A Study of Privacy and Security Concerns on Doctors’ and Nurses’ Behavioral Intentions to Use RFID in Hospitals

Thomas Winston
Nova Southeastern University
thomwins@nova.edu

Souren Paul
Nova Southeastern University
spaul@nova.edu

Lakshmi Iyer
UNC – Greensboro
lsiyer@uncg.edu

Abstract
Radio frequency identification (RFID) is a useful technology that has myriad applications in retail, manufacturing, and healthcare settings. RFID can scan devices in their proximity and report the data to information systems. RFID in healthcare settings presents potential security and privacy concerns to the people and processes being tracked by the devices – particularly healthcare workers including nurses and doctors. This research presents a theoretical model that will assess the effect of six independent variables: cognitive factors, perception of external control, privacy concerns regarding surveillance and RFID devices, subjective norms, existence of security policy, and persistence of data on two dependent variables, medical staff, intention to use RFID, and actual use of RFID. The model is validated with an empirical study. The results suggest that cognitive factors, persistence of data captured through RFID, and the awareness of the existence of security policy influence medical staff members’ use of RFID in hospitals.

1. Introduction
Radio frequency identification (RFID) is a useful technology that has myriad applications in retail, manufacturing, and healthcare settings. 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 is a generic term used to identify devices or objects. 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 [5].

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 stated by [27] 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 [27]. Lee [27] discovered that security concerns play a role in RFID acceptance. Anderson and Agarwal [5] found that privacy and security are always major concerns with RFID usage in medical contexts; however they were dependent on the emotional state of the patient. RFID usage in mandatory environments could violate a nurse’s privacy rights, due to the surveillance capabilities the technology enables [10]. The factors that influence the intention to use RFID by medical staff have not been studied adequately. We intend to address this gap by proposing a theoretical model that integrates the effects of cognitive factors, perception of external control, privacy concerns regarding surveillance and RFID devices, subjective norms, existence of security policy, and persistence of data on medical staffs’ intention to use RFID. The theoretical model presented in this research is based on the technology acceptance model (TAM) and the extended theory of planned behavior (ETPB). This research extends the extant and well-documented research regarding technology acceptance embodied by TAM, and its variants, and the Extended Theory of Planned Behavior, by adding the dimensions of privacy and security to the ETPB model. 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. We conducted a survey to validate the model with empirical data.

The rest of the paper is organized as follows. Section 2 presents the literature review. Section 3
introduces the theoretical model of the study. Section 4 explains the research methodology approach; section 5 presents the results of the survey. We end the paper with discussion on future directions and conclusion for research.

2. A Brief Review of the Literature

In order to develop the research model used in this proposed research, it was necessary to consider several issues: privacy research in RFID usage, security research in RFID usage as well as models used to determine acceptance of any technology. Since the research proposed here is related to behaviors, the first part of this literature review will consider how extant models of technology acceptance apply to this research, and more importantly how they help formulate the acceptance model presented herein. The second part of the literature review will detail context of the variables chosen for the proposed theoretic model.

2.1. Overview of the Models Used for Technology Acceptance

TAM, and its predecessors determined links between perceived usefulness, intention to use and actual use of new technologies. Researchers have used TAM, and its extensions TAM2 and TAM3 to determine whether or not a user population will accept a new technology. TAM2 and TAM3 added constructs to better capture behaviors associated with technology acceptance [39]. The importance of user acceptance of a technology has been stressed IS research [14, 20, 33]. Researchers have used the theory of planned behavior model (TPB) to investigate the factors influencing physicians to accept the Medline System [22]; TAM and TPB have been used to understand attitudes toward and user acceptance of RFID technology in mixed context (mandatory or voluntary use) healthcare settings [13, 20, 27]. We present the overview of these theories in the next sub-section of the paper.

2.2. Technology Acceptance Research Models

Technology Acceptance Model

TAM and the Theory of Planned Behavior (TPB) are based on Fishbein and Adjzen’s theory of reasoned action (TRA). TAM focuses on how perceptions influence a person’s intentions. Critical in its relationship to intention to use, another construct of TAM, these variables build the foundation for whether or not a user accepts information technology. Studies have used the TAM to determine outcomes in information technology adoption [14, 15, and 28]. The Theory of Planned Behavior (TPB) focuses on how an individual’s external environment influences his or her intentions, known as subjective norms. Subjective norms are perceptions of social pressure to either engage or not engage in a behavior [28]. 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 [21].

TAM underwent modifications, notably TAM 2 and TAM 3. TAM was extended to TAM 2, to expand upon the construct of perceived ease of use to include control, intrinsic motivation and emotion [37]. TAM 3 focused on interventions, which lead to greater acceptance and effective utilization of Information Technology to help direct leadership decision making processes [39].

Theory of Planned Behavior

The first iteration of the TPB was an extension of the Theory of Reasoned Action (TRA), which added a new construct – perceived behavioral control [1][4]. The TRA positively correlates intent of an individual to engage in an action with the actual engagement of that action [12]. TPB focuses on relationships between external environments and a person’s intentions [28]. The variables of intentions to perform a given activity were related to subjective norms, perceived behavioral control and attitude toward the behavior [2]. TPB has been applied to many information systems adoption problems, regarding adoption, use and disuse. [39.5] [2].

Subjective norm is defined as an individual’s perception of whether people important to the individual think the behavior should be performed [2]. The constructs in TPB help researchers to better understand why individuals engage in certain behaviors [2]. TPB is an effective tool in evaluating such decisions in healthcare settings. TPB was used to better understand binge drinking among young people [31]; condom use [7]; and likelihood of physical activity [17]. TPB is also useful in determining technology adoption in mixed (forced or voluntary) control contexts.

There are important differences between mandatory and voluntary use environments [11]. Voluntary-use environment as “one where users perceive the technology adoption or decision to use as a willful choice” [11, p. 284] while in mandatory-use environments, employees have to adopt a particular technology to keep their jobs, thereby eliminating the emphasis on prior beliefs and attitudes about the
technology [11]. Mandatory-use environments can have deleterious effects on employee perception, possibly leading to delays in implementation, or possibly leading to alternative potentially destructive employee behavior [11, p. 284].

Extended Theory of Planned Behavior
TPB was extended later by dividing the construct of perceived behavioral control into two separate variables: self-efficacy and controllability [1][2]. Extended TPB (ETPB) model was used to predict undergraduate students’ intentions to apply to Northern Ireland civil service [12]. ETPB was used to understand influences on adolescent engagement with social networking technology [6]. Group norm was found to be more useful than the construct subjective norm, in that it significantly predicted behavior intention by explaining 10% of the variance above and beyond standard TPM variable of subjective norm [6]. This finding was consistent with the subsequent research on ETPB [18][23][29].

3. Proposed Research Model

The research model presented in this paper will use the ETPB and TAM3 models and prior research on the willingness to provide access to personal health information [5]. Electronic health information privacy concern and trust in electronic medium influence patient’s willingness to provide access to personal health information and intended purpose (of use of the information) and requesting stakeholder have moderating effects on these relationships [5]. Our theoretical model is shown in figure 1.

![Conceptual Model](image)

**Figure 1. Conceptual Model**

Specifically, our model considers the effects of subjective norm, data persistence, existence of security policy, perceptions of external control, and cognitive factors of privacy concerns regarding surveillance and RFID devices, as well as trust in the electronic medium on intention to use RFID by nurses and doctors in a healthcare setting.

Next, we elaborate the different components of the theoretical model. We start with a discussion on the determinants of intention to use RFID to the medical staff.

3.1 Intention to Use, and its determinants

The factors leading a person to use a particular technology, or “intention to use” can be defined as the sum of the perceived relative weights of attitude toward the behavior and subjective norms toward that behavior. [37]. Persistence of data and subjective norm are expected to affect intention to use based on the fear that requirements to retain data may create privacy risks for patients. Another variable affecting intention to use is existence of security policy.

3.1.1 Cognitive factors and intention to use RFID.

Prior studies investigated privacy issues concerning RFID usage among nurses in a mandatory use environment [32]. According to an unidentified nurses’ union, mandatory usage of RFID tags on a nurses constituted a violation of privacy rights [32]. Privacy and security issues with devices providing location based information are mentioned in a body of literature that focuses on privacy issues considers the issue of providing location based information on an ongoing basis, as well as the privacy and security risks this poses. Prior studies demonstrate that the willingness to disclose information as a condition for transacting is an outcome variable that is consistent with prior privacy research [8, 19]. These studies investigated ways to mitigate privacy concerns with the constant transmission of personal devices that showed location, using the global positioning system. Prior studies also demonstrate that the users are reluctant to provide context (location) information, particularly when the data is automatically captured by the system [35]. RFID transmission can be intercepted and thus, it poses privacy-based risk with security ramifications, which will almost certainly negatively affect the user intention to engage in the use of the technology.

Privacy issues, such as location information security, and trust of electronic medium complicate the potential of location-based [40]. 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. LBS can also be used in asset tracking, such as in the case of RFID [40]. Prior
studies also suggest that personal health related information has gradations of importance, based on the type of information, intended use of the information, and finally the identity of the entity requesting the information [5]. The privacy concerns, described in this study as cognitive factors are negatively related to the intention to use LBS [40]. Hence:

Hypothesis 1: The cognitive factors of privacy concerns regarding surveillance and trust in the electronic medium have a negative relationship with intention to use.

3.1.2 Persistence of data and intention to use

RFID users are concerned about the issues of privacy, and value of the data, when it is collected surreptitiously and continuously [25]. Understanding 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 will affect a user’s 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 affect intention to use. Persistence of data is related to privacy concerns in sensor networks [24]. 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 [24].

Security vulnerabilities of RFID technology, such as a lack of cryptographic capability, the ability clone the device, detect duplicates, and data retention either on the device or in a centralized database cause other security concerns, which would affect intention to use [41]. 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.

In a study on consumers’ intention to use electronic medium, trust and perceived risk are found to be direct antecedents of intention to use the electronic medium for transaction, suggesting that uncertainty reduction is a key component of acceptance [34]. Juels 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 how data retention either on the device or in a centralized database causes other security concerns, which would affect intention to use [41]. Hence:

Hypothesis 2: There is a negative relationship between persistence of data and intention to use.

3.1.3 Subjective norm and 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 [12][14][15][36]. Hence:

Hypothesis 3: There is a positive relationship between subjective norm and intention to use.

3.1.4 Security policy and intention to use

According to Topa and Karyda in [47], Dinev and Hu explored factors, which showed that technology awareness has a significant impact on the intention to use protective technology (p.172). It is quite reasonable to expect a similar relationship between the existence of security policy and medical staff members’ intention to use RFID in hospitals, as in some instances RFID devices are used to protect patients and or medical staff. However, it is the awareness of the existence of a security policy (regarding RFID) and not the security policy per se that will influence medical staff members’ intention to use RFID. Hence:

Hypothesis 4: There is a positive relationship between the existence of security policies and intention to use.

3.1.6 External control and intention to use

The perception of external control affects intention to perform actions and the actual action itself. Ajzen [2] stated that perceived behavioral control, together with behavioral intention can be used directly to predict behavioral achievement. Hence:

Hypothesis 5: There is a positive relationship between external control and intention to use.

3.1.5 Intention to use and actual use

Taylor and Todd [36] showed a positive relationship between intention to use and actual use. Others such as Davis et al. [15] stated the effects of behavior beliefs and behavior intention on actual use change over time with users employment of the technologies. Hence:

Hypothesis 6: There is a positive relationship between intention to use and actual use.
4. Research Design and Methodology

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. After obtaining IRB consent, and developing a survey tool using both validated and new constructs we were able to collect approximately 115 responses from cross-section of doctors and nurses in the USA. The stratified sampling technique focused on a target population of male and female medical doctors and registered nurses aged 18 years and older. We determined using G*Power that a minimum sample size of 100 was required to have a significance level of .05.

The survey used a Likert scale as well as two dichotomous scale questions and was derived from previously validated questions such as those created by Xu and Gupta, and Taylor and Todd [36][40]. 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 [45]. We used the framework specified by Chin [42] and protocols described by Chin [42] and Wong [44] 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 [42, p. 656] and Wong [44, p. 5] emphasized that PLS applications “Do not use goodness-of-fit (GoF) Index” and similarly, Hair [43] 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 [42, 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 [44]: (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 (β) 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 [42][44].

5. Results

The latent variables, the indicators, and the measurement scales used to construct the PLS path model are defined in Figure 2.

![Figure 2](image)

5.1. Measurement Model Analyses

5.1.1 Descriptive Statistics

The frequency distributions for the latent variables are illustrated in Figure 3. The mean of the 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.

![Figure 3](image)

5.1.2 Evaluation of Outer Model Loadings
Figure 4 presents a copy of the outer model path loadings. All of the outer model path loadings were strong (≥ .5). The high proportion of strong factor loadings provided evidence to support the factorial validity of the model.

5.1.2. Internal Consistency Reliability

Figure 5 presents the composite reliability coefficients, average variance extracted and Cronbach’s alpha values for the latent variables. Composite reliability does not assume tau equivalency among the measures with its assumption that all indicators are equally weighted [42]. The composite reliability for Data Persistence and External Control was good (> .8). The composite reliability for Subjective Norm and Security Policy was excellent (> .9). The reliability of Cognitive Factors, Actual Use, and Intention to Use could not be estimated because these three variables were each measured with only one indicator.

5.1.3. Convergent and Discriminant Validity

Figure 6 presents the evidence for convergent validity indicated by the average variance explained (AVE) in the latent variables with multiple indicators. Convergent validity was strong (> 50%) for all constructs.

The square root of AVE for each latent variable was computed to test for discriminant validity. Discriminant validity was confirmed because the square roots of AVE were larger than the corresponding inner model path coefficients (beta-values) associated with the latent variables in Figure 8.

5.2. Structural Model Analyses

5.2.1 Inner Model Path Coefficients and Significance

The inner model path coefficients or standardized PLS regression weights (β) are presented in Figure 8. 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.
5.2.2. Explanation of Variance and Significance

Chin [42] and Hair [43] 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 8.

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 $CF \rightarrow IU$ 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 ($R^2 = 32.5\%$) was greater than the proportion of the variance explained in Actual Use ($0\%$).

6. Conclusions and Future Research

We recognize 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, we 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. Furthermore, intention to use was not a significant predictor of actual use. 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 and actual use.

Future research should explore further relationships between data persistence, security policy and cognitive factors. In exploring those relationships researchers should consider other factors that influence intention to use, or perhaps reformulation of the items altogether. There is a large body of literature from the technology acceptance and extended theory of planned behavior research that supports H3, H5, and H6 and this sample although consistent with G*power recommendations likely was not complete enough to well represent those hypotheses [15][2][37]. This research is the first of its type to find a strong relationship between the cognitive factors of privacy concerns regarding surveillance and trust in the electronic medium and intention to use.

The theoretical model used in this research should be refined for further research, 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 months before the Blue Cross Anthem data breach, and this alone may have been enough to change the future augmentations to this theoretical model. Developing
further lines of questioning that focus on personal data loss, as opposed to general data loss may elicit responses that better support H2 and H4. Finally, a larger population of respondents may provide better statistical power and thus increase the likelihood of rejecting the null hypothesis.

7. References


