahan, T. (2010). *Surveillance in the time of insecurity*. Piscataway, NJ: Rutgers University Press.
- Moon, J-W., & Kim, Y-G.(2001). Extending the TAM for a world-wide-web context. *Information & Management*, 30(4), 217-230.
- Muller-Seitz, G., Dautzenberg, K., Creusen, U., & Stromereder, C. (2009). Customer acceptance of RFID technology: Evidence from the German electronic retail sector. *Journal of Retailing and Consumer Services*, 16, 31-39.
- Myles, G., Friday, A., & Davies, N. (2003). Preserving privacy in environments with location-based applications. *Pervasive Computing, IEEE*, 2(1), 55-64

- National Conference of State Legislators. (2010). *State statutes relating to radio frequency identification (RFID) and privacy*. Retrieved from <http://www.ncsl.org/default.aspx?tabid=13442>
- Norman, P., Bennett, P., & Lewis, H. (1998). Understanding binge drinking among young people: an application of the Theory of Planned Behavior. *Health Education Research*, 13(2), 163-169.
- Norten, A. (2011). *Nurses' acceptance of RFID technology in a mandatory-use environment* (Doctoral dissertation). Retrieved from electronic holdings, Nova Southeastern University.
- Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill
- Ohkubo, M., Suzuki, K., & Kinoshita, S. (2005). RFID privacy issues and technical challenges. *Communications of the ACM*, 48(9), 66-71.
- O'Leary, T.J., & O'Leary, L.I. (2004). *Computing Today*. Dubuque, Iowa: MacGraw-Hill Companies.
- Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 129-136.
- Palvia, P., Leary, T., Mao, E. Midha, P., Pinjani, P., & Salam, A. F. (2004). Research methodologies in MIS: An update. *Communications of the AIS*, 14, 526-542.
- Pavlou, P. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, 30(1), 115-143.
- Pavlou, P., & Chellappa, R. (2001). The role of perceived privacy and perceived security in the development of trust in electronic commerce transactions. *ISR, special edition on "Electronic Commerce Metrics"*.
- Petronio, S.(1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, 1(4), 311-335.
- Petter, S. , Straub D., & Rai, A. (2007). Specifying Formative Constructs in Information Systems Research. *MIS Quarterly* 31(4), 2007, 623-656.
- Phelps, J.E., D'Souza, G., & Nowak, G.J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), 2-17.

- Pirim, T., James, T., Boswell, K., Reithel, B., & Barkhi, R. (2008). An empirical investigation of an individual's perceived need for privacy and security. *Information Security and Privacy*, 2(1), 42-53. Doi 10.4018/jisp.2008010103
- Podsakoff, P.M., MacKenzie, S. B., Lee, J-Y., & Podsakoff, N. (2003). Common method biases in behavioral research. *Journal of Applied Psychology*. 88(5), 879-903
- Raad, M. W. (2010). A ubiquitous mobile telemedicine system for the elderly using RFID. *International Journal of Security and Networks*. 5(2), 156-164.
- Rahimi, N., Jetter, A. (2015). Proceedings in *Portland International Conference on Management of Engineering and Technology (PICMET)*. Portland, OR. IEEE. 2465-2495.
- Rettinger, D. A., & Hastie, R. (2001). Content effects on decision making. *Organizational Behavior and Human Decision Processes*, 85(2), 336-359.
- Rhodes, S. D., Bowie, A. D., & Hergenrather, C. K. (2003). Collecting behavioral data using the world wide web: Considerations for researchers. *Journal of Epidemiology and Community Health*, 57, 68-73.
- Röcker, C. (2010). Information privacy in smart office environments: A cross-cultural study analyzing the willingness of users to share context information. In: D. Tanier, O. Gervasi, V. Murgante, E. Pardede, B. O. Apduhan (Eds.): *Proceedings of the International Conference on Computational Science and Applications (ICCSA'10)*, LNCS Volume 6019, Springer, Heidelberg, Germany, 93 - 106.
- Roscoe, J.T. (1975). *Fundamental research statistics for the behavioral sciences* (2<sup>nd</sup> ed.). New York, NY: Holt, Rinehart, and Winston.
- Salkind, N. J. (2006). *Exploring research* (6<sup>th</sup> ed.). Upper Saddle River, NJ: Pearson Education.
- Sarma, S.E., Weis, S.A., & Engels, D.W. (2003). RFID systems and security and privacy implications. In *Workshop on Cryptographic Hardware and Embedded Systems 2003*, 2523 454-469. Doi 10.1007/3-540-36400-5\_33
- Schneider, F.B. (2000). Enforceable security policies. *ACM Transactions on Information and System Security (TISSEC)*, 3(1), 30-50.
- Sekaran, U. (2003). *Research Methods for Business: A skill building approach*. Hoboken, NJ: John Wiley & Sons.
- Shalhoub, Z.K. (2006). Trust, privacy and security in electronic business: The case of the GCC countries. *Information Management & Computer Security*, 14(3) 270-283.

- Sheng-Rong, H., Gwo-Jin, H., & Gwo-Jia, J. (2008). Intelligent hospital space platform combined with RFID and wireless sensor network. In *Proceedings of the 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (1001-1004) Harbin, China. doi: 10.1109/IIH-MSP.2008.88
- Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1) 31-41.
- Stevens, J. P. (2002). *Applied multivariate statistics for the social sciences* (4th ed.). Mahwah, NJ: Lawrence Erlbaum Associates.
- Stored Communications Act. 18 U.S.C. §§ 2701-12. (1986).
- Straub, D. W., Boudreau, M.-C., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems* (14), 380-426.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, 13(2), 147-170.
- Tabachnick, B. G., & Fidell, L. S. (2006). *Using multivariate statistics* (5th ed.). Boston, MA: Allyn & Bacon.
- Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, 2 53-55.
- Taylor, S., & Todd, P. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, 6(23), 144-176.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2) 186-204.
- Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information systems research*, 11, 342-36.
- Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences* 39(2), 273-315.
- Vinzi, V., Trinchera, L., & Amato, S. (2010). *Handbook of Partial Least Squares*. Berlin, Heidelberg, Germany: Springer-Verlag.
- Westin, A.F. (1967). Privacy and freedom. *Washington and Lee Law Review*, 25(1), 166-170.



- Warren, S., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4, 193.
- Wong, K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, 24, 1-32.
- Woon, I., Tai, G. W. & Low, R. A. (2005). Protection Motivation Theory approach to home wireless security. In Proceeding of 26th international conference on information systems.
- Wu, J-H., & Wang, S-C. (2005). What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model. *Information & Management*, 42(5), 719-729.
- Wu, D., Lowry, P., & Zhang, D. (2015). *Proceedings from 48<sup>th</sup> annual Hawaii Interantional Conference on Systems Sciences (HICSS)*. Kauai, HI. IEEE. 2976-2984.
- Xu, H., Gupta, S., & Shi, P. (2009). Balancing User Privacy Concerns in the Adoption of Location-Based Services: An Empirical Analysis, *iConference* (iSociety: Research, Education, and Engagement), University of North Carolina-Chapel Hill.
- Yang, K. (2005). Exploring factors affecting the adoption of mobile commerce in Singapore. *Telematics and Informatics*, 22(3), 257-277.
- Yin, S., Tserng, H. P., Wang, J. C., & Tsai, S. C. (2009). Developing a precast production management system using RFID technology. *Automation in Construction*, 10(5). Doi 10.1016/j.autcon.2009.02.004
- Yousafzai, S.Y., Pallister, J. G. & Foxall, G.R. (2003). A proposed model of e-trust from electronic banking. *Technovation*, 23(11), 847-860. Doi 10.1016/S0166-4972(03)00130-5
- Zhao, Y.L, & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce*, 16(4), 53-90.
- Zuboff, S. (1988). *In the age of the smart machine*. New York, NY: Basic Books.