2017

A Qualitative Exploration of the Security Practices of Registered Nurses

Beth Ann Savage
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Beth Savage

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Jean Gordon, Committee Chairperson, Management Faculty
Dr. Robert DeYoung, Committee Member, Management Faculty
Dr. Janice Spangenburg, University Reviewer, Management Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

A Qualitative Exploration of the Security Practices of Registered Nurses

by

Beth Ann Savage

MSN, Duquesne University, 1995

BSN, LaRoche College, 1989

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

College of Management and Technology

Walden University

April 2017

Abstract

Increased breach occurrences in healthcare cause concern for health information as reported by the Federal Government. Significant effort, regulations, and safeguards are in place to protect the systems used in the healthcare industry. Employee handling of security remains an area of vulnerability related to security protocols. The unified theory of acceptance and usage of technology (UTAUT) served as the model for this qualitative exploratory study with the purpose of understanding registered nurse (RN) perceptions and lived experiences related to IT security. Face-to-face interviews were conducted with 20 participants from the Three Rivers Chapter American Association Critical Care Nurses. Transcribed data were analyzed with a priori codes aligned to the constructs of UTAUT and emergent themes. The emergent themes from the RNs' lived experiences revealed perceptions of IT security mishandling, including walking away from the computer without log-off, and sharing of accounts through single sign on authenticated badges. Strategic planning for the organizational IT security may be strengthened due to the insight about the RNs' workflow related to IT security. Understanding employee perceptions, expressed intentions, and self-reported behaviors to IT security allows for the ability as managers to apply that knowledge to IT security systems, access methods, and implement procedures that will provide for increased organizational IT security and increased patient confidence. The social change from this work may provide contributions to the development of IT infrastructure systems for healthcare helping to create and maintain continued access to and availability of electronic medical records and data for increasing numbers of people who need health maintenance and care.

A Qualitative Exploration of the Security Practices of Registered Nurses

by

Beth Ann Savage

MSN, Duquesne University, 1995

BSN, LaRoche College, 1989

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

College of Management and Technology

Walden University

April 2017

Dedication

I dedicate this study to my parents and grandparents who taught me that the pursuit of a formal education is a privilege. Once attained, that education is something no one can take away, but it should be given away through sharing. My parents instilled in me a love for learning, a passion for practicing what I have learned, and an obligation to share the knowledge I gain. I have been blessed to have them as my first educators, having them help me build the foundation for all I have done in my life.

Acknowledgments

I would like to thank the many family members, friends, and colleagues for the roles they took in supporting me while making sure I got to the finish line of this journey. A special thank you to Tim, Ben, Meg, and Timmy. Tim helped protect my time and sanity throughout. Ben, Meg, and Timmy together all made it possible for me to laugh and get over hurdles when I needed it most. I love you all dearly and appreciate that you understood me giving up family time to accomplish my goals. Thanks to my friends and colleagues who gave me insight when I needed it Kathy, Char, Patty, and John; they helped push me through. Thanks to those mentoring nurses who planted the seed of advanced education long ago, Joann, Meg, Ginny, and Linda, I am forever grateful. My colleagues who inspired me in the world of informatics, Chris, Beth, and Marianne, thank you for your passion. Thanks to the Carpenter's Club, my dear colleagues who have and are traveling the same road in learning, Cheers! Special thanks to all the nurses working every day caring for patients and trying to do the "right thing" with IT security. And finally, I acknowledge and thank my committee. The stars were aligned when my committee was established because I was bestowed with the best chair I could possibly have, Dr. Jean Gordon, who supported me every step of the way through this dissertation. I was honored to have Dr. Robert DeYoung as my committee member who was engaged and provided detailed feedback and Dr. Janice Spangenburg as the URR for my work. I appreciate the contribution that each of them made in the creation of this final dissertation. My education is well beyond scholarly. The lessons I gained extend into managing work and life. I am and will be forever thankful for this journey.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Security systems and the security of information technology (IT) have multiple components. When these components are being managed in a complex environment, the exposure of having a weak link is monumental. Ferguson, Schneier, and Kohno (2011) described the weakest link property as security being only as strong as the weakest link and they suggested that all users of IT understand the weakest link property and associated results.

Employees within healthcare each hold responsibility toward maintaining the IT security of the system by using security practices set forth within the organization. One important area for the organization is password use to access the network and other clinical devices. For all healthcare IT, security is a critical aspect that requires protection and operational safeguards (Kruger & Anschutz, 2013). The registered nurses' (RNs') perceptions of IT security are not well known and may influence the IT security risk management. Further study into this gap of knowledge was the foundation for this study.

Security practices include many aspects of password management that are clearly prescribed by the healthcare IT experts. Unfortunately, these are not well understood or even known by clinical practice employees who are on the front lines of operational areas. Furguson et al. (2011) discussed the development of improper passwords, and Albarrak (2012), Fernández-Alemán et al. (2015), and Medlin et al., (2008) were able to identify password mishandling by nurses, healthcare workers, and employees. In this study, I explored the RNs' perceptions of the IT security practices that are part of their professional role as seen through the lens of the behavioral constructs from the model of the unified theory of acceptance and usage of technology (UTAUT), Venkatesh, Morris, Davis, and Davis, (2003) used as the conceptual framework for this study.

In Chapter 1, I will outline the plan for the study and will include the background of the study, statement of the problem, purpose of the study, research questions, conceptual framework, nature of the study, definitions, assumptions, scope and delimitations, limitations, and the significance of the study. In the section of the significance of the study, I will describe the importance to the practice, theory, and social change.

Background of the Study

Security of IT in healthcare organizations is the responsibility of all employees within the organization, and most of those within would suspect that a breach in security would come from the outside. However, according to Simpson (1996), most security issues are caused inadvertently by security mishandling internal to the organization. Arce (2003) identified that the current weakest link is the personal computer in combination with people's behaviors that create excessive vulnerability and produce insecure systems. These behaviors were identified in the top seven reasons for a data breach associated with authorized internal users (Kruger & Anschutz, 2013). Tam, Glassman, and Vandenwauver (2010) discussed that human behavior is the weakest link in the maintenance of internet security because of the individual level of the knowledge and use of the passwords. The behavior and use of the password practice by individuals, as it relates to the Internet, are behaviors that translate into other areas that require password protection (Cheswick, 2013). Passwords are only a single aspect of the IT security within the healthcare organization, which is a critical factor protecting access to the frontline security of the data and operations of the organization. This data includes protected health information that is governed by several regulations including the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and other regulatory oversight. IT security is complex, management of the IT security involves protecting the network, managing the users, and maintaining the appropriate IT security tools (Kruger & Anschutz, 2013). Liu, Chung, Chen, and Wang (2012) identified that the healthcare security threats came from the employees internal to the system in 70% of the cases. These authors identified the complexity of variables in healthcare that leads to the many factors for potential internal breach of the system (Liu et al., 2012). Like Simpson and Arce, Liu et al. identified the need for internal users to have knowledge of information security and good practice related to that experience.

The healthcare industry uses IT security practices in both the clinical equipment for patient care and most of the patient information gathering, maintenance, and transfer within the acute care hospital environment as well as billing and collection. The methods and level of the security maintenance by every RN are paramount to the organizational protection and overall risk management. The behaviors they employ with the use of passwords and the security practices may correlate with the description by Kruger and Anschutz (2013) who discussed the access to the electronic patient health information gained either maliciously or nonmaliciously within the organizations. These described behaviors and variant accessing of systems may be one cause for healthcare to be leading in the number of data breaches as recorded in 2011 as among the top 10 industries (Kruger & Anschutz, 2013).

Personal information security has become progressively more important with increased public awareness that has been heightened for multiple reasons, including increased reporting within the public-sector news reports, regular governmental statements, and targeted marketing to the public. O'Harrow (2012) published an investigative report identifying the many vulnerabilities of IT security occurring within the healthcare industry identified over the course of a year. These included password mishandling, insecure practices, known security access issues that were left unaddressed, and wireless device access points that were insecure, each allowing the organization open for risk of breach.

With the recent hacking of Anthem, one of the United States largest Health Insurers, the American people are even more aware of vulnerabilities toward personal information and health information (Abelson & Goldstein, 2015, Balbi, 2015). Information to approximately 80 million records was available to the hackers once they gained entrance into the Anthem system. A phishing scam was used to access the credentials of five employees from Anthem as reported by Amerigroup, the operating company of Anthem (Balbi, 2015). Similar reports were reported by Verizon in the 2011 data breach experience where phishing emails were opened and malware infected the executives' laptops allowing access to the system (Baker et al., 2011).

Access to health records is more desirable than gaining access to general credit accounts because the files from health records contain more information such as Social

Security numbers, birth dates, addresses of the individual and significant others, employment information, emergency contact information, and other personal information. A collection of such personal information allows for rapid high-level identity theft. Finkle (2013) discussed that Dell Secure Works identified in a recent report that hackers can sell complete health insurance credentials for $20 per set of data as opposed to $1 to $2 for each credit card number with a security code in underground markets. The magnitude of potential profit with this type of transaction creates a very strong interest in the sale of this information that is causing the healthcare organizations to be more inviting targets for hackers and social engineers. Finkle also discussed the statements by the Federal Bureau of Investigation (FBI) warning that healthcare remains vulnerable to cyber-attacks.

Within the healthcare organization, employees functioning in the clinical arena face accessing the electronic systems and devices during and between patient care activities. Each of these situations requires interaction with both the patient and the medical record and clinical devices. The electronic health record is necessary for accessing and gathering information as well as entering data by members of the clinical team for varying reasons at differing points during the care continuum. Potential issues that occur within each of these employee encounters with technology without accurate IT security becomes a management and organizational problem. Employees using the systems without the application of principles from the four constructs of UTAUT (Venkatesh et al., 2003) may not appreciate or understand the importance or consequence of risk under which they place the organization.

A review of the literature related to the healthcare organization IT security reveals three important avenues for the future including: (a) the state of IT in the healthcare system interwoven with the employee perception, (b) the reporting structure with oversight management by the healthcare leadership, and (c) where the healthcare IT is headed in the future. Bigalke (2009) discussed in order to fill the healthcare IT gap by 2015 that it would take a focused effort and critical goals to change behaviors of staff while bringing in new technologies. The existing literature aimed at the clinical provider presents the current state of IT security in healthcare as being focused on the electronic medical record and HIPAA.

Simpson (1996) discussed that a lack of policy and procedure, education, and oversight from leadership within the organizations allows for breaches in the security. IT leadership, healthcare organizations, and orientation programs have made strong attempts to address many of the issues that Simpson had discussed in the 90s. Some organizations have implemented consequences causing workforce employee fear of not following the rules to be an effective measure for successful implementation (Workman, Bommer, & Straub, 2009). Compliance with the security practice continues to be anecdotally reported in the popular business and healthcare literature and is captured along with the reports of the security breaches as they occur. The business management problem continues to exist because there is a lack of research and insight into how breaches and violations of the security occur. Simpson (1996) and Gaunt (2000) more than 15 years ago identified the lack of personal and professional responsibility to follow policies for information and system IT security. There appears to be an abundance of literature written related to the strengthening of policy and procedure within the healthcare organization IT and recommendations made for the education of staff associated with the security measures.

Problem Statement

IT initiatives and the security focuses in healthcare organizations have been related primarily to the electronic medical record, HIPAA, and business applications, all of which are aimed at protecting patient and organizational confidentiality and security (Graham, 2010). Measures taken to protect this security involve a vast array of security aspects, which protect the hardware and software applications used by employees of the healthcare organizations. Even though the aspects associated with security fall within the scope of IT security, they require operational management and oversight. One particular measure of the security management in healthcare is the maintenance of password confidentiality and security (Cazier & Medlin, 2006).

Currently, 37.4% of all hospital labor costs are comprised of RN labor (Welton, 2011). As the RNs make up such a large portion of the employee base and are using the technology applications for multiple purposes, it is important to identify their knowledge related to the implications and consequences of the security risk and breach. Albarrak (2012) identified that the behaviors of nurses allow for the potential security risk related to the password practices. Nurses have been found to mishandle the passwords through sharing their information, exchanging the passwords, and ignoring the need for the password resets in Albarrak's study (2012). Fernández-Alemán et al. identified a password sharing rate of 31.7% among healthcare workers. Medlin et al. (2008) were able to show findings of 73% of respondents having shared their passwords.

Security of healthcare IT is the responsibility of everyone within the organization. All employees are to have some understanding of what consequences might occur with an IT security breach. The risk of the IT security breach occurring from internal security violations is a real threat to an organization (Chopra, 2013). An internal breach of IT security may occur in many ways; however, for purposes of this study, inclusion of violations of the security practices, sharing or other mishandling of a password, and lack of the logoff procedure were explored. The business management problem is that employee mishandling of IT security poses undue risk to an organization for potential risk of breach.

Healthcare organizations expend huge amounts of resources, both human and financial, in efforts to protect the IT security. At the core of this IT security is the intent to sustain the provision of integrated healthcare using electronic systems with vast communication and trust. When this cycle of IT security is disrupted there is potential risk to the quality of care provided and the confidence of information being handled within the organization. The narrower aspect of the problem, that of understanding RNs' perceptions of IT security and related behaviors have not been explored in the literature. There is a documented and known need for IT security within the healthcare environment and that RNs have a responsibility to maintain IT security. Consistent with the healthcare literature being limited to the research targeting the security as identified by Appari and Johnson (2010), the subset of the literature that would address the perception of the RN users maintaining responsibility for and proper application of the IT security as part of their professional role is absent. There is a gap in knowledge related to the RNs' perception of what their role is in maintaining the IT security.

Purpose of the Study

Little research exists to provide reliable information to address the business management problem of RNs' perceptions of their role in relationship to IT security and how they manage passwords. To gain insight into this gap, a qualitative study was conducted "searching for meaning and understanding" (Merriam, 2014, p. 39) from the perspective of the employees own contextual interactions within the healthcare organization. The purpose of this qualitative case study was to explore the perceptions of the RN within four of the constructs of UTAUT that are specific to use behavior (Venkatesh et al., 2003). The experiences and perceptions of the RN were analyzed as they relate to the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions. Themes that emerged within each construct were independently analyzed.

The outcomes of this study are now available to provide insight into a large portion of the healthcare workforce, thus allowing employee education and development to become a part of organizational frameworks. The elimination or reduction of barriers in the security practices that are necessary within the healthcare workforce must allow for engagement with the employee allowing that employee the ability to perceive how the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions are each applicable in relation to IT security. If employees perceive these constructs as pertinent to practice, they will apply them to the work and maintain the security of the system. The risk to overall security breach for the organization is likely to then be reduced due to the increased provision of improvements to the global security practice.

Research Questions

The following is the overarching question that was used for this qualitative study: What are RNs' perceptions, expressed intentions, and self-reported behaviors of IT security?

The following research questions provided the supportive data designed to guide the work of this research using the four constructs of UTAUT that are consistent with behavioral intention and use behavior.

RQ 1: What are RN perceptions, expressed intentions, and self-reported behaviors of the performance expectancy of IT security practice?

RQ 2: What are RN perceptions, expressed intentions, and self-reported behaviors of the effort expectancy related to the IT security practice?

RQ 3: What are RN perceptions, expressed intentions, and self-reported behaviors of the social influence related to the IT security practice?

RQ 4: What are RN perceptions, expressed intentions, and self-reported behaviors of the facilitating conditions of the IT security practice?

Conceptual Framework

Venkatesh et al. (2003) described the model UTAUT, which served as the theoretical base to support and guide this research work of the security practices of RNs.

This theoretical base provided the foundational framework to identify the clinicians' knowledge levels, understanding of the password management processes, implications of a breach, and the applications of both the policy incorporation and education of the security practice within the acute care environment. Venkatesh et al.'s use of identifying and incorporating the determinants that influence the behavioral intentions to use technology within UTAUT is an ideal match for this study. Use of this model provided the depth and breadth necessary for the assessment of the definition and relationships to guide exploration toward identifying perceptions, expressed intentions, and self-reported behaviors of the RNs within the study structure. The UTAUT model delves into the construct of use behavior that lies at the core of adoption and sustaining practice.

Venkatesh et al. (2003) developed and validated the UTAUT model and they claimed the previously published acceptance theories were fragmented and incomplete in nature. The like context and components from eight models of theory were incorporated for analysis, testing, validation, and final confirmation that the UTAUT model would stand statistically proven having clearer definition and improvement toward the intention of behavior. Following testing within the study, UTAUT was shown to perform stronger than the eight models from which it was drawn. This strong performance is one of the reasons UTAUT had been chosen for the work of measuring the security practices of RNs. Four of the seven constructs identified within UTAUT are important in the behavior of the user as identified by Venkatesh et al. The four constructs include performance expectancy, effort expectancy, social influence, each of which contributes to behavioral intention, and then facilitating conditions, which contribute to use behavior along with the behavioral intentions (Figure 1).

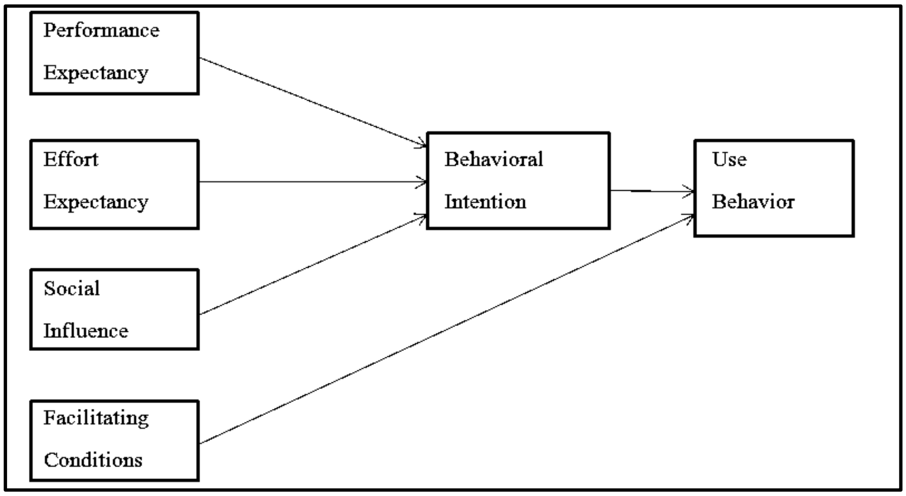


Figure 1. Constructs of UTAUT contributing to use behavior. Adapted and used with permission from CCC (Appendix 1) from “User Acceptance of Information Technology: Toward a Unified View,” by V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, 2003, *MIS Quarterly, 46*(2), p. 447.

The four UTAUT constructs that are described in this study, performance expectancy, effort expectancy, social influence, and facilitating conditions, appeal to the specific aspect of the security practice that was explored. Performance expectancy plays a role in the employees’ usage of the security practices. The belief the employees have will help them maintain aspects of their job that pertain to the patient, medical record, and system security. Exploration of how the identified employee perceives that work is influenced by the security practices and may or may not be enhanced or improved by these practices. Effort expectancy is associated with how easy it is to use the security practices. Employee perceptions related to the security practice ease may have a direct correlation with the utilization of those security practices. Social influence is the method for which the employee perceives his or her peers or significant other relevant professionals in the clinical environment believe they should be using the security practices. Within this study, the employee perceptions of social influence was an important aspect of the clinical setting related to varying levels of social support that may or may not permit sharing of passwords, mishandling of passwords, and other security issues, including no log-off.

Facilitating conditions, as perceived by the employee, include the technical methods that support the RN in using the security practices. There was expected to be a direct correlation between employee perceptions of the security practice facilitation through the conditions of technical approaches in this study exploration. Each of these constructs helped to convey insight and understanding to the security practice of the employee in the healthcare work environment. The literature review within Chapter 2 provides more in depth detail and insight into the conceptual framework information and methods as they were planned for this study.

Nature of the Study

A qualitative case study design was used to determine the perceived experiences of the RNs recruited for this study. The value of a qualitative study brings into view the meaning of the problem being studied within the research as the user sees, experiences, or understands his or her world (Merriam, 2014). The qualitative study allows for interviewing the employees of the organization thus providing insight into the RNs' perceptions, expressed intentions, and self-reported behaviors of the IT security and while using the constructs of UTAUT to guide the research. The interview is better to understand the lived experience of the individuals by listening to their stories and collecting A priori results aligned to the constructs of UTAUT and emergent themes not necessarily bounded.

The advantage that the qualitative case study with an interview process allowed over the quantitative methodology included the indepth description and analysis of the phenomenon for which the RN was experiencing related to the use of the IT security practices. Within this study, determining the interaction of significant factors within the healthcare environment and the role they play in the constructs of UTAUT were conducted. These are aspects that would not be able to reveal themselves in a quantitative study, thus it was a potential advantage of the qualitative approach with interviewing.

Data gathering and maintainance was done using ethical research principles. The population was drawn from within the professional nursing organization of critical care nurses in the acute healthcare rich regional area of Pittsburgh, Pennsylvania. The requirements of participation included that the individual must be an RN and also a member of the professional organization Three Rivers Chapter American Association of Critical Care Nurses (AACN), work full time in a clinical environment, have been oriented to the work environment, have authentication (sign on) privileges to the electronic record in the work environment, and have access to the work policies. The results of this qualitative case study were based on the representation from the personal interviews. I conducted interviews with 20 participants and had saturation reached within that population. The data analysis software NVivo v11 was used to facilitate the process of coding, sorting, trending, and managing the data. Themes emerged from the data, and

I analyzed those themes. Chapter 3 provides a more in-depth description of interview, data collection, and data maintenance processes, along with the data analysis strategy.

Definitions

For the purposes of this study, the following terms are defined:

Authentication: Method of identification or validation that the user is legitimate and may have entry to the system for which he or she is attempting to access resources or services (Milenković, Latinović, & Simić, 2013, Rajarajan, Prabhu, Palanivel, & Karthikeyan, 2014).

Clinical workflow: This is the pattern of RN work in time and motion as it relates to patient care, assessment, medication administration, patient information communication and documentation, charge nurse and preceptor duties, incorporation of clinical devices and technology including the electronic medical record, and other work of the clinical environment as carried out by the RN as part of an assignment responsibility according to policy and procedure or protocol/practice (Kashiwagi et al., 2016, Koloroutis, 2004, Zheng, Haftel, Hirschl, O'Reilly, & Hanauer, 2010).

Clinician: A person such as a doctor or nurse who works directly with patients rather than in a laboratory or as a researcher (Clinician, n.d.).

Intranet: This is a connection of workstations, personal computers, clinical devices sharing information, or host systems that are all internally managed in the organization and for internal use (Liu et al., 2012). A firewall protects the intranet creating a separateness from the Internet that is private.

IT security policy awareness: This is the individual awareness of the consequences of failing to comply with the organizational security policies (Rotvold, 2008).

Security practice: This is the behavior the nurses use to maintain the security or not by properly authenticating and maintaining the security of their accounts in order to protect the confidentiality, integrity, and availability of data (Chopra, 2013).

Security risk: This is influenced by the security practice and is defined as a threat that the password privacy or other access to the account has exposure of a kind including a violation during use due to deviation from policy, protocol, or practice, that has allowed for the threat of harm potentially rendering the system no longer secure (Rotvold, 2008).

Single sign on (SSO): A system functionality providing the end user the ability to authenticate only one time yet have full use of all systems for which they would usually be required to provide authentication (Milenković et al., 2013). This functionality will allow the user increased ease of use and decreased time spent authenticating.

Wireless on wheels (WOW): This is a common term used for a mobile cart with a computer that can be used for clinical applications.

Assumptions

A working assumption of this qualitative study was that I would act as an effective and unbiased data collection instrument with the competencies and abilities required of an interviewer including each of the following: (a) a questioning stance with regard to work and life context, (b) high tolerance for ambiguity, (c) being a careful observer, (d) asking good questions, (e) thinking inductively, and (f) comfort with writing

(Merriam, 2014). It was assumed that there would be a full review of the interview tool to assure that the tool was unbiased prior to use for the interview. I would perform with integrity and an ethically unbiased stance throughout the interview (Merriam, 2014). I would use bracketing to avoid bias. Registered nurses of the Three Rivers Chapter AACN would have e-mail accounts and have access to the Internet. This medium allows for communication, access, and response, to research communication. There was also an assumption that RNs of the Three Rivers Chapter AACN would be capable of participating in research. The environment of work within most organizations allows for and encourages professional participation in research. Research participation is a cultural norm and part of the mission statement within the professional realm of nursing at the Three Rivers Chapter of AACN. It was assumed that the RNs have had previous exposure to the terms used in this research study and had a basic understanding of IT security. Another assumption was that the RNs within the membership of Three Rivers Chapter of AACN would voluntarily participate and that they would answer honestly and completely when interviewed in the research study becoming an integral influence to the integrity of the study.

Scope and Delimitations

The scope of this research was limited to one specific professional group, the RNs. The participating professional RNs were geographically chosen from one specific professional organization within a large geographic region. The content of understanding and exploration is targeted to areas concerning the security practice, security risk, and security awareness. The four constructs of UTAUT (a) performance expectancy, (b) effort expectancy, (c) social influence, and (d) facilitating conditions were explicitly explored. The results of the RN perceptions of the IT security is reported and discussed in Chapter 4. The research boundaries were determined by the population contributing to the data collection and overall research findings. Exploration for context-dependent knowledge emerged at the point when saturation was reached with this population.

Limitations

Limitations of this study included that the study sample of RNs represented a single professional nursing organization and therefore lacked generalizability. The results from this population represent the security behaviors that can be provided in a limited descriptive presentation but are not be predictive of the future behaviors of other RN populations due to multiple contributing factors within each geographic region and organization. Additionally, the study participants were self-reporting. Limitations of self-reported results may contain bias, are not able to be verified, and are influenced by past or current situational experience (Brutus, Aguinis, & Wassmer, 2013). The members may have experienced frequent surveying by their hospitals, other agencies, and other researchers that could have created the limitation of a lower yield in an interest of participating in this study. Lastly, a final limitation is that the RN's concern for the identification or potential for leakage of information potentially leading to disciplinary action due to variance from policy may have yielded false or dishonest response, limited response, or nonresponse to the questions within the interview process.

Significance of the Study

The potential yield for positive social change as it relates to the IT security and the impact that it has in the healthcare arena is substantial. Chen, Nyemba, and Malin (2012) discussed that the lack of security in the healthcare systems may be due to the complexity and allows for risk behavior related to electronic medical record handling. There are many challenges in the healthcare industry related to security and management of the security systems. Public perception of the protected health information security and confidence of the security of their individual files are of high importance. Through the identification of the security behaviors, organizations may be able to convey a strong public confidence in an improved manner with stronger public perception.

Significance to Practice

For most individuals, healthcare providers and administrators, the aspects of the security are considered to include the electronic medical record and the aspects of HIPAA, but they do not often think of the operational systems and management objectives that are required to secure the systems and tools used to house and access information. The IT security system for not only patient information but organizational information is large and complex including but not limited to servers, data warehouses, networks, Internet, intranet, multiple vendor clinical products (both hardware and software), and the most commonly thought of accessioning devices such as personal computers. Organizational leaders must manage and safeguard the employee practices as they relate to the IT security including workflows and authentication practices. Awareness of the employees practice to carry out the accurate procedure and process for security behavior and management may be an arduous task. Insight into how registered nurses, one specific group of healthcare employees, practice and relate to the IT security will influence development and security system builds. Stronger insight and understanding of employee use of the security applications will allow administrative and IT oversight to create the policy and procedure that are nurse, clinician, employee, and patient care friendly so that the healthcare organizations are less susceptible to risk. Removal or reduction of the barriers to using the IT security along with an improved insight of employee perception will be helpful in developing a stronger process for creating the security compliance.

Significance to Theory

Future research recommendations by Venkatesh et al. (2003) included understanding organizational outcomes associated with the technology. The current literature related to theory does not connect the IT security practices of employees with the perceptions of the four constructs of UTAUT that contribute to use behavior. Allowing a pathway for understanding the connection between theory and perception may lead to a positive change in behavior of use as the constructs become meaningful as related to IT security in healthcare.

Outcomes of this work did provide insight into the role of the employees in the healthcare organizations related to the IT security allowing for a refreshed, focused, and successful planning and governance approach to the organizational IT security within the strategic plan. This study contributes to the field of IT security-specific to the healthcare security management and risk mitigation. It adds new knowledge in the fields of employee behavior related to the security and creates awareness regarding the importance of the perceptions of the RNs role related to the security management. Based on the findings of this work a framework will be established from which social change may be promoted by helping employees to gain ease of use in the security practices. The change in the promotion of the security practices may be accomplished by eliminating or reducing barriers that will decrease the risk of protected health information release and overall security breaches for an organization thus improving global security practice.

In the workflow of nursing practice, the role of maintaining IT security is an elemental part of the RN role and may be a newly recognized finding from this study. If this is an outcome, there will be an opportunity for nurses to be within the early adopter stage of IT security. Taken from Rogers's *Diffusion of Innovations* (1962), “An early adopter or Lighthouse Customer is an early customer of a given company, product, or technology; in politics, fashion, art, and other fields, this person would be referred to as a trendsetter” (p. 283).

Significance to Social Change

Utilization behavior of the employee is determined through four of the constructs identified by Venkatesh et al. (2003). If the employee perceives these to be important, then he or she will find the purpose of the IT security to be valuable and applicable to their practice. The anticipated implications to social change for the healthcare industry include identifying the gap between current theory and perception of employees related to IT security. The lack of secure password handling by nurses as described by both

Albarrak (2012) and Medlin et al. (2008) in each of their respective studies identifies one large subset of healthcare employees who expose the healthcare organization to risk.

Healthcare costs in the United States of America were at 17.4 % of the gross domestic product in 2013, according to the Medicare and Medicaid Services (2014). These healthcare costs include the burden of technology costs, security, and breach recovery. Improvements in the process related to the IT security in the healthcare arena would allow for a potential impact of cost reduction, patient safety, and patient satisfaction. Provided the employees were engaged within each of the four constructs that lead to use behavior the resulting change in security protection would ultimately position healthcare for cost reductions as a result of the decreased breach and risk. Agaku, Adisa, Ayo-Yusuf, and Connolly (2014) concluded that increased strategies include higher security for the protected health information so that the trust of the information security will not be undermined any further. Recent public reports of security breaches within the healthcare insurance companies serve to continue the media surge that raise general citizen concern that hospitals are more at risk causing lack of confidence. The general public is concerned with privacy and their general security of the information. The Federal Governments Office for Civil Rights at the Department of Human Services reported that over the last 5 years, there were 740 major security breaches within healthcare that affected 29 million people (as cited in Abelson & Goldstein, 2015). Increasing the security within the healthcare organizations creates a more confident feeling for patients individually and extends to the global public who become more comfortable. The work of identifying one population's perceptions with gained insight and potential for improvement of the IT security behavior and handling of security practices may become the catalyst to some of the change that is needed in healthcare security processes related to IT management that will promote increased patient confidence.

Through these aspects of the research, positive social change may be fully realized in two categories. The first is that when users are more confident that information is secure, they are more apt to use the electronic health record and with increased use, there is potential for maximizing healthcare delivery. Second, when organizations are able to reduce costs and resources used for security, those resources can be deployed for other healthcare contributions, such as providing additional disease prevention, community education, and further research toward healthcare advancements.

Summary and Transition

One-third of the labor force within the hospital is comprised of RNs, and they make critical decisions related to the operational use of current information systems. The RN influences his/her peers, subordinates, and other professionals within the clinical teams. Identifying RN knowledge related to the implications and consequences of the system and information security risk and breach are important. By researching the RNs operational applications of the security practice and security risk behaviors, there will be a new benefit to the organization for multiple purposes. The nurses' perceptions, expressed intentions, and self-reported behaviors of the IT security were explored using the process outlined in this chapter. Chapter 2 encompasses a review of the literature presenting a foundational frame for this work. In this review, I will identify the IT security in the healthcare setting as it relates to nursing and nursing awareness of a potential breach and risk management. The theoretical UTAUT model is incorporated into the review along with the IT security literature and a discussion of the application into the clinical environment. A view through the lens of the security awareness and how organizations approach education and policy setting are included in the review. Chapter 3 includes the research design, qualitative case study methodology, development of the interview tool, data collection methods, and methods for data coding, data analysis, and statistical analysis. Chapter 4 covers the discussion of techniques used for analysis of the data revealing findings in relationship to the research questions. Finally, Chapter 5 addresses the implications of the findings along with limitations and conclusions of the work, as well as any identified avenues for future research. Implications for social change are incorporated into the final discussion.

Chapter 2: Literature Review

Within Chapter 2, literature is identified and reviewed to frame and set a foundation for this qualitative case study of the security practices of registered nurses (RNs). Information Technology (IT) security and breach literature are available in depth and breadth in many fields and specialties. The literature focus for this study is narrowed to the management of IT security specific to the way that healthcare employees take a role in the safeguarding of such. Literature search strategy methods, an overview of the literature review search, conceptual framework, and literature associated with the foundational development of the research are discussed.

This study relates to Albarrak's (2012) research that found nurses used inappropriate security practice and password handling and then discussed that their behavior may pose a security threat up to and including a breach. The business management problem proposed for exploration is the aspect of employee handling of IT security and the level of risk upon an organization with an associated potential for risk of breach. A data breach may occur in confidential patient information, proprietary information, and general organizational risk mitigation efforts if the mishandling of IT security occurs. The focus on IT security was explored through the lens of the unified theory of acceptance and usage of technology (UTAUT). The purpose of this study was to explore the perceptions of the RN within four of the constructs of UTAUT that are specific to use behavior (Venkatesh et al., 2003). Within this chapter, I reviewed current literature that relates to the concepts of IT security within the realm of security practices that nurse would use when managing a password and logging on and off of systems for which they are authorized to authenticate and access. Literature related to the purpose of this study is aimed at inclusion of violations of security practices, sharing or other mishandling of a password, lack of logoff, and the theoretical framework of UTAUT. The aspects of IT security in alignment with the four constructs of UTAUT remained the focus of the literature review even though there are many other concerns of an internal breach of security.

Literature Search Strategy

I accessed the Walden Library for scholarly peer-reviewed literature using the search engines EBSCO host, AIB/INFORMS Complete, MEDLINE, CINAHL Plus, PUBMED, COMPUTERS and APPLIED SCIENCESCOMPLETE, and Google Scholar. While using these search engines, the key search terms of *security, breach, password(s), information technology, nurse(s)*, and *healthcare* were used. The initial Boolean search via EBSCO host using search terms information technology, security, and healthcare yielded 183 articles. The Boolean search via EBSCO host using search terms *information technology, security,* and *nursing* yielded 18 articles. The Boolean search via EBSCO host using search terms *technology, security*, and *nursing* yielded 107 articles. Password searches related to nursing produced only one article. Literature analysis did not result in a significant volume of scholarly works and journal articles that addressed security related to password use in the healthcare setting. Literature related to the theoretical foundation for this research, which focused on UTAUT and the other acceptance models of technology that were precursors are included in the conceptual framework. The precursors to UTAUT include the technology acceptance model as it evolved in 2003 (TAM 2), the original technology acceptance model (TAM), and the seminal work done by Rogers (2003) the fifth edition of his original work Diffusion of Innovations all of which were accessed and incorporated into this review.

Conceptual Framework

The incorporation of theory into this chapter required a thorough investigation of the books and journal articles related to IT and are discussed within the major themes of IT adoption, application, and usage. The theme of perception, as it relates to behavior, is described in the works of the developing theories of IT adoption. The theme of IT adoption, application, and usage theory work, which has evolved through Rogers (2003), Venkatesh, and Davis, (2000), and Venkatesh et al. (2003) is discussed and reviewed. These works and their constructs are discussed in detail as they have been evolving since the inception of the initial diffusion model with adoption to the application of this study using constructs from within UTAUT.

The theoretical foundation for this study is the unified theory of acceptance and usage of technology (UTAUT) as described by Venkatesh et al. (2003). The four core constructs that influence behavioral intention to use technology within UTAUT that are discussed and used for this study include performance expectancy, effort expectancy, social influence, and facilitating conditions.

Performance expectancy plays a role in the RNs' usage of the security practices due to the belief it will help them maintain aspects of their job that pertain to patient, medical record, and system security. Within the construct of performance expectancy, the user finds the system to be useful in his or her job and helpful in accomplishing tasks, improving productivity, and increasing opportunity for pay increase (Venkatesh et al., 2003). Exploration of how the RN perceives that work is influenced by the security practices and may or may not be enhanced or improved by these practices. When the culture of the organization supports IT security, there may be an inherent tendency toward support of the necessary behaviors within this construct.

Effort expectancy is associated with how easy it is to use the security practices. Within the construct of effort expectancy, the user finds the system to help with clear communication, improve system skill, create ease of system use, and make learning easy (Venkatesh et al., 2003). Within this study exploration of RN perceptions of security practice ease may have a direct correlation to the use of those security practices that were explored. When IT security is part of the workflow and is helpful to clinical care, employees are more likely to include the associated behaviors required to carry the security measures out fully.

Social influence is the method by which the RN perceives others, such as his or her peers or significant other important professionals in the clinical environment and the belief that they should be using the security practices. Within the construct of social influence, the user believes that the way he or she uses the system is important to their peers and will influence their use as well as the reverse their peers are influential to the way he or she are using the system. Equally important within this construct is that if the business leaders believe the system should be used, and the organization supports the system use these influences may have social influence on the end users (Venkatesh et al., 2003). Within this study, the RN perceptions of social influence are an important aspect within the clinical setting related to varying levels of social support that may or may not permit sharing of passwords, mishandling of passwords, and other security issues such as no log-off.

Facilitating conditions as perceived by the RN, include the technical methods that support the RN in using the security practices. Within the construct of facilitating conditions, the users believe they have resources and knowledge required to use the system, they determine if it is compatible with other systems that they use, and they have someone to assist them when needed (Venkatesh et al., 2003). Within this study, exploration of RN perceptions of security practice facilitation through the conditions of technical approaches was expected to have a direct correlation.

Each of these constructs help to understand the security practice of the RN in the clinical environment while performing the duties of clinical workflow. Venkatesh et al. (2003) described the performance expectancy, effort expectancy, and social influence as the three direct determinates of intention to use the system. These constructs along with the facilitating conditions described as a direct determinant of usage behavior are the reasons for these four constructs being chosen as the foundational constructs from which to conduct this study.

Adoption of technology is an area of important literature as it relates to the human interactions with technology applicable to the development of UTAUT. Historically, the first provision for context of adoption and diffusion of innovation that explained the acceptance of technology using empirical models derived from social cognitive theory began with Rogers (2003). Rogers (2004) identified attributes contributing to adoption that include, (a) relative advantage: The innovation is perceived as better than the precursor, (b) ease of use: Degree to which innovation is perceived to be difficult to use, (c) image: Perception that the innovation will enhance one's status, (d) visibility: Ability to see the system used within the organization, (e) compatibility: Degree to which innovation can coexist with values, culture, and goals of adopters, (f) results demonstrability: Ability of using the innovation results, and (g) voluntariness of use: Perception of innovation being voluntary.

The technology acceptance model (TAM) was later described by Davis (1989) at which time the user acceptance behavior was defined. TAM revealed that the individual user has an attitude toward the system that influences his/her beliefs about the system, which in turn determines how he or she will react and use the system. Within the development of TAM the following constructs are identified: (a) perceived usefulness, (b) perceived ease of use, (c) external variables, (d) attitude toward using, and (e) behavioral intention to use. Each of these constructs plays a role in the user's willingness to use the system.

Venkatesh and Davis (2000) identified that usage intentions do supersede the perceived usefulness and ease of use of mandatory systems in their model of TAM2 which extends TAM. TAM and TAM2 become foundational work for UTAUT and are factors in the consideration of behavior when assessing clinician decision making to share passwords.

Literature Review

Albarrak (2012) has identified that the behaviors of nurses when handling passwords include sharing of information, exchanging passwords, ignoring logoff procedures, and allowing for lack of secure procedures in other aspects, which place the organization at risk for breach. Organizations face the risk of security breach and must be aware of internal violations that create this situation (Chopra, 2013). The business management problem is that there is a documented and known need for IT security within the healthcare environment and that the RN maintains IT security, but current literature does not address the perception of the RN users maintaining responsibility for and proper application of IT security as part of their professional role.

The purpose of this qualitative case study was to explore the perceptions of the RN within the constructs of the unified theory of acceptance and usage of technology (UTAUT) as described by Venkatesh, Morris, Davis, and Davis (2003). The relationship of the UTAUT four constructs performance expectancy, effort expectancy, social influence, and facilitating conditions aligned with the research design and aspects of the study specific to security behavior of the employee. Each of these is specific to use behavior. Additional purposeful outcomes of this study are expected to include development of a framework for reducing barriers in security practices that are necessary within the RN workflow, decreasing risk of protected health information release, and decreasing security breach for the organization by providing knowledge areas for improvement to the overall security practice.

Information Security in Healthcare

Previous healthcare research related to information security is scarce, so other specialties and categories of literature analysis are included within this review encompassing general and specific aspects of information security not related to healthcare. There is expansive literature related to HIPAA but the focus of security for this study relates to the electronic environment in which databases of information allow clinical employees access. The implementation of the electronic health record thwarted efforts to enhance security with a range of oversight policies from categories of organizational to governmental (McGonigle & Mastrian 2015). Healthcare organizations worked diligently to implement electronic health records as incentivized dollars became available from the government. Healthcare organizations faced growing technology infrastructure and associated growing needs for maintaining information security plans and strategies for maintaining their systems. The development of information security through regulation and culture began to affect the way those healthcare organizations and their employees relate to the concept of security.

Before 2004, there was concern within the United States about the coordination of medical information and the ability to move toward an electronic platform to house medical information and data (Sochalski & Weiner, 2011). Decision making related to the movement of electronic medical records became a legislative agenda item and moved to the federal government. The migration of paper charts to electronic health records within 10 years became a forefront issue with the healthcare industry challenged by President George W. Bush's administration in 2004 to make this become a reality (Kirby, 2015). This challenge to become electronic included the sharing of a patient's documented medical history throughout the patient care continuum no matter where delivering care occurred. Medical information being maintained by IT systems became a point of conversation in the American household as much as in the healthcare arena. When the economic stimulus package was signed into legislation as part of the American Recovery and Reinvestment Act (ARRA) of 2009 there was a creation of a new vision for expansion of health IT (Sochalski & Weiner, 2011). This act is the driving force behind what most healthcare providers know as meaningful use.

The Health Information Technology for Economic and Clinical Health Act (HITECH) Act is an important part of the American Recovery and Reinvestment Act. Essential components of HITECH include certified electronic health record technology that meets governmental standards, enterprise integration that links all healthcare providers to enable information exchange, and qualified electronic health records to handle all necessary information needs to provide healthcare related needs (Graham, 2010, Kwon & Johnson, 2012, McGonigle & Mastrian, 2015). HITECH has aimed to improve healthcare quality, reduced costs due to inadequacies, improved overall health, facilitated future care through research, and secured a realm to house patient information. HITECH and healthcare leaders' focuses maintain alignment towards the same goals and visions (McGonigle & Mastrian 2015). The implementation of this program began the incentive for healthcare systems to make a substantial investment in the implementation of IT systems that would maintain patient information and data.

The introduction of meaningful use along with the HITECH legislation by the federal government occurred in 2009 as a part of the American Recovery and Reinvestment Act. Healthcare organizations are “scurrying to select decisively, implement, enhance, or measure the care impact of electronic health records so they may achieve the meaningful use criteria” (Murphy, 2011, p. 153). Meeting the meaningful use criteria allows for the qualification of the Centers for Medicare & Medicaid Services Incentive payments. The incentive payments allow for continued support of the healthcare infrastructure.

Regulatory compliance in IT is a factor that influences the governance of the management and operations in all businesses. When applied to the healthcare industry there are not only the aspects of IT governance but also the overlapping health IT governance including HIPAA and HITECH. Project planning incorporates security practice in healthcare from the point of plan development through implementation and adoption. The security practices and regulatory compliance of such within the healthcare industry is a segment of manageable practice. Several regulatory agencies provide guidance and oversite related to the security of healthcare practice and management. These regulatory agencies include the US Department of Health and Human Services regulations, HITECH, HIPAA, and state regulations. Kwon and Johnson (2012) reported that there is varying compliance in security practice within the healthcare industry due to differing interpretations of the guidance and written compliance directives. Safeguarding, auditing, HR management, and third party security management were the four types of security practices identified as used when reviewing the organizations that maintained high levels of security leaders (Kwon & Johnson, 2014). Within their research, the authors found that the hospitals with high rankings in the adoption of security practice and compliance with the technical aspects still varied in the application of practice. The authors believed this variation was a result of the adoption of policy and procedure and to what level that infusion into the organization occurred. This representation of necessity for technical and non-technical solution adoption done simultaneously is paramount.

For most individuals, healthcare providers, and administrators, the aspects of security include the electronic medical record and aspects of HIPAA, but they do not often think of the operational systems and management objectives that are required to secure the systems and tools used to house and access information. The IT security system not only for patient information but also for organizational information is large and complex including but not limited to, servers, data warehouses, networks, Internet, intranet, multiple vendor clinical products (both hardware and software), and the most commonly thought of for accessioning devices such as PCs. Clinicians within the healthcare organization, depending on their role and daily functions, each have workflows and the need for access to gain and or enter information. For all the previously mentioned components of the system to be protected, those employees who access the system must be legitimate, and the system must sustain levels of strict security and privacy. Authentication of the employee is one way of maintaining these objectives for the system security, and passwords are one way of authenticating. Authentication is the method of identification or validation that the user is legitimate and may have entry to the system for which they are attempting to access resources or services (Milenković, Latinović, & Simić, 2013, and Rajarajan, Prabhu, Palanivel, & Karthikeyan, 2014). The healthcare organizations attempt to assure ease of use related to secure practice by implementing authentication practices using single sign-on (SSO) allowing the user ease of access to multiple applications. According to Milenković et al. single sign-on allows the user increased ease of use and decreased time spent authenticating because of the functionality to authenticate only once and have full use of all systems. With authentication methods known and established by the organization for employees, it is up to the employee to carry out the accurate procedure and process for security behavior and management.

Another aspect of employee interaction with IT security is the use of devices. Koivunen, Niemi, and Hupli (2014) demonstrated in the study of health professionals using communication devices that barriers prevent correct processes toward security and tools for best outcomes are not always present even if the user wants to use secure practices. Healthcare organizations are accountable for security practices of the employees and with this study, Koiven et al. (2014) identified that healthcare needs more information to support better the growing field of device management and security.

Leaders of the organizations take responsibility for overseeing the IT security programs from all aspects of development, implementation, and evaluation to assure it is ongoing and protecting the organization. Often the Chief Information Officer (CIO) is the individual to lead the organization with focused information related to the management and oversight of IT security. Landolt, Hirschel, Schlienger, Businger, and

Zbinden (2012) conducted a study of 112 hospitals in German-speaking Switzerland gaining information from the CIOs to find if the organizations were compliant with the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standard ISO/IEC 27002. The study investigated if the standards implementation was nothing through to complete. Of 51 responding hospitals, there was a 51.1% score of implementation. Switzerland has an implementation plan suggesting that the hospitals are facing difficulty in implementation with the standards similarly to many other countries. Interestingly, the university hospitals have lower percent compliance than the private hospitals but it was not statistically significant. This study demonstrates another set of standards and a group of leaders attempting to oversee security measures for healthcare organizations.

IT security is complex, management of the IT security involves protecting the network, managing the users, and maintaining the appropriate IT security tools (Kruger & Anschutz, 2013). In a review of current statistical data conducted by Liu, Chung, Chen, and Wang (2012), they identified that the healthcare security threats came from the employees internal to the system in 70% of the cases. These authors identified the complexity of variables in healthcare that leads to the many factors for potential internal breach of the system. Box and Pottas (2013) discussed that the general operational functioning of healthcare professionals is naturally within an honorable and trusting community culturally implicit of a low threshold for need of security sensitivity. Unfortunately, this leaves many of the frontline with a limited sense of need for IT security awareness.

Enhancements of security are an avenue that continuously develops even as the basic security measures remain weak or continue development at the same time. Liu et al. discussed advancing the protection of the medical information using firewalls since most healthcare organizations now use the internet as part of their regular course of business. Like Simpson (1996) and Arce (2003), Liu et al. identified the need for internal users to have knowledge of information security and good practice related to that experience. Organizational IT security depends on the secure behaviors of all employees.

The healthcare industry uses IT security practices in both the clinical equipment for patient care and most of the patient information gathering, maintenance, and transfer within the acute care hospital environment as well as billing and collection. Intranet and Internet use by the employees are areas of importance for clinical attention similar to all clinical devices. The intranet is an internal connection for the workstations, personal computers, clinical devices sharing information, or host systems that are as a group internally managed in the organization and for internal use (Liu et al., 2012). Firewall protection separates data used on this internal system from the Internet and maintains a secure privacy. The internet allows open access between the organization and the "Internet highway" diminishing security practice thus many healthcare clinical desktops that use clinical applications including the electronic medical record do not allow open access, but limited - controlled access, to the Internet. Chen, Nyemba, and Malin (2012) discuss the predictability of behavior related to the employee handling the medical record in comparison to social technology computing companies like Twitter. The findings that they presented included healthcare organizations being stable inclusive of the networks or departments representing the organizations and employees as dynamic in nature. These findings are positive given the electronic record and the data collected through the record are constantly transforming. Health information exchange is on the forefront of advancing communications between clinicians and organizations to improve patient care while tracking patients and identities (Crawford, 2014). These types of health intelligence will continue to increase as data driven care continues. Security requirements will continue to increase as this field grows.

Administrative and management oversight is important in the leadership of employee engagement with IT security. Alshaikh, Ahmad, Maynard, and Chang (2014) conducted a review of management activity related to security that was in the literature. The authors reviewed 284 academic papers and 192 test books to develop a preliminary taxonomy. The findings of the study included organizations policy management strategies of building a security team, which may include a security manager, to (a) implement and manage security, (b) manage information security risk, (c) develop employee security awareness, (d) maintain documentation of technical controls, and (e) act as an organizational liaison. The findings from the taxonomy included within each of the practice areas a guide for assessment, development, implementation, evaluation, and sustainability. Alshaikh et al. discussed in future research that by omission the literature did not differentiate practices into managerial or technical categories. The findings, from the review of organizations with a security team, were positive of which became helpful to the users.

Understanding the benchmarks presented in the literature along with best practices identified in case studies related to the administrative and IT oversight the importance of employee engagement related to IT security is evident. This is the foundation for understanding the connection made between the RN role and security compliance. Applying this literature built a foundation for identifying the construct of Performance Expectancy and understanding how it plays a role in the RNs usage of the security practices. According to Venkatesh et al. (2003) within the construct of performance expectancy, the users find the systems to be useful in their job and helpful in improving overall productivity.

IT Security

IT security, in general, has a great wealth of information with vast literature available. Exploration of that literature with application to the health IT security may be of some benefit. Many of the organizations find similarity in culture, employees, system management, regulatory compliance, and straddling new technology and approaches to challenges. Often organizations implement compliance regulations with the intent that all will be perfect, and it just does not work. There is much more to the story of regulation and as Kwon and Johnson (2012) points out in his work, there is no correlation between individual measures and breach performance thus there is no guarantee to security performance.

Technical aspects of IT security include managing software and hardware, devices communications, wireless, intranet, internet, and system access technologies. Identity management is one example of a system that is managed by IT security. Single sign-on, an identity management system that allows for authentication to multiple applications, is widely used in corporate environments. Milenković et al. discuss that the identity management system solves the problem of users having to create and remember multiple passwords that would most likely cause the creation of insecure passwords, forgetting passwords, or wasting time with multiple authentications. Organizations overseeing the authentication process must consider the system use for the single sign-on authentication. All users with multiple applications will most likely use the functionality creating desired participation and required security oversight. Password and biometric authentication are both methods of gaining access to systems securely. Li, Wen, Li, Zhang, and Jin (2014) discuss that the biometric authentication scheme protects information security and privacy.

Practices that improve culture must involve the employees and organizational stakeholders to change security culture alike (Gaunt, 2000, & Kwon & Johnson, 2014). The culture of an organization influences responses to IT security. Kwon and Johnson (2014) demonstrated in his work that there were three levels of security practice adoption based on culture, leaders, followers, and laggers. Those identified organizations noted as leaders were training and managing risk and breach incidents.

Human factors are frequently mentioned in the literature when discussing IT security and often through history have been referred to as the weakest link (Arce, 2003, Tam et al., 2010, and Ferguson et al., 2011). Kwon and Johnson (2014) discuss that the healthcare industry faces two weak links the internal threat and the external threat. Because healthcare has not adequately ramped up to deal with the security risks through investment, remainders exist of uncertainty related to coping with the two weak links. Evaluating and managing the human factors is one of the key aspects of IT security. Negligence is often cited as a human factor that affects the organization. Negligence can fall into several categories of security risk. Kruger and Anschutz (2013) discussed the insider negligence at the root of data breaches. They discussed the false sense of security that everyone inside is safe but outsiders find ways in and not all insiders are honest (Kruger & Anschutz, 2013). Security related behavior is an ever-pressing topic related to overall IT security. The employees' behavior must be reviewed and understood within the organization so that there is an opportunity to delineate risk behaviors. Once delineated, the behavior must be addressed in a manner that will be corrective. A vigilant program will increase employee IT security awareness.

Nurses Awareness of Security

Review of the literature revealed the limited field of work written related to awareness of IT security by the end user. Most of the employee IT awareness information is imbedded in the IT education and IT policy literature or is inferred within implementation of IT project literature. Documentation in the literature about the knowledge of handling IT security is limited. As the focus narrows toward IT awareness of nurses, the literature available is increasingly sparse. Direct awareness of IT security is often targeting the nurses' awareness and concern for privacy during the use of technology in regards to communicating patient information. In studying factors effecting compliance of IT security, Harris and Furnell (2012) discuss that the employees of organizations have been found to have only moderate to low awareness when asked about behaviors required for security compliance. Albarrak (2012) who studied the population of nurses identified that the nurses were deficient in security awareness and the importance of overall IT security in relation to patient data. However, Albarrak was able to identify that the nurses had a 92% awareness of the need for password authentication when accessing the electronic system for patient information. Harris and Furnell (2012) and Albarrak's (2012) findings are both contrary to what Koivunen, Niemi, and Hupli (2014) identified in their study of nursing professional's experience using communication devices in that nurses had a concern for information security during the use of such devices and expressed awareness as they relayed barriers of use. There was no description within any of the three studies as to the reason for the state of IT security awareness. One may be able to consider the point of evaluation for awareness as the study that identified IT security awareness involved devices that were used with points of contact and consideration in the midst of patient information sharing as opposed to initiating and ending a session for access to a system.

Insight into human behavior and intention gives clues to awareness as described by Yoon and Kim (2013) and reveals employee characteristics maintaining IT security. Within their study, the findings described that behavioral intention is a key variable in IT security awareness. Discussion included that the individuals' beliefs of protection from being part of an organization that provides security is important to maintaining security. Ifinedo (2012) discussed that the by holding a regular IT security awareness campaign managers will increase presence with the employees and be shaping the future security behaviors of the employees.

Policy and Penalty

Literature from Simpson (1996), Gaunt (2000), and others more than 15 years ago, identified the lack of personal and professional responsibility by users to follow policies for information and system IT security. The following education and policy literature review covers aspects of organizational and employee response and interaction to IT security policy, strengthening of policy and procedure within the healthcare organization, IT involvement in education and policy, and recommendations made for the education and consequence of staff associated with IT security measures.

Simpson (1996) discussed that a lack of policy and procedure, education, and oversight from leadership within the organizations allows for breaches in the security. IT leadership, healthcare organizations, and orientation programs have made strong attempts to address many of the issues that Simpson had discussed in the 90's. Gaunt (2000) discussed the need for training to increase awareness. There are many aspects to security policy compliance related to the human factor with one of the first being awareness (Belanger, 2011; Renaud, & Goucher, 2012; Vance, Lowry, & Eggett, (2013); & Barlow, Warkentin, Ormond, & Dennis, (2013). An employee must first be aware of a policy before being able to follow that policy. Renaud and Goucher (2012) reaffirm that it is unlikely that the employees will read policies without encouragement, so it takes management interaction, education, and oversight to assure that the employee gets the information. Following awareness, there are several other strategies that an organization would employ.

Belanger (2011) found that attitudes regarding policy implementation for security were not affected based on knowledge of consequence even if there was a known consequence and the breach was severe. A secondary finding revealed that technical competence had a relationship to a decrease in policy enhancement, which Belanger concluded might be due to the mandatory aspects of change thus impacting pride. When mandatory processes are implemented, the individual is placed in a challenged position and with competence being questioned a negative attitude may develop.

Through the years, many different strategies have risen as implementation solutions for organizations including one of consequence. Consequences causing workforce employee fear of not following the rules is an effective measure of successful implementation as reported by Workman, Bommer, and Straub, (2009). In a field, study focused on individual and organizational factors Workman et al. (2009) used survey and observation to gather data and conduct an analysis of that data using exploratory factor analysis. The factor analysis led to high congruence between the self-reported data and the observation data thus z-score was applied. Predictive amplification of procedural justice was applied to all hypotheses in the study resulting in a conclusion that the security focus was on either the individual or the organization factors but not on both. When individuals believe the threat is high and is directly expected to influence them personally, they will respond by supporting policy much more than if the threat is perceived as distant. Findings related to procedural justice were important in this study when the organizational processes supported justice related to employee concerns or grievances and management addressed them there was a 20% increase in security behaviors.

Guo, Yuan, Archer, and Connelly (2011) identified that misuse of organizational information security policies without malicious intent to cause harm is the definition of a non-malicious security violation. Based on this definition, Guo (2013) identified behaviors of security violation that include (a) intentional, (b) nonmalicious self-benefitting, (c) voluntary rule breaking, and (d) possibly causing damage or security risk. Considering each of these behaviors as undesirable, Guo (2013) discusses the multifaceted approaches to the resolution of security risk. He suggests additional literature including deterrence with a focus on prevention, punishment, contingency factors, neutralization, and relative advantage in job performance.

Yoon and Kim (2013) examined the practices of 162 employees of Korean organizations to identify a model for analyzing employees' workplace related computer security behaviors. Yoon and Kim identified that the moral obligation and attitude toward computer security are predictors of individual employee's intention to practice computer security behavior. The identified model aligns with the UTAUT model as it prescribes similar tracts leading to behavior and use. Interestingly, this study brought the concept of moral obligation into the realm of a security behavior rather than an ethical issue, which allowed this examination to take place as a self-control measure. This measure of moral obligation contributed to the social norms as a positive deviant to security behavior. Ifinedo (2014) suggested in the findings from his study that management providing atmospheres where employees could share organizational values through socialization with fellow workers could increase security compliance. Gajanayake, Shame, and Lane (2013) described an information accountability system that allows for minimizing risk if the proper governmental regulations are in place. This is done through instruments of measuring evaluation of protocol coupled with user context. It is based on user awareness and actual user adoption. Gajanayake et al. (2013) evaluated this method of accountability on an eHealth system allowing for the variance of healthcare information, personnel, and patients.

Agaku, Adisa, Ayo-Yusuf, and Connolly (2014), Kim, Yang, and Park (2014), and Umphress, and Bingham (2011) each discussed the behavioral aspects of employee compliance with security policy and organizational protocol providing varying reasons for behaviors. Agaku et al. (2014) identified that employees are willing to take measures of security with protected health information but do not easily make the connection to other security measures that encompass and protect the system housing the patient's medical records. Kim et al. (2014) demonstrated that there is a relationship between the belief of security policy effectiveness and policy compliance, thus the higher the trust in the security policy the higher compliance with the policy. Conversely, Umphress and Bingham (2011) identified that there may be developed unethical pro-organizational behavior that influences culture in which the employees believe they are protecting the organization by purposefully violating the policies. Because the actions are seen as protecting the organization it is overlooked and becomes a cultural norm. These unethical acts although violating policy and procedure are seen as doing bad for good reasons by the employee and the employment social group with outcomes that lead to risk. The relationships are complex and warrant further research. This concept of neutralization is violating policy but believing it is for the good of the organization is justifying the reason for violation of policy. The justification or rationalization may occur in many forms as the employee moves through the process of violation. Barlow et al. (2013), Kim et al. (2014), and Umphress and Bingham (2014) all concluded that neutralization is prevalent with in the employee base and requires training to raise awareness. Barlow et al. (2013) discussed that based on neutralization, employees will violate policies even with the knowledge that there are deterrent policies in place suggesting that they rationalize the deterrence consequence. Healthcare providers often justify the work they do finding applications to patient care. Thus, neutralization may be a plausible application to the clinical personnel when applying security principles to the clinical workflow.

Agaku et al. (2014), Kim et al. (2014), Yoon et al. (2013), and Umphress and Bingham (2011) all subscribed to the necessity of training for information security so that when the employee is faced with the security situation, no questions arise, the process of knowing what and how to take measures of protecting the system is second nature. In this situation, the employee knows the policy, has practiced, and will be without a risk of security breach. Training includes basic security knowledge, policy awareness, neutralization awareness, and communication methods (Barlow et al., 2013, and Renaud et al., 2012). The education and communication processes are foundational knowledge for the implementation and sustainment of policy and protocol knowledge related to information security. Barlow et al. (2013) and Kim et al. (2014) discouraged neutralization to reduce IT policy violation. Although the education is not a single factor of success toward security maintenance, it is required so that there is a basic level of understanding by employees for performance expectation. Several methods of communicating basic knowledge including policy introduction to employees at the point of entry to the organization on orientation is accomplished during the following; annual competency review periods, information review of policies, and during regular communication rollouts within the organization. Once provided education reaches the employees', engagement in the security process is elicited and is best incorporated into the performance expectation. Vance, Lowry, and Eggett (2013) recommend accountability processes for the reduction of access policy violations. Within the study, (a) monitoring awareness, (b) auditing, (c) engaging in approved actions, and (d) emulating social presence were four aspects of positive influence toward accountability (Vance et al., 2013). Accountability means that the employee is responsible for the security but they must also be empowered to care for the security of the organization, meaning they need to have the correct knowledge and tools. If the employees can view the responsibility of security as shared, they will adjust along with management staff when supported to appropriately uphold the security efforts of the organization (Renauld et al., 2012).

Another look at consequences for human motivation related to rule following in the realm of information security is punishment or reward. Son (2011) and Ifinedo (2012) explored variables of intrinsic motivation and motivation theory and how they relate to security compliance. In contrast, Harris and Furnell (2012) explored shaming and the impact that it had on behavior and awareness toward security compliance. Shaming was found to be impactful because it outweighed the act itself and the employee was aware of the wrongdoing. If the employee was not aware of the wrongdoing, then the shaming was not effective and created a negative perception of IT. The negative perception of IT becomes counterproductive to the efforts of building relationships and communication pathways. The most concerning and severe report of shaming by the employees was when an employee' name and a photo was placed publicly for the rest of the peer group to see. An example given was a posting within the break room. The employees felt as though the shaming sanctions were harsh and they did respond but Harris and Furnell (2012) cautioned that the risks of alienating staff from information security staff and ideas might be detrimental to overall efforts. The study by Son (2011) demonstrated that there is a lack of attention toward the intrinsic motivation of human behavior. Provided managers connect with internal values of employees, stronger connections toward security compliance would occur. Ultimately, alienation through shaming would not be the ideal in creating connections.

Leaders and top management in the organization are individuals that influence the cycle of information security compliance. Hu, Dinev, Hart, and Cooke (2012) explored the aspects of leadership, culture of the organization, and the employee behavior. The findings included that the top management has a critical role significantly affecting the organizational culture and employee beliefs. Organizational culture has a significant effect on employee attitudes. It is important that top management is helping to form the culture of security for and along with the employee. Box and Pottas (2013) suggested that the actions must be taken to promote positive attitudes along with the policy implementations toward IT security behavior. This will only be accomplished through the motivational properties of emotion.

Facilitating Conditions as perceived by the RN, include the technical methods that support the RN in using the security practices. Within the construct of facilitating conditions, the user believes they have resources and knowledge required to use the system, they determine if it is compatible with other systems that they use, and they have someone to assist them when needed (Venkatesh et al., 2003). Within this study, exploration of RN perceptions of security practice facilitation through the conditions of technical approaches is expected to have a direct correlation.

Throughout this section of security related policy and associated behaviors, the patterns of password management by employees and risk of breach are additional areas of literature that impact the foundational work for this study in framing the business problem. Compliance with the security practice continues to be anecdotally reported in the popular business and healthcare literature and captured along with the reports of the security breaches as they occur. The business management problem continues to exist because there is a lack of research and insight into how breaches and violations of the security occur.

Password Management

Maintaining the security of the IT system within any organization must focus on the employees who access the system. Protecting access to the system is most frequently accomplished through password authentication (Albarrak, 2012; Belanger, 2011; Cazier

& Medlin, 2006; Rajarajan, Prabhu, Palanivel, & Karthikeyan, 2014; Sharma, & Sugumaran, 2011; and Tam, Glassman, & Vandenwauver, 2010). From an organizational perspective, the IT system is composed of three parts, technology, management, and the people (Cheng, Li, Li, Holm, & Zhai, 2013). The people or employees remain the weakest link in security and password management even though there have been strides in technology systems (Medlin et al., 2008; & Tam et al., 2010). According to Sharma and Sugumaran (2011) a clear understanding of the asset and the value of such asset is required for a company to create the policies and changes around the process to ensure adequate security including employee practices. A review of literature related to password practices is presented in this section and demonstrates the interrelatedness to behaviors or violations of IT security literature.

Reviewing the history of passwords, Cheswick (2013) discusses the Green Book that the U.S. government published in the 1980's providing advice for passwords and avoiding threats against technology. Cheswick (2013) makes comparisons from the 1980's with today identifying how the paradigm has shifted noting that there are very different password creation methods for protecting the security. An example provided is that in the 1980's it was a general rule of thumb not to ever write a password down but to create a password you would remember because the threat was that someone at the office or in your desk area was the threat of theft. Today the threat is remote and can access the computer system from miles or countries away so creating a strong password that you may not remember except for writing it down is much less of a threat. Cheswick (2013) suggests ways to remember the password by writing phrases that will help you remember it without actually writing the password down thus making it even more secure.

Measures to protect IT security involve a vast array of security aspects, which include the hardware and software applications used by employees (Crazier et al. 2006; Medlin et al., 2008, & Rajarajan et al., 2014). Even though the aspects associated with security fall within the scope of IT security, they require operational management and oversight. One particular measure of the security management in healthcare is the maintenance of password confidentiality and security (Cazier & Medlin, 2006, and Medlin et al., 2008).

To understand the population of employees that will be included in this study, a brief summary is provided here. There are 3,972,327 professionally active registered nurses in the U.S. (KFF, 2015). According to Charles, Gabriel, and Furukawa (2014, May) there are currently 94% of hospitals with basic electronic health record adoption and 59.4% with certified electronic health record adoption. Between 2008 and 2014, there has been a two-fold increase in electronic health record adoption by office-based physicians (ONC, 2015). Provided the governmental incentives described earlier remain in place these numbers will continue to rise creating few environments remaining for a nurse to practice without accessing an electronic medical record and IT system. Within the workforce of healthcare today, 37.4% of all hospital labor costs are comprised of RN labor (Welton, 2011). Because the employee base is comprised of a large portion of RNs who are using the technology applications for multiple purposes, it is important to identify their knowledge related to the implications and consequences of the security risk and breach.

Albarrak (2012), Fernández-Alemán et al. (2015), and Medlin et al. (2008) identified that the behaviors associated with password practices allowed for password sharing. Albarrak (2012) identified that nurses mishandled the passwords through sharing their information, exchanging the passwords, and ignoring the need for the password resets. Fernández-Alemán et al. (2015) discussed that sharing of passwords among healthcare employees who responded to the password security questions identified that they shared passwords. A review of security scoring was done to evaluate relationships between education level, work experience, professional category, and gender of which none were significant for the sharing of passwords. Medlin et al. (2008) concluded that the employees did not view the IT security aspect of password management as important. Albarrak (2012) reported the password sharing at a rate of 33%, Fernández-Alemán et al. (2015) at a rate of 31.7 %, and Medlin et al. (2008) at a rate of 73%. In these three studies, sharing of passwords occurred with coworkers or colleagues and friends of their coworkers. Reasons for sharing were not described.

Developing and managing a password was discussed by Albarrak (2012), Belanger (2011), and Medlin et al. (2008) identifying that users had knowledge of how to create a strong password but did not choose to do so when an easier to remember alternative could be used. Belanger (2011) described this user preference as “ease of use”. This path of ease is the avenue that most users will default toward when developing their passwords if left to their own devices. Medlin et al. (2008) identifies that memorization of passwords is not practical or effective as the short-term memory is not capable of holding such if it is correctly crafted. Often the lack of ability to memorize the difficult password is what leads to the easy password creating those that are then easy to guess making the system vulnerable to risk. Medlin et al. (2008) identified that most users' passwords fell into four primary categories that were previously defined, Family, Fan, Fantasists, Cryptic and the four expanded groups of Other, Faith, Place, and Numbers. The password categories are each briefly defined in Figure 2.

Category	***Definition***
Family	Name or nickname, name of child, partner or pet, birthday
Fan	Names of athletes, singers, movie stars, fictional characters or sports teams
Fantasists	Evidence of sex is evident in passwords such as "sexy" "stud" and "goddess"
Cryptic	Unintelligible passwords or a random string of letters, numbers and symbols
Other	Common English dictionary terms that did not include religious terms or places
Faith	Terms associated with religion or religious terms or places
Place	Names associated with towns or cities
Numbers	A string of all numbers

Figure 2. Primary and expanded password categories and definitions. Adapted from Analyzing the vulnerability of U.S. hospitals to social engineering attacks: How many of your employees would share their password? by Medlin, B., Cazier, J., & Foulk, D. (2008). *International Journal of Information Security and Privacy*, 2(3), p. 74-75.

Medlin et al., (2008) did make a correlation in findings that those who made stronger passwords were less willing to share their passwords (29%) than those who included family in the password who were willing to share at 60% and those who included numbers at 50%. Along with categories of password creation findings of password strength or complexity is identified. According to Crazier et al. (2006), the password should be complex to create the secure environment and maintain the password as the protective gatekeeper to the patient information. The complex password definition includes a combination of at least eight characters with a mix of upper and lower case letters and at least one special character (Crazier et al., 2006). Tam et al. (2010) identified that even if there was intent to create a complex password it does not lead to a password that is better. Albarrak (2012) had no nurse create a strong password that would meet the definition of complex. Another issue that Albarrak (2012) explored with nurses was them changing the password once they were aware that others knew the password and 54% responded that they would not. Along with the previous concerns of password management, a paralleled aspect of security management is computer log-off. Albarrak (2012) identified that 16% of the nurses studied did not log off of the system they were working with, allowing for others to access confidential information under their authentication, again representing a lack of understanding or connection with IT security.

Tam et al. (2010) and Cheswick (2013) discussed that the issues surrounding password management are related to the human factors and that people will trade convenience for the security. Even though password knowledge is present, Tam et al. found that users were more concerned about family and friends gaining information than that threat of hacking or identity theft. Tam et al.’s (2010) findings regarding password selection showed that users were able to understand a passwords quality but often chose a weak password because it was more convenient basing this on the concept of the influence of a near event versus the likelihood of a future event. The example provided is the protection from a future event such as identity theft versus the current event remembering my password (Tam et al., 2010).

Social Influence is the method by which the RN perceives others, such as their peers or significant other important professionals in the clinical environment, believe they should be using the security practices. Within the construct of social influence, the user believes that their use of the system is influential to others and others that are important think that it should be used, the business leaders believe it should be used, and the organization supports the system use (Venkatesh et al., 2003). Within this study, the RN perceptions of social influence are an important aspect within the clinical setting related to varying levels of social support that may or may not permit sharing of passwords, mishandling of passwords, and other security issues such as no log-off.

Workflow

In an examination of the workflow of those employees that work directly with the patient population in acute healthcare settings and those that support them in the work that they perform, all employees have a responsibility to maintain IT security within the scope of the work duties (Renaud, & Goucher, 2012). Several themes and recommendations related to the workflow were present in the literature. Recommendation for structure and system enhancement of the workflow and environment presented a potential resolution of current issues and continuing errors

(Alsalamah, Gray, Hilton, & Alsalamah, 2013, Kraemer & Carayon, 2006, and Schwartze, Haarbrandt, Formeier, Haux, & Seidel, 2014). Alsalamah et al. (2013) discussed the aspect of patient-centered care, collaboration, and decision-making and the impact of the workflow on the medical information following an observational methodology study that analyzed cancer pathways. The study focused on the legacy systems with case management as the population. Findings from the observation revealed the need for open information creating a difficult situation for maintaining security. Alsalamah et al. identified six themes necessary for security; (a) Role-based access control, need to know basis for access to information; (b) Fine-grained access control, different positions gain varying levels of access to information; (c) Circle of trust, allowing members with specific levels of access to gain emergent access in specific circumstances "breaking the glass" (p. 814); (d) Persistent control, continually maintain the ability to track information flow by user throughout the life of the records; (e) Dynamic control, the ability to change security and protection levels; and (f) Human-level policy awareness, share policies with users related to level of access and protection. Schwartze et al. (2014) conducted research to find an applicable authentication method for clinical workflows through a systematic literature review. Within this literature review, Schwatze et al. (2014) identified that the system and the user allowed for risk when focused on the clinical requirements specific to workflow. An example of workflow concern is the login sessions that were not logged out allowing for another to gain access. This lack of logging out, either intentional or unintentional is both a system and user issue but not readily resolved by any additional security implementation. In all cases of plans for correction, this is nothing more than adding security to an insecure workflow. The conclusion reached within this review was that the username and password combination is the most practical and secure authentication solution in the clinical workflow process (Schwatze et al., 2014).

Each clinical discipline has a workflow that is unique unto itself including tasks and interventions based on knowledge and expertise within their field of clinical practice. The clinical workflow for the RN includes each of the following: The pattern of RN work in time and motion as it relates to (a) patient care, assessment, medication administration, patient information communication and documentation, (b) charge nurse and preceptor duties, (c) incorporation of clinical devices and technology including the electronic medical record, and (d) other work of the clinical environment as carried out by the RN as part of an assignment responsibility according to policy and procedure or protocol / practice (Kashiwagi, Sexton, Graves, Johnson, Callies, Roger, & Thompson, 2016, Koloroutis, 2004, and Zheng, Haftel, Hirschl, O'Reilly, & Hanauer, 2010). While employees have IT security aspects within the scope of responsibility for their profession and job descriptions, it is identified in the literature that they do not identify a working implementation of that responsibility within the workflow of the duties they perform. Gunawan (2016) discussed the basic concepts to electronic health records being used in nursing practice and the attributes such as ease of use, user friendly, and good performance coinciding with the workflow. Workarounds are a possible outcome of technology implementation and was identified by Rack, Dudjak, and Wolf (2012), who concluded that it should be easier to use the technology that is being implemented than to develop a workaround. The environment and work should support the technology implementation. Zafar, Ko, and Clark, (2014) in a healthcare case study discussed that the clinical staff does not see the IT security as being part of the clinical work. They identify that the clinical staff were busy with clinical patient care and duties related to patient management thus maintaining a perception of the IT security being separate, different, and nonclinical. This qualitative study identified many issues of IT security within the clinical workflow that inhibit the process of accurate use and inclusion of IT security. The perception of the clinical professionals was that they did not have time to incorporate or "worry about" the IT security (Zafar et al., 2014, p. 743). Zafar et al. (2014) discussed the importance of executive management support and empowerment of the team so that IT security becomes a part of the workflow. Engagement of leadership within the organization is critical.

Clinical leadership, decision making, and overall success of the healthcare institution is determined at the executive level by a group of individuals, the Chief Medical Officer (CMO), the Chief Executive Officer (CEO), and the Chief Nursing Officer (CNO). This group must work closely with the Chief Information Officer (CIO) and the Chief Nursing Information Officer (CNIO) to coordinate the electronic medical record and data maintenance of the organization. The CNO and CNIO work in close collaboration with all levels of nursing leadership including the informatics teams and clinical departments to ensure proper flow, management, usage, and functionality are conducted. The CNO and CNIO also work closely with the CMO, CIO, and CEO to ensure and maintain accountability for the organization as being financially responsible for the care provided, the technology used, and patient outcomes (Hebda, & Czar, 2013; Hovenga, & Grain, 2013). Leaders are responsible for creating change but in particular the nursing leader creates a platform for change in nursing practice. Salmela, Eriksson, and Fagerstrom (2012) reported that the knowledge of nurse leadership methods of leading change is through relating, translating, and transforming practice by the roles they play in the change processes. Change requires a continuous learning and reshaping within the organizational culture. Thought patterns restructuring, reshaping of ideas, and movement of change in opinion and value is the basis for the creation of genuine change. Change becomes important as implementation and sustainment of IT security are at the forefront of leadership and organizational goals.

Nurse executives are also prepared in the knowledge of nursing operation at the bedside and in the strategic vision of the healthcare system while moving the informatics implementation into the clinical environment to foster the best patient care and outcome. The nurse executive has to conceptually and operationally know both sides, the clinical plan of bedside care and the vision of the organizational mission, vision, and goals. They become the most knowledgeable of the executive leadership team from a global perspective when integrating informatics within the institution. Sockolow, Rogers, Bowles, Hand, and George (2014) discussed many of the important facets of nurse executive’s communications and considerations for implementation and maintenance of technology and software to assure success. They describe the nurse executive role as critical to interacting with the nurse in decision making and using evidence based systems to combat hurdles faced with technology. One of the nurse executive competencies is that they are a to be a progressive thinker who can predict and/or anticipate the future of nursing practice and the needs that come along with the transitions in practice; this places them in the category of an early adopter of the electronic record and other devices within the healthcare world. As a nurse leader founder of nursing and the first nurse executive, Florence Nightingale documented patient care to track a patient's progress (Kirby, 2015). During the Crimean War, Florence Nightingale considered the patients' needs, projected the best way to meet those needs, and recorded them in patient notes.

Effort Expectancy is associated with how easy it is to use the security practices. Ease of use is determined within the workflow. Within the construct of effort expectancy, the user finds the system to help with clear communication, improve system skill, create ease of system use and make learning easy (Venkatesh et al., 2003). When IT security is part of the workflow and is helpful to clinical care employees are more likely to include the associated behaviors required to carry the security measures out fully.

Risk and Breach

Organizational protection and overall risk management are impacted by the level of security maintenance by every employee. Behaviors that are employed with the use of passwords and the security practices may correlate with the description by Kruger and Anschutz (2013) discussing the access to the electronic patient health information gained either maliciously or nonmaliciously within the organizations. These behaviors and variant accessing of systems as described may be one cause for healthcare to be leading in data breaches as recorded in 2011 among the top 10 industries (Kruger & Anschutz, 2013). IT improvements help to create major advances in the healthcare sector providing improved quality with advances in medical science and reductions in costs, but the down side is increased violation of the security and privacy (Appari & Johnson 2010). Healthcare organizations are increasingly becoming the targets of hacking in the same manner as sought after personal information. Public awareness and concern of hacking are becoming more prominent (Kwon & Johnson, 2014).

The majority of this section will focus on the threat of a system breach due to an unauthorized access of the system or an intrusion of some type to gain information without permissions. I would, however, be remiss if I did not mention the concept of systemic threat that some patients experience. According to Appari and Johnson, (2010) the systemic threat is a threat to patient privacy from those within the organization who are legally accessing the information and using it to the patient's detriment. Examples of systemic threat include using medical information to deny health or life insurance, deny employment, or creating other burdensome financial hardships (Appari & Johnson 2010). Although this threat exists, the focus of threat for the purpose of this literature review will be toward a security breach.

Employee awareness of policy related to IT security is an important aspect of organizational IT security and protection from a breach. There is a great deal of literature related to IT security policy implementation and compliance yet there is little agreement in the literature about what creates compliance and overall organizational security. IT security policy awareness is the individual awareness of the consequences of failing to comply with the organizational security policies (Rotvold, 2008). Security practice is the behavior the nurses use to maintain the security or not, by properly authenticating and maintaining the security of their accounts to protect the confidentiality, integrity, and availability of data (Chopra, 2013). Security risk is influenced by the security practice and is defined as a threat that the password privacy or another access to the account has exposure of a kind including a violation during use due to deviation from policy, protocol, or practice, that has allowed for the threat of harm potentially rendering the system no longer secure (Rotvold, 2008). This process of security deviation allows for breach and renders the organizations system vulnerable to breach from the inside.

The average breach, usually tracked to an insider rather than a malicious hacker, costs an organization approximately $6 million or more for each incident according to the Ponemon Institute ("Cyber Attacks", 2015 & "State of Cybersecurity", 2015). After a surge in healthcare breaches that creates exposure of data for millions of patients, the cost was reported for 2014 by Eddy (2014) to be $5.6 Billion and currently after a five-year study is now reported to cost over $6 Billion ("Cyber Attacks", 2015). Personal information security has become progressively more important with increased public awareness that has been heightened for multiple reasons including increased reporting within the public-sector news reports. People are more affected than ever with numbers increasing over five years from 1.4 to 2.3 million adult victims of medical identity theft ("Cyber Attacks", 2015). The investigative report published by O'Harrow (2012) identified the many vulnerabilities of IT security occurring within the healthcare industry. These included password mishandling, insecure practices, known security access issues that were left unaddressed and wireless device access points that were insecure leaving the organization open for risk of security breach or inappropriate access to the system. Ponemon Institute reports in their whitepapers that the top reasons for healthcare breach remain employee negligence with lost and stolen devices (Eddy, 2014 & “Criminal Attacks”, 2015).

Chopra (2013) discusses controls required for hospital security of which one category is technical and includes seven aspects, (a) filtering of web traffic, (b) e-mail server filters with removal of malicious attachments, (c) patching procedures or automatic patching, (d) anti-virus, (e) controlled PCs and hardware, (f) encrypted storage devices, and (g) restrictive firewalls. If these measures are in place then the other measures such as support services for security access, technical controls to allow for access between groups, security teams dedicated to specific work and response, and management team members that are responsive to IT security will all supplement a successful security program (Chopra, 2013).

With the recent hacking of Anthem, one of the United States largest Health Insurers, the American people are even more aware of vulnerabilities regarding personal information and health information (Abelson & Goldstein, 2015). Information from approximately 80 million records was available to the hackers once they hacked into the Anthem system. A phishing scam was used to access the credentials of five employees from Anthem as reported by Amerigroup, the operating company of Anthem (Balbi, 2015). Similar reports were reported by Verizon in the 2011 data breach experience where phishing emails were opened and malware infected the executives’ laptops allowing access to the system (Baker, Goudie, Hutton, Hylender, Niemantsverdriet, Novak, & Ostertag et al., 2011).

Access to health records is more desirable than gaining access to general credit accounts because the files from health records contain more information such as Social Security numbers, birth dates, addresses of the individual and significant others, employment information, emergency contact information, and other personal information. A collection of such personal information allows for rapid high-level identity theft. Finkle (2013) discussed that Dell Secure Works identified in a recent report that hackers can sell complete health insurance credentials for $20 per set of data as opposed to $1 to $2 for each credit card number with a security code in underground markets. Because there is a rapid high return when monetized with great profit for health information over credit card data sets up to $20 or more as opposed to $1 to $2 when sold in the underground, a very strong interest in sales of this information creates. The healthcare organizations are more inviting targets for hackers and social engineers because of the ease of breach and significant profitability. Finkle also discussed the statements by the Federal Bureau of Investigation (FBI) warning that healthcare remains vulnerable to cyber-attacks.

Healthcare costs in the United States were at 17.4 percent of the gross domestic product in 2013 according to the Medicare and Medicaid Services (2014). These healthcare costs include the burden of technology costs, security, and breach recovery. The economic impact to the average organization costs $2,134,800 per organization based on a calculation of an average of five attacks annually (“Criminal Attacks”, 2015).

Most organizations report they are not confident they will be able to detect data losses in the event of a breach. Response to security incidents is an obligation of the security management team within the organization. Effective incident management is critical to the reduction of threat impact to an organization. Ahmad, Hadgkiss, and Ruighaver (2012) identify that the response process consists of five main practices, namely “preparation for, identification, containment, the eradication and recovery from incidents” (p. 643). Improvements in process related to the IT security in the healthcare arena would allow for a potential impact of cost reduction, patient safety, and patient satisfaction. Provided the employees were engaged within each of the four constructs that lead to use behavior the resulting change in security protection would ultimately position healthcare for cost reductions as a result of the decreased breach and risk. Agaku et al. concluded that increased strategies are calling for higher security for the protected health information so that the trust of the information security will not be undermined any further. Recent public reports of security breaches within the healthcare insurance companies’ serve to continue the media surge that will raise general citizen concern that hospitals are more at risk causing lack of confidence. The general public is concerned with privacy and their general security of the information. The Federal Governments Office for Civil Rights at the Department of Human Services reports that over the last five years there were 740 major security breaches within healthcare that affected 29 million people (Abelson & Goldstein, 2015). Increasing the security within the healthcare organizations creates a more confident feeling for patients individually and extends to the global public who become more comfortable. Rapid and constant changes within healthcare require a continual reassessment of security status (Chopra, 2013). The work of identifying one population’s perception with gained insight and potential for improvement of the IT security behavior and handling of security practices may become the catalyst to some of the change that is needed in healthcare security processes related to IT management that will promote increased patient confidence.

Summary and Conclusions

In this chapter, there has been an incorporation and presentation of review of the literature staging a foundational frame for this work. An overview of the search and review of literature collection procedures were presented. The conceptual framework was developed from the work of Rogers (2003 & 2004) through to the model of UTAUT (Venkatesh, 2003). The four core constructs that influence behavioral intention to use technology within UTAUT have been highlighted for use and were discussed within the literature; they include (a) performance expectancy, (b) effort expectancy, (c) social influence, and (d) facilitating conditions. A review of the supporting literature was conducted for each of the following categories, information security in healthcare, IT security, nurse awareness, policy and penalty, password management, workflow, and risk and breach.

Connections to social change include increased knowledge and understanding of impacts to social change following the literature review. With dramatic costs to healthcare organizations and 2.3 million adult victims of medical identity theft annually there is a place for change. Moving into Chapter 3, I will discuss the research design, development of the tool, data collection methods, and methods for data analysis. Chapter

4 will include the discussion of techniques used for analysis of the data and emerged findings in relationship to the research questions. Chapter 5 will incorporate discussion of the areas for future research, implications to social change, and closing remarks.

Chapter 3: Research Method

The purpose of this qualitative case study was to explore the perceptions of the RN within four of the constructs of the unified theory of acceptance and usage of technology (UTAUT) that are specific to use behavior (Venkatesh et al., 2003). The experiences and perceptions of the registered nurse (RN) were analyzed as they related to the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions. I formulated a research plan to conduct independent analysis as themes emerged within each construct. The research methodology is set forth in Chapter 3.

This chapter includes discussion of the research design that was used to conduct this study. The role of the researcher, methodology, and the issues with trustworthiness are each included in the research design. Within the methodology section a detailed review of participant selection, instrumentation, expert panel review, procedures for recruitment of the participants and their participation, data collection methods, and the data analysis plan are each discussed in detail. Targeting the issue of trustworthiness for exploration to confirm the credibility, transferability, dependability, confirmability, and ethical procedures intended for use within the study procedures are reviewed.

Research Design and Rationale

In Chapter 2, the literature review provided a grounded base supporting the importance of maintaining information technology (IT) security and the behaviors associated with it that are essential to healthcare organizations. The purpose of this qualitative case study was to explore how RNs perceive IT security behaviors in acute care hospital settings based on the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions. I asked the following overarching research question for this study: What are RNs' perceptions, expressed intentions, and self-reported behaviors of IT security?

The following research questions were used to provide the supportive data designed to guide the work of this research using the four constructs of UTAUT that are consistent with behavioral intention and use behavior:

RQ 1: What are RN perceptions, expressed intentions, and self-reported behaviors of the performance expectancy of IT security practice?

RQ 2: What are RN perceptions, expressed intentions, and self-reported behaviors of the effort expectancy related to the IT security practice?

RQ 3: What are RN perceptions, expressed intentions, and self-reported behaviors of the social influence related to the IT security practice?

RQ 4: What are RN perceptions, expressed intentions, and self-reported behaviors of the facilitating conditions of the IT security practice?

A qualitative case study design was used to determine the perceived experiences of the RNs recruited for this study. Merriam (2014) discussed that the value of a qualitative study allows for the meaning of the problem being studied to be viewed within the research as the user sees, experiences, or understands his or her world. The qualitative study allows for interviewing the employees of the organization thus providing insight into the RNs' perceptions, expressed intentions, and self-reported behaviors of the IT security and while using the constructs of UTAUT to guide the research. The qualitative case study with interviewing is a design more suited to this set of research questions as I was seeking information related to the perceptions, expressed intentions, and self-reported behaviors of the RN. Each of these attributes was discussed in various themes that could be missed if other design methodologies would have been used.

Other research designs available in the qualitative domain do not provide the same depth for rich exploration within the case review. A phenomenological design would allow the gathering of information but would limit the view of the clinical aspect of interaction (Marshall & Rossman, 2016) one that is not optimal for the RN perception of the world. The ethnographic design would have looked at the cultural behaviors according to Marshall and Rossman (2016) and that would not have fulfilled the research questions. The grounded theory would be used to find a new discovery or underlying theory as described by Merriam (2014) and was not a correct fit for this work.

Role of the Researcher

As the researcher, interviewer, and observer, it was important to examine and be aware of personal experience and potential conceptual ideas already framed related to the planned research. Podsakoff, MacKenzie, & Podsakoff (2012) discussed that it may be necessity to consider the development of controls measures by multiple contributors to avoid risk for bias based on individual tendency for word choice or item formation. Including other field experts in development along with a thorough examination of self-perceptions is essential to a well-developed study.

The interest in IT security by RNs has intrigued me for as long as the electronic systems have been in place in the hospital setting. I have been a manager who has dealt with the consequences of poor conduct in IT security practice and related outcomes that are impactful to the organization, patient, and employee. In the past, I had believed managing staff who were noncompliant to comply with IT security in a hospital setting was unavoidable because the scope was so large and perhaps unmanageable. As time has passed and technology, security systems, base knowledge, and employee training has improved there are known ways and best practices that lead to strongly secure environments in many industries. Healthcare is not in line with other industries in the level of security connections with employees and, as this became evident through the literature, I became intent on exploring the RNs' perceptions, expressed intentions, and self-reported behaviors of IT security while practicing in the acute care hospital setting.

My role as the researcher took place with RNs who were part of the Three Rivers Chapter AACN professional nursing organization and practiced in the clinical setting. My continuous interest in the research was maintained in two realms, doctoral research and nurse executive knowledge. The recruitment of participants was targeted and criteria based with specific qualifications for inclusion. The criteria that was used for inclusion served to eliminated the possibility of including any direct subordinates or RN employees who I have influence over employment.

Methodology

This research study was conducted as a qualitative case study in the Pittsburgh, Pennsylvania region. Volunteers were recruited from a professional nursing organization using criteria based selection for participation. Interviewing methods for data collection, usage of NVivo v11 for data maintenance and analysis, and conducting relational application to UTAUT to operational findings were the procedural strategies used in this study and are described in this section.

Setting

The professional nursing organization Three Rivers Chapter of American Association of Critical Care Nurses (AACN) agreed to provide access to their membership. I recruited potential candidates for interview from this professional organization. The Three Rivers AACN had provided a letter of support (Appendix B) following IRB approval. The Three Rivers Chapter AACN has many nursing members who participate in the Beacon Award and nurses are eager to participate in research. I was hopeful that the keen interest to participate in research by the RNs related to Beacon would create an overzealous response to participate in this study. The potential for strong interest in research was one additional reason for the need of selection criteria.

Participant Selection Logic

The population that was used for this study came from the membership of Three Rivers Chapter AACN. The total membership includes 224 RNs from the Pittsburgh, Pennsylvania and the surrounding region. Request for volunteer participation was made through email to membership contacts with an invitation to participate. The invitation to participate outlined the specific criteria required for participation. Identification of participants' verification of meeting criteria was made at the point of initial contact with me based on a self-report of an RN role. Participants who were selected self-reported to be RNs who met the following inclusion criteria: They (a) were a member of the Three Rivers Chapter AACN, (b) worked full time in a clinical environment, (c) had been oriented to the work environment, (d) had authentication (sign on) had privileges to the electronic record in their work environment, (e) had access to the work policies and (f) were willing to participate in the study.

The participants interested in the study were contacted for recruitment to this study by e-mail as the initial contact. Access to the membership with contact information attainable through Three Rivers AACN membership contact list and provided to me by the individuals occurred once consented by the organizational administrative representative of the professional organization (Appendix B). The initial contact to the potential participant included a cover letter that served as an invitation to participate including a description of the study intent and objectives with sample questions that would be included in the interview. There was additional information for participation available if the individual wanted it. The invitation to participate used to recruit participants for interview was submitted to the IRB. The initial membership access and fliers were provided as the initial contact to individuals. All follow-up communications were conducted once the relationship was formally established between me and the member.

Participants were interviewed to a sample size of 20 with saturation reached. Saturation is defined as the time in the data collection process of the interviewing in which there are no new concepts being brought forth or considered absent from what has been being collected of those being interviewed (Fusch & Ness, 2015). Face-to-face interview methodology was used. The interview is appropriate to understand the lived experience of the individuals by listening to their stories. Face-to-face interviews were conducted for the purpose of obtaining data related to the particular phenomenon of this topic. Seidman (2013) discussed that the interview allows an exploration of a potential emergence of new content and findings. I expected to discover new findings. The interview questions were posed in an unbiased manner using interview techniques that are specifically crafted to maintain uniformity and objectivity. I maintained a neutral manner during the interview process allowing for active listening throughout each interview session. Each interviewee was allowed the opportunity to answer all items and to provide any additional insight into the content matter of IT security behaviors.

Informed Consent

Informed consent was described within the cover letter requesting participation. Once the potential participant expressed interest, I met face-to-face with the potential candidate, explained the research and obtained informed consent. Informed consent as described by Halse and Honey (2014) is the process of providing clear, well-defined, and truthful information about the research. Informed consent is voluntary and must be provided of free will by the participants. The informed consent must also address any potential for distress or discomfort (Halse & Honey, 2014). I did discuss with participants that I would keep copies of the participants informed consent documentation. I then answered any questions that participants had by providing contact information. The participant received a copy of the informed consent document. The prospective participant was provided my contact information and was encouraged to make contact with any questions prior to or following our scheduled interview. Participants were provided the opportunity to opt out or withdraw from the study up to the point of post transcription verification (member checking) and prior to data entry into NVivo.

Instrumentation

A scripted questionnaire was used for direction during the interview. The questionnaire allowed me to remain on topic and unbiased without missing essential content, yet the open-ended questions allow the interviewee to answer with openness related to his or her lived experiences. During each of the interviews, a basic audio recorder was used so that the interview could be transcribed following the interaction. Confidentiality of the interaction was discussed with the participant to allay any concerns prior to the use of the recorder.

Procedures for Recruitment, Participation, and Data Collection

Recruitment for the study was voluntary and criteria based with self-reported verification. The RNs who volunteered to participate in the study and met the criteria of being a member of the Three Rivers Chapter AACN, working full time in the clinical environment, having been oriented to their work environment, having authentication (sign on) privileges to the electronic record in their work environment, and having access to their work policies were invited to participate. Following a participant's agreement to enroll, I met with that individual to obtain informed consent and schedule the interview. Once informed consent was obtained, scheduling for the meeting time and place for the face-to-face interview with me occurred. My contact information was provided so that the participant was able to contact me to answer any questions they may have had related to logistics or the study. Once enrolled to participate, each participant was assigned a unique code (ex. RN1, RN2, RN3, etc.) for identification. Private space that was convenient for the member was provided for the interviewing session.

As the primary researcher, I conducted the interviews and collected the data. Initially, there was a brief inquiry and collection of demographic data to align with the literature that has been established including variances between male and female, age, and educational preparation that have been shown to have a relationship to adoption of technology and change. These demographic items may also play a role in the alignment to the construct themes of UTAUT toward use behavior.

Each interview was expected to last approximately 30 to 45 minutes. Each session was done in person with handwritten notes taken during the interview and an audio recording made of the session. Following the interview session, the audio recording was submitted to a secure transcription company to be fully transcribed to a word document. Following transcription, member checking was conducted. The member checking is a process of participant review of their transcribed interview to assure accuracy of information. The member checking allows the interviewee to verify that the information transcription is as accurate as possible (Harper & Cole, 2012).

Following member checking the data was input to NVivo v11 software for analysis. The data collection of all interviews was conducted over a period of 3 months to reach saturation. During that period, I made a second outreach to the membership with requests for participation targeting additional participants within the professional organization.

At the conclusion of the interview, participants were thanked for their participation and offered a contact number if they had any questions that arose following their departure. All information gathered in the face-to-face interview were to be transcribed verbatim into documents and stored into a secure computer program. Participants have been made aware of study results and presentations of the study through the Three Rivers Chapter AACN.

Confidentiality was assured to the participants upon agreement to engage in the study as part of the consent process. The participant was provided with my contact information upon enrollment. My contact information was provided for the key purpose of contact in the event of a question but also in the event of the participant desiring to exit the study. A participant was afforded the possibility to exit the study at any time for any reason. The exit would be completed by contacting me to opt out.

Data Analysis Plan

Data analysis was conducted using NVivo v11 qualitative data analysis software. The data was input to the program from the interview observations, researcher notes, and transcriptions following the audio recordings and member checking of the interviews. Headings were used for theme development to capture key areas of concepts that emerged. Several rounds of coding were required to identify the categories of themes (Bazeley & Jackson, 2013). The themes represent the interviewees lived experiences related to perceptions, expressed intentions, and self-reported behaviors of IT security. Bernauer, Lichtman, Jacobs, and Robinson (2013) discussed that NVivo provides a model for researchers that allows them to use critical thinking processes in applications and presentation of data and conceptual relationships.

The type of coding that I performed was labeling and chunking of information categories as themes emerge. With the use of NVivo the natural language processing was used on text transcriptions to assist in the determination of themes along with the researcher determination and coding. Crowston, Allen, and Heckman (2012) discussed the advantageous and cost effective nature of natural language processing when used in qualitative research processes. Their work highlighted aspects of coding to include conceptual coding of emotional expressions, positive politeness, and negative politeness and the importance of capturing this information within the bracketing of information. According to Tufford and Newman (2012) and Sorsa, Kiikkala, and Astet-Kurki (2015) bracketing is used when personal experiences may trigger preconceptions about the information being collected. By using bracketing throughout the collection of information and coding process awareness is maintained. This information is being stored in NVivo.

The researcher is responsible for acquiring the appropriate level of interpretive data from the interview that is fundamental in qualitative research (Merriam, 2014). When discrepant data is identified and is associated to a case interview that case would be excluded from the analysis and the inclusion for saturation. The study credibility was strengthened by assuring that these measures are were place.

Issues of Trustworthiness

Credibility

The qualitative case study method allows for construct validity through evidence established from a chain of multiple sources, member checking, pattern matching, explanation building and using logic models (Amerson, 2011). Internal validity was supported with saturation. According to Fusch and Ness (2015), saturation is reached when there is no new information, no new coding, no new themes, and an ability to replicate the study and this must be in place to enhance the validity of the qualitative study.

The interview questionnaire was submitted to an expert panel of four individuals who were experienced and respected as knowledgeable and proficient in informatics science and technology. Each of the panel members were invited by email (Appendix C) to review the 31 questions that had been developed for relevance to the study, appropriateness to the topic, accuracy in content, and clarity to the population. Two clarity issues were identified during the initial review. Those issues were corrected. Following the corrections, a resubmission of the interview questions (Appendix D) was circulated to the expert panel for final review and approval. Expert approval was granted by all members of the panel. Validating the questionnaire through the use of an expert panel lends credibility to the process of qualitative research (Bengtsson, 2016).

Transferability

The external validity of this qualitative case study was supported by using the constructs of UTAUT as the foundation for the research questions. The use of UTAUT allows for an established protocol incorporated into the study design (Amerson, 2011). The framework of UTAUT and each of the constructs being used within this research study were established and validated thus support the work as proposed in this research study. Thomas and Magilvy (2011) discussed the transferability of a study as applying research findings from one group or population to another. The findings from this study were expected to have applicability to other clinical populations within the healthcare arena.

Dependability

Dependability was assured through comparative hand notes taken by the me and the audio recording that was transcribed verbatim by a secure transcription company with repeated review following transcription. I conducted those repeated reviews of the audio recordings. The purpose of the repeated reviews was to improve interpretation and identify cues related to the lived experience that had been shared during the interview. I input all elements of data collected, researcher notes, audio recordings, transcripts, etc. into NVivo v11 software that provided assistance to me in determining accurate and dependable results.

Confirmability

Confirmability, sometimes considered neutrality of the qualitative study, was achieved when each of the following had been addressed according to Noble and Smith (2015); (a) truth value, (b) consistency, and (c) applicability. Links, philosophical positions, or experiences associated to me functioning in the position as the researcher and were not revealed throughout. Tufford and Newman (2012), and Sorsa et al. (2015)

identified that bracketing supports increased reflexivity by the researcher when conducted thoughtfully.

Ethical Procedures

The nine procedures of this research were conducted within the framework of approval under the Walden University Internal Review Board (IRB). Permission to conduct this study was granted under IRB number 07-22-16-0232839 with an expiration date of July 21, 2017. Within this approval informed consent was approved as described. All participant recruitment and data collection commenced following the approval of the research by the IRB.

Confidentiality was assured to the participants upon agreement to engage in the study as part of the consent process. The professional nursing organization participation provided for members from many areas within the region to participate. Various locations of office settings that were both easy to access and not identified as specific to any identified organization or hospital were made available for use as the interview locations creating an anonymous setting. The site was neither the same location as the professional organization nor their workplace. Data collection occured through the interviews with audio recordings and journal notes resulting in transcripts and electronic data entry. All data (transcripts, recordings, journal notes, and any other electronic data) are stored in a secure location in which all data is securely housed (external drive/password protected). This measure allows for increased security, anonymity, and confidentiality for the participants. Data handling and maintenance procedures were discussed with participants in full disclosure and transparency. The transcribed information from the interviews were stored in a secure computer environment. The participant codes, consents, meeting schedules, and any other data collected were housed in a locked area that only I have access. This data will be maintained for a period of 5 years. The destruction of contact information occurred following the completion of study and before the formal sharing of those results at professional forums.

Summary

This chapter included a presentation of the research methodology and design for this qualitative case study. The purpose of the study and research questions were presented continuing to guide the study. My role as the researcher was reviewed along with the relationship to the research participants. Access to the population, protection of that population, and treatment of information including management of all data maintenance was detailed. Interview procedures were reviewed as the method of data collection, followed by data analysis and assurance of rigor. In Chapter 4, I discussed the data analysis procedures and presented study findings that included the labeling and themes that emerged from the case studies as they relate to the research questions. Finally, Chapter 5 addressed the interpretations, implications, and potential applications of the findings along with limitations and conclusions of the work, as well as identified future research. Implications for social change are incorporated into the final discussion.

Chapter 4: Results

Introduction

The purpose of this qualitative case study was to explore the perceptions of the registered nurse (RN) within four of the constructs of the unified theory of acceptance and usage of technology (UTAUT) that are specific to use behavior (Venkatesh et al., 2003). Gaining insight into the lived experiences of RNs related to information technology (IT) security was at the heart of this study. The experiences and perceptions of the RN were analyzed as they relate to the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions. Using the UTAUT model as the theoretical framework, the following overarching research question was used for this study: What are RNs' perceptions, expressed intentions, and self-reported behaviors of IT security?

Using the four constructs of UTAUT that are consistent with behavioral intention and use behavior, the four following research questions were used as supportive to the overarching research question:

RQ 1: What are RN perceptions, expressed intentions, and self-reported behaviors of the performance expectancy of IT security practice?

RQ 2: What are RN perceptions, expressed intentions, and self-reported behaviors of the effort expectancy related to the IT security practice?

RQ 3: What are RN perceptions, expressed intentions, and self-reported behaviors of the social influence related to the IT security practice?

RQ 4: What are RN perceptions, expressed intentions, and self-reported behaviors of the facilitating conditions of the IT security practice?

In this chapter, I present the data analysis with results. The data collection and analysis were derived from 20 RNs who met the requirements of participation, including that the individual was an RN and also a member of the professional organization Three Rivers Chapter of the American Association of Critical Care Nurses (AACN), worked full time in a clinical environment, had been oriented to the work environment, had authentication (sign on) privileges to the electronic record in the work environment, and had access to the work policies. Each of the participants shared through an interview their experiences and information of those lived experiences related to IT security in the clinical area of which they were employed. The results include insight from direct quotes of the participant interviews. Exploration of the participants' relationship with and knowledge of IT security as their lived experience has yielded multiple findings related to the RNs' use of IT security in relation to the research questions with underlying similarity to research premises in quantitative studies presented in the literature review.

Research Setting

The face-to-face interviews were held in meeting spaces that were available to me and conveniently located for the participant. All sessions were held in locations that provided privacy for the participants' protection and quiet for recording purposes. One participant requested to meet at her organization prior to her work shift, otherwise all meetings were held away from the workplace organizations at public office or meeting locations.

Influences that may have impacted interviews include two participants scheduling interviews following their 12-hour shifts and two scheduling interviews immediately prior to their shifts of work. In the first situation when the interviews were held following a shift, the participants could have been tired or anxious to finish quickly. It was possible they might have just wanted to get home, although in both cases, the interviews were similar in length to all the others. In the second scenario where they were scheduled prior to their shift, they might have been nervous about getting to work on time. In both of these cases, they were relaxed during the interview and conversed openly without giving the impression that they were hurried.

Participant Demographics and Sampling Strategy

Following AACN approval through the Letter of Agreement (Appendix B) and IRB approval, emails were submitted to AACN members through the connections feature, fliers were circulated, and announcements were made at the local monthly meetings to garner participation from the purposeful population of the local AACN chapter, Three Rivers Chapter AACN membership. The initial call for participants resulted in 14 responses over 2 months. A follow up request was made that afforded an additional six responses. Several members were interested in participating but did not meet the criteria for inclusion because they were fully immersed in an educational or management position and not currently practicing in a clinical area. The criteria for participation included that the individual was an RN and also a member of the professional organization Three Rivers Chapter AACN, worked full time in a clinical environment, had been oriented to the work environment, had authentication privileges to the electronic record in the work environment, and had access to the work policies.

Those who participated in the study came from the Three Rivers Chapter AACN that has over 224 members, with about 30 members actively participating in monthly meetings. The members come from various hospitals and hospital systems from the tristate area of Western Pennsylvania, Ohio, and West Virginia. The RNs who participated in the study came with a wide range of experiences although not included in the demographic data. Some were lifelong critical care RNs, others had experiences in many different clinical settings. Some had been staff nurses throughout their career, and others had various specialty or management experiences in their past. I did not collect these types of details within the demographic details. The demographic data were purposefully kept to a minimum to maintain anonymity. Following the introductory discussion, the demographics were discussed. Each participant was given an option to opt out or to share the demographic information that included (a) their sexual identification as male or female, (b) the age range group that they fit into, (c) the highest RN education that they had received, (d) the highest non-RN education they had received, and (e) the years they had been employed as an RN (Table 1).

Table 1

Participant Demographics

Participant	Sex	Age group	Highest RN education	Highest non-RN ed.	Years RN employment
RN 1	F	26-35	BSN	—	5
RN 2	F	56-65	MSN	—	39
RN 3	F	66+	MSN	—	50
RN 4	F	56-65	MSN	—	28
RN 5	F	26-35	Diploma	BS	2
RN 6	F	56-65	MSN	—	35
RN 7	F	26-35	BSN	—	7
RN 8	F	46-55	BSN	—	27
RN 9	F	46-55	BSN	BS	30
RN 10	F	46-55	BSN	LNCC	8
RN 11	F	26-35	BSN	—	5
RN 12	F	46-55	BSN	—	28
RN 13	M	26-35	AD	BS	2
RN 14	F	56-65	BSN	—	37
RN 15	M	36-45	AD	MBA/HMS	10
RN 16	F	56-65	Diploma	—	37
RN 17	F	46-55	BSN	—	31
RN 18	F	26-35	BSN	—	4
RN 19	F	46-55	Diploma	—	28
RN 20	F	26-35	BSN	—	5

Data Collection

Data collection was conducted as approved by the IRB to fulfill the study requirements. A targeted approach was conducted for recruitment of participants from the Three Rivers Chapter AACN professional nursing organization using email contacts, fliers, and chapter newsletter articles. Recruitment for the study was voluntary and criteria based with self-reported verification. The 20 RNs who volunteered to participate in the study met the criteria of being a member of the Three Rivers Chapter AACN, working full time in the clinical environment, having been oriented to their work environment, having authentication privileges to the electronic record in their work environment, and having access to their work policies. Following a participant's agreement to enroll, I met with that individual to schedule a meeting time and place. During the scheduled face-to-face meeting following a brief introduction, I conducted an explanation of the research, reviewed the informed consent with provision for questions and clarification, and obtained signed consent for participation. Once informed consent was obtained, the face-to-face interview began.

My contact information was provided so that the participant would be able to contact me to answer any questions they may have related to logistics or the study. As each participant was enrolled he or she was assigned a unique code (ex. RN1, RN2, RN3, etc.) for identification. This code was cross referenced on a master list that only I maintained. The voice recording and any other records of the interview, including my interview notes were recorded using the candidate's unique code only. The candidates were instructed on the privacy coding and security of data management. They were given the information about the transcriber being the only other individual receiving the recorded file that would be identified only by the assigned unique code.

Prior to recording the interview, I collected demographic information from the candidate. Following the initial conversation and demographic questioning, I waited until the candidate was generally exhibiting a sense of being comfortable. I then conducted the interview, both recording the session and taking researcher notes as data collection methods. The 20 interviews lasted between 26 and 38 minutes. Following each of the interview sessions, the audio recording was transcribed verbatim to a word document by a secure transcription company. Upon return of the transcribed document, I reviewed it for any major errors and then forwarded it to the candidate so that member checking could be conducted. The member checking process for most participants did not require any changes. However, two participants, RN 17 and RN 19 had several requests for changes to their documents that were made through multiple rounds of review. Harper and Cole (2012) discussed that member checking is the method of assuring accuracy of the transcription when allowing the interviewee to review the document. Following completion of member checking, the data were input to NVivo v11 software for analysis.

The data collection from interviews was conducted over a period of 3 months to reach saturation and volume. Neither the minimum number of participants, nor saturation was reached with the initial call for participation so a second round of targeted recruitment occurred. Following the second recruitment effort there were enough interviews accomplished to reach both minimum number of participants for the study and saturation.

Once the recording of an interview was concluded, the participant was thanked for his or her participation and offered a contact number in the event that he or she might have questions or would decide that they wanted to withdraw from the study for any reason following the departure. Each participant was reassured of his or her privacy, understanding the data would be maintained for 5 years with the electronic files being encrypted and along with other files be locked in a secure location. Each participant folder that is identified with a unique identifier maintains my individual notes. Those folders are locked securely along with all other paper materials and the encrypted drive of files (voice recordings, excel. NVivo) from this study.

Data Analysis

I used inductive and deductive coding for data analysis. I first used coding that aligned with the UTAUT theoretical framework that the research questions were based upon and the general area category titles of the topics of questions included in the interview. Then I went back and identified additional themes that were emerging from the response text naming codes into categories of similar content. I linked the codes following the two sessions of coding to identify like nodes and classifications of codes allowing for a comprehensive and thorough coding of the data. This coding effort identified predetermined nodes and emerging nodes resulting in a total of 62 nodes. Detailed assessment and further coding allowed for the combination and coordination of primary themes and subthemes (both parent and child nodes) and was finalized into 42 nodes with eight parent nodes or primary themes within NVivo v11. Six of the eight parent nodes have UTAUT constructs that correspond with the nature of the parent and child nodes (Figure 3).

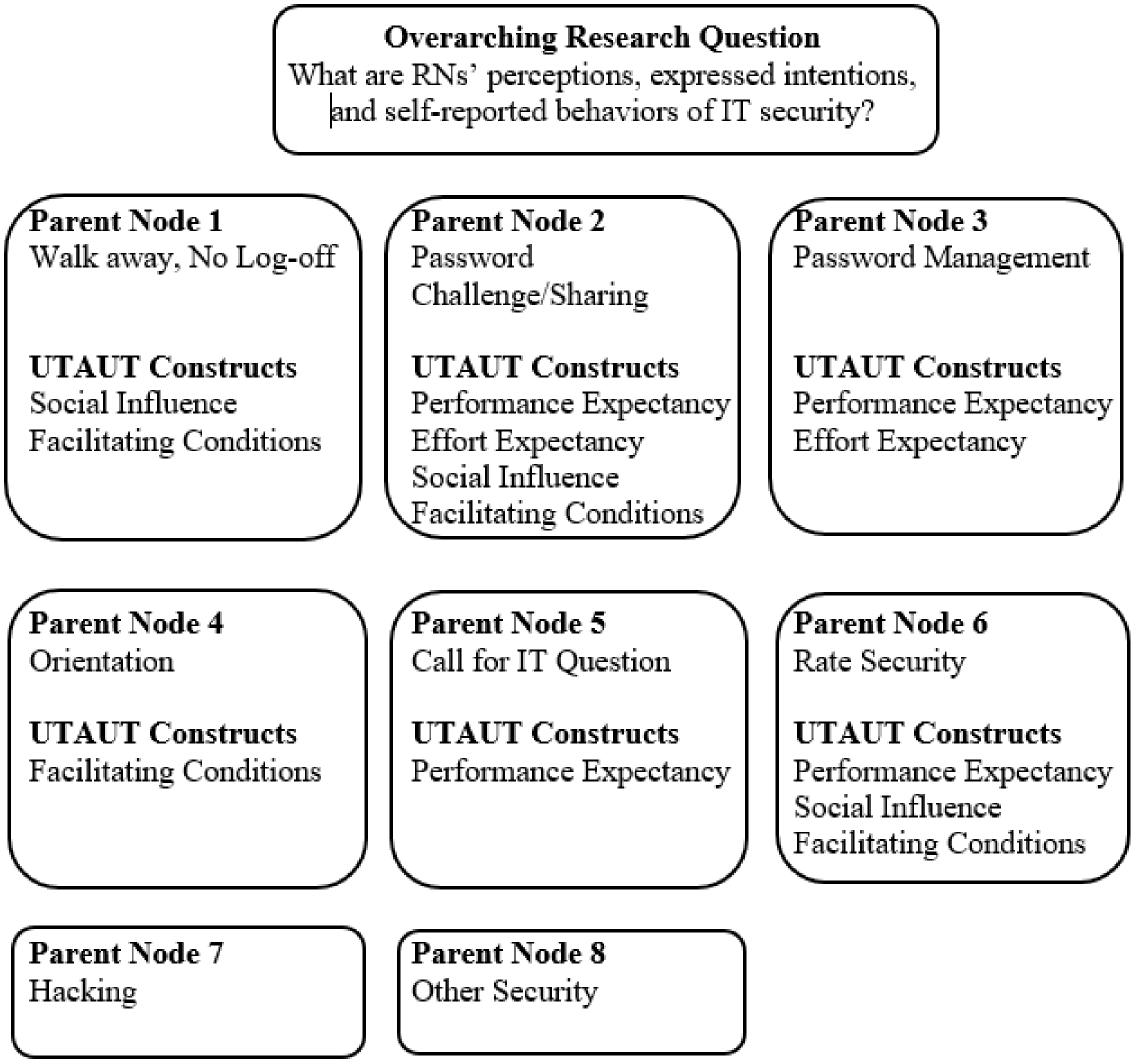


Figure 3. Parent nodes and associated UTAUT constructs. Parent nodes identified and compiled with UTAUT constructs during data analysis to identify findings for the answer to the overarching research question.

Each of the primary themes and subthemes is presented with a representation of participant quotes to represent the findings within that theme or subtheme development.

Primary Theme 1: Walk Away No Log-Off

Computer log-off was discussed in the literature review as an important aspect of IT security presented as a potential for lack of understanding or connection with IT security. Albarrak (2012) discussed that 16% of the nurses allowing for others to access confidential information under their authentication was because they did not log-off of the system. The lived experience of this sample is that walking away from the computer without log-off is a reality as part of the regular workflow. Samples of participant responses are presented in Table 2.

Table 2

Primary Theme 1: Walk Away No Log-Off

Participant	Response
RN 1	“I think that nurses are always pulled in a couple of different directions at one time. So, you’re doing multiple things. Whether you have a computer actually in the room and you walk away from it or it’s a computer at the desk and you end up walking away from it due to family, call bells, doctors, grounds, I mean times of different scenarios. But I have been guilty.”
RN 11	“Pretty much all the time. Constantly if I have to run to a med room because I was getting medication and I forget to grab a medication. To go in and say for example maybe I work in the ICU. So, if a patient is starting to wake up then attempts to self-exacerbate or something crazy like that, like fly right in the room. So, pretty frequently.”
RN 15	“Oh! They are several, I work in the ICU. So, I'm constantly called away to answer a monitor or a colleague and there some pretty important things we have in the IUC to answer this quickly. So, I’d say during shift I'm probably called away without logging off my computer at least 6 times.”
RN 9	“Only usually during an emergency. Like if something they might have a patient jumps out of bed and you got to catch them or something on the monitor. But other than that, I usually log off.”

Participants described the desire to log-off believing it was the correct process but that it was not part of their regular workflow. Three respondents stated that they do log-off but they went on to describe situations that occur causing situations with an inability to log-off.

Within this first primary theme there were six subthemes to emerge. They include staff awareness of safeguards in place to protect them if they walked away from their computer and left it unattended, did those safeguards inhibit patient care, were they aware if anyone had ever used their account, what was the unit norm for log-off, what did they think others reasons were for not logging off, and did it make a difference if the computer could be seen. Examples of participant responses are shared in Tables 3 - 8.

Table 3

Safeguard for Walk Away

Participant	Response
RN 2	"I do know that the computer does log off, after a period of time, but I don't recall what that period of time is. Because I know that, if I don't utilize the electronic medical record for you know some period of time it just automatically logs you off. So, I don't know the exact time but there is some type of safeguard."
RN 5	"I know our system does log you off after a certain amount of time, and it will lock it for you. But I'm not sure of the amount of time that is."
RN 6	"Yes, after a time period the computer goes into a, like shut down mode or it logs me off automatically."
RN 7	"I know like it goes to a screensaver that locks out, but I don't know how long, like what the actual time is."

Sethi, Lane, Newton, Egan, & Ghosh (2014) discussed that the clinical desktop at the nursing station is a source of potential breach and is best to have an auto log-off. The RNs were aware that there was a safeguard but they did not know the timing nor how it actually worked. A few included that the feature was more of a hindrance to their care than a help. They discussed that because it had such a rapid lock out feature that they were then required to login again quite regularly throughout the shift causing wasted time. This created the next theme of Walk away safeguard inhibiting care.

Table 4

Walk Away Safeguard Inhibits Care

Participant	Response
RN 1	"I'm at the patient's bedside and then all of a sudden it's already logged off. So, I guess those are good things. Sometimes they delay care because you're constantly logging back in when you're at the bedside."
RN 10	"I think maybe if the screen would not time out, I could give better care. It is a distractor."
RN 16	"Sometimes they delay care because you're constantly logging back in while at the bedside."

Gaining insight into the RNs understanding of what happens during that period of time while the computer is unattended and logged in under their authentication credentials was provided during discussion with these elements. They each discussed what happens while they are not logged off and away from the computer, had anyone used their computer. Many of the nurses responded in a way that signified an emotional strong interest to discuss this topic. They were open to discuss situations demonstrating that accounts could easily be used between people and electronic signatures would be intertwined. They discussed the risks of this documentation, authentication of wrong types of accounts such as physician for nurse and vice versa, and the general risk of access to information that is not appropriate. They expressed passion and interest for detail as they engaged in their recounts of situations related to account use and misuse. Two respondents were very concerned about the "trouble" (discipline) they would face because they were looking at records they should not be viewing.

Table 5

Someone Used My Account

Participant	Response
RN 13	"Yes, like if you logged on and you might walk away for a second somebody just wants to print out a clinical note or other clinical doc."
RN 5	"Yes, some just jump on the logged-on computers if you might walk away for a second when they just want to view labs or clinical info."
RN 8	"Yes, because I've come back to the desk and found doctors using mine, like where I haven't signed out and my name is still on the computer. I make them log off, log back in under their own name."
RN 8	"Yes, and they were looking at patient records which that's not my patient that I'm caring for and I can get in trouble."

Each participant was willing to discuss the unit norm and while they generally began their discussion with the unit norm is to log-off, they would quickly follow up with reasons why their peers did not log-off on a regular basis. With probing into this matter of log-off, they would describe that there was widespread variation in log-off procedures within their unit setting.

Table 6

Unit Norm: No Log-Off

Participant	Response
RN 2	"In some cases, if someone is taking care of their patient they may have their WOW at the door and then they go and take care of the patients but without logging off. Sometimes they, will have their screen still be out, but they will go and get medicines, they will go and get any patient care supplies. So, it's not consistent, that people log off as soon as they walk away from the screen. It's like up, with the patient's information there it may not be facing a common area, sometimes it is, sometimes it's not. So, I can definitely see kind of a mix of both, where screen has been facing public areas, and the screens where, times when the screen is not facing public areas. I guess kind of a little bit of both distraction, thinking about their next task that they have to do rather than you know logging out and securing the computer before they leave."
RN 7	"I would say more often than not people are not logging off, it just depends I guess how busy we are. Or you're probably in the middle of doing stuff, walk away, you know, kind of forget to log off. You're just going to be like, oh crap, I didn't log off and then."
RN 8	"I would think it's a norm to walk away without logging off."
RN 18	"I'd say the norm is not logging off. We have had computers in every room as well as outside of the rooms and also at the nursing station. It's not uncommon to have a nurse leave their screen up in a room or especially in a nurse's station."

While discussing peers not logging off, additional discussion and insight into those reasons for no log-off emerged and formulated the subtheme for why others in the unit did not log-off. While the RNs were only attempting to surmise these reasons because they know the workflow and work closely within the unit, it was reasonable to attempt a discussion about their impressions and observations.

Table 7

Unit Others: No Log-Off Reason

Participant	Response
RN 12	"I think it's a matter of convenience they just walk away or they think they are going to come back and pick up where they left off. Like if they are interrupted to go see a patient or whatever. But, many times they are done with rounds and they are logged on until it actually logs them out automatically."
RN 14	"I see people leaving theirs, because that's where they are charting at this particular desk. But then it really, it shuts off, I mean you can't keep it the whole night. Researcher note: Participant looked visibly upset during this discussion as if she was shaking with concern for the violation in process."
RN 17	"They could have looked at meds and went to get the meds and just wanted to still be in that computer because they have to go to the med cart and then come back and check their meds against the med list. They didn't want to log in again because it takes too long to boot up."
RN 18	"I think it's probably mostly convenience. Also, I think sometimes if nurses are in the middle of charting a complete assessment. They may fear that closing out that they'll lose their spot even though that's not true. Most of the time when they do walk away from the computer it is for patient care."

The subtheme of computers being seen emerged as participants' responses about computer location on their units and the workflow that they use to document related to log-off. RNs and physicians have a code of honesty so they feel protected in their domain and if the computer is in a zone that only they can see they feel as though they will protect it so there is less need to log-off. If it is not in a zone that is well protected or encompassed by staff, they will more likely log-off.

Table 8

Computers Can Be Seen

Participant	Response
RN 6	"Where I work is pretty open and you can, everyone has visuals of what's happening. So, if someone walked over you would see it." Researcher Note: Implied in discussion that staff would go right to it and protect that PC.
RN 9	"If somebody was at a computer where you were, and they didn't belong there, especially at the bedside that would be very obvious."
RN 2	"If we see each other's computers, we protect those so that no one accesses them that should not. We have each other's backs you could say."

While not all nurses specifically discussed the visualization of the computers they each echoed the concept of trust working as a group within their respective units. This extended into the discussion of passwords and the use of accounts or working with each other in the clinical area.

Primary Theme 2: Password Challenges

The primary theme of password challenges had subthemes emerge in the areas of ease of use/log-on, supports workflow, sharing password or account, password sharing situation, reward for sharing, share by badge scanning, password frustration, and clinical concern. Albarrak (2012) identified that the behaviors of nurses allow for the potential security risk related to the password practices. The findings in the interviews of these 20 participants found that there are many password challenges they face and these tend to factor into the subthemes related to passwords.

Table 9

Primary Theme 2: Password Challenges

Participant	Response
RN 3	"I've had to change it because I was told by security that, I guess they do a check on social media and somehow my password was seen somewhere and I had to change it."
RN 6	"Before it was a simple password, now it's a complicated password that you have to come up invent some complicated password. Now, they don't want you to reuse a password that you've used in the past. So, that's made it more complicated."
RN 14	"I mean you have to change it. Well so far, I think I've only had to change it twice in epic but you finally get your grove with the numbers and the letters and you know the password and then 3 months later you are changing it again. So, it's just hard, we have so many passwords all the times and then you are off for a week and you are like, okay, my password was just changed which one was it now, they are trying, we should write it down more often."
RN 15	"The problem too with the passwords is, like sometimes I would just make a change on it, like maybe, like say my password is abcdefg capital A, then you had to add a number oh! I would make the last number 1. Then the next time I have to change I'll make capital A, bcdefg2. Well our systems seem to be getting a little smarter. They are like, "Well you can't have that because that's similar to what your last one was." So, then you have to come up with something brand new and then that really makes it hard to remember what that password is. Especially when it's one of the accounts that you don't use too often."

Challenges of password is closely associated to password use which was quickly identified as a subtheme with rich information related to the many additions of technology to the workplace that require password access and have associated workflow process.

Table 10

Password Ease of Use

Participant	Response
RN 5	“Very easy because now we have finger prints AcuDose but then to log on to our computer we just use single sign on, so, I only have to type it in once my whole shift and that’s it. Then any time after that you can just use your badge to enroll, sign you on automatically.”
RN 8	“Your badge is encrypted and you touch, they have little, there are little boxes on your computer that you just, you log in the first time in the morning and it will keep you, I would say it’s probably 12½ hours, it’ll, when you tap your badge to that box it will log you in. which I can see will be a problem with someone that holds a badge.”
RN 11	“Pretty easy, I usually stick with one or two, and switch between the 2, and I try to just keep it simple so, I would say it’s easy.”
RN 20	“Pretty easy, I’m pretty sufficient with being able to type quickly so, I can memorize my password for the 12 weeks or whatever it is until I have to reset the new one.”

Ease of use for password was considered to be fairly easy and adjunct technology was considered better than the electronic medical record because it was typically described as more advanced including fingerprint or single sign on (SSO) technology. Along with this discussion there was raised another subtheme of ease of log-on.

Table 11

Ease of Log-In

Participant	Response
RN 10	“Pixis, Epic, and the email were all the same log-on. So, when you would go to get your meds out it was the same, along with the finger press scan, your initial sign and it was all the same password and then log in. So, it made it easier.”
RN 13	“We have finger prints for AcuDose and log on to our computer with badge to enroll. This will sign you on automatically so sign in is only once my whole shift then I just tap and get on the computer.”
RN 18	“Single sign in badge works for all systems that you access.”

The responses related to ease of log-on for many participants was a discussion specific to the use of single sign on (SSO) technology related to timesaving and advantages for workflow. Password effect on RN workflow followed in the discussion.

Table 12

Password Supports Workflow

Participant	Response
RN 1	“I think there is a necessity for passwords, I do like at, my casual job that I can type your password in and you’re logged in to the system and then you can actually scan your badge. So, that helps my workflow.”
RN 11	“I would say the password is part of my work. I think if an error occurs, like say narcotic discrepancies or meds that were previously given. it’s easier to track future discrepancies and the medication for example. I think it easily identifies the user in case there is an error with anything.”
RN 19	“Yeah because no one can get into it and access your stuff.”
RN 20	“Yeah, it’s just how it is.”

Once password challenges and password workflows were freely discussed the sharing of passwords and accounts were discussed as a consequence of difficulty of password access. While some participants reacted somewhat cautiously all responded openly and willing to talk about unit culture and their “feeling” about what should or should not happen and what actually happens during their normal days at work. There were no responses of individual sharing of a password. Several participants shared situations of knowing of sharing passwords and being aware of sharing but they personally had never shared their password. Several participants had shared accounts through badge sharing which is described as a separate subtheme, Share by Badge Scanning (Table 16).

Table 13

Sharing Password or Account

Participant	Response
RN 2	"I have not shared, not me personally."
RN 10	"I can't imagine needing anyone else's password if we have the same access."
RN 14	"I don't feel like, since we moved to a new system, but before we have somebody that's very busy. You are in the middle of resuscitating a patient and you had already logged on your charting and somebody will say, "What's your password?" Because they want to close your thing out so they can jump on finish charting whatever were doing in the room."
RN 15	"I can honestly say, I've never given either to each and that's only because I have such a paranoid personality that even close coworker would. Well here is something that happened years ago. Coworker as a practical joke someone left their computer open and while the person was gone she went in and typed kind of like something funny in the chart. That wouldn't be appropriate to be written on the chart and was certainly not related to the patient at all. The person came back and maybe types the person and hits save. So, that now became part of the preliminary record. I felt, "Oh! My God! I can never have that happen to me." I felt oh! You know I have worked with a bunch of tricksters and stuff not that this would ever happen and be like such one of the better chance of happen. So, I just never have given that out. I've been in situations where other people have said to me, "Oh! my password is just, just type it in really quick." You know they need something and I do. But I keep thinking well I can't be the person to go back in and do it. Plus, I can't remember password. So, a series of numbers after that I can't remember. So, I won't say I haven't but I have used other people's passwords to get into their accounts."

Several participants discussed situations that sharing passwords might occur or that they had been aware of password sharing in the past. Those situations were captured within a subtheme.

Table 14

Password Sharing Situation

Participant	Response
RN 4	“They don’t have time to document so, they will do it for them or they will, the nurse will do it and she would, the doctor might say, put some orders in for me. So, they would know their password and then put them in or the doctor would walk away and say, my computer is open you can use it and put these orders in or look for this for me.”
RN 11	“I know sometimes people, people that have previously worked where I currently work will come back to pick up like over time. But then are not in like press B system anymore. So, they get kind of logged out of certain things, and I think in that instance they would like need to use somebody else’s ID and password.”
RN 15	“It's usually like an emergency situation. Beginning with I work in ICU so, patient is going on the tubes and they are hanging a bunch of bags like pressers which keeps blood pressure up. They are just like, “Type this in and try that we hang this or throw a set of vitals in for me real quick?” because they are maybe doing God knows what. I mean if there are expressions or something that should not be written down manually but we might not have gotten to that point yet but we might be suffering the dream we call it. We just want to start documenting but they have so many other things they need to do.”
RN 19	“If someone is at home and you want to look up their lab work and they are not there. Or you want to check something for them that is their personal information in their chart.”

Interestingly, one of the examples of sharing passwords was for personal record review while the employee was off campus and had another employee check their personal health record. In this scenario, it was not related to access to the electronic medical record for patient care, documentation, or workflow improvement. According to the participant this information could have been gained through a patient portal by the individual who had shared the password. When the aspects of password sharing situations were provided, I probed and asked what the reward for sharing a password might be. The rewards became another subtheme.

Table 15

Reward for Sharing

Participant	Response
RN 4	"The benefit is to know that he or she doesn't have to do the work that the nurse is doing the work for them."
RN 5	"It's just faster because to log on and to log off takes so long."
RN 11	"They can't get in to anything because they are not necessarily in press B system anymore, but kind of outsource or work elsewhere. Now have access to system through our password."
RN 14	"That's for the patient, I mean it's because we are busy doing patient care. I mean we are not just sitting at the desk next to them. We are not standing next to them in the room, you know, I mean we are busy physically doing something with the patient that I can't really just turn around and put my password in if I'm changing an IV dressing."

There was no identification by participants that they personally shared their password but they shared many examples of password sharing that they were aware of previously in their experience and currently within their departments. Through the discussion of advantages, a twist on sharing passwords was described. This subtheme is about account sharing in that the RNs with a badge registered as single sign on (SSO) will swipe in and allow another RN to use their account for access or pass off their badge to allow access, primarily for documentation and review of data. Respondents described hand off of badges to each other for various reasons, in one case to non-RN staff.

Table 16

Share by Badge Scanning

Participant	Response
RN 1	"I do like at, my casual job how you can type your password in and you're logged in to the system and then you can actually scan your badge. So, that helps my workflow and our team working together sharing."
RN 5	"So, we actually do use each other's account by swiping the badge for each other during rapid admissions and critical events when we work as a team. But we never do share actual passwords."
RN 13	"I'm getting an admission and they're charting. I give them my badge so they do single sign on under my name. They can search for anything under me like vital signs, new labs, and stuff."
RN 18	"Other than that, sometimes the badging situation can be of concern if people lend their badges out to go get coffees. Or lend their badges out to get to medication room. So, if they logged in once with their passwords that the badge can find into any computer with just tapping it on by the computer. Most times that the badges are handed off is when we have like a coffee shops and a bunch of people want coffee. So, one person will go to pay for it because we can pay with our badges too. Then there are scenarios, not too often but if I'm in a patient's room doing patient care and one of the nursing assistants comes up to me and says they need in the medication room which is only in the night shift. Because they stock in there they have to get in but they don't have access with their badges. So, they have to get our badge to get in so that they can stock and that's it."

While discussing the need to share badges and other password practices there were discussions of frustrations with passwords. Balozian and Leidner (2016) discussed the developments of frustration creating an avoidance of technology and the use of security practices. This is consistent with the findings of the participants in this study as the more frustrating the work of IT security becomes the more they looked for workarounds.

Table 17

Password Frustration

Participant	Response
RN 1	"It's time consuming to retype that all the time, but my fulltime job, we don't have that capability of scanning the badge. So, I do have to physically type my password every time I go on to a computer."
RN 6	"It gets more complicated, I think as the years have gone by. Before it was a simple password, now it's a complicated password that you have to come up invent some complicated password. Now, they don't want you to reuse a password that you've used in the past. So, more complicated. And we have so many logins. I mean to get to the actual screen where I'm doing my work, I've signed in, or I attempted to sign in 3 or 4 times. You sign in and maybe you mistype or have a typo to sign in again. Then another screen pops up and then you have to sign in again and then you might mistype again. So, times it's like 4 or 5 attempts to signing in before you actually can get your work done."
RN 12	"We have so many different passwords for different things, and they let you help to log in and we can use them simultaneously if there are all logging out after only a few seconds. That's just going to take more time away from the bed side care."
RN 17	"Logging in and off just this morning I had to look at chart records and it was 3 screens that I had to log into just to get there. I don't know why but I do that many times a day. Our organization is so built on administration and then this world that takes care of patients that they don't realize the impact and like say, "Oh! Didn't you get that email?" well the email does not cross into the patient. But it's all these layers of security that sort of make a barrier for you to get that information flow to this information flow. So, now I didn't know that the system is going down in 5 minutes. Now I didn't know that because I don't look at my emails while I'm taking care of patients. I think security is probably why we don't easily connect. I don't know why it's not my thing to know. But they are completely different worlds."

The frustrations that were described by the participants impact the workflow within the clinical practice of the work environment. RNs perceive that both the time factor and impact to care are important in the process of password use. Along with frustrations, participants discussed the clinical concerns that arise when using passwords and accessing the system of the electronic medical record.

Table 18

Clinical Concern

Participant	Response
RN 10	"At this point, I would worry about if somebody would kind of get into my password is utilizing it to way smart cards like that. Even when I do sign off. I mean that's the big worry in the hospital is job diversion and I would be concerned that if somebody knows there is a way to waste in computer system that will not need someone. Like if you wasted the med station you would be able to focus that there is a way to do it through epic that also wasted with, at the bed side? So, you don't have to go to the med station, however, if somebody had your password they would be able to do that without you there. So, that's the only thing I've noticed so far, "You can do this here too?" So, if somebody did get someone's password, they would be able to simulate that person wasting on my card."
RN 15	"It's usually like an emergency situation. Beginning with I work in ICU so, patient is going on the tubes and they are hanging a bunch of bags like pressers which keeps blood pressure up. They are just like, "Type this in and try that we hang this or throw a set of vitals in for me real quick?" because they are maybe doing God knows what. I mean if there are expressions or something that should not be written down manually but we might not have gotten to that point yet but we might be suffering the dream we call it. We just want to start documenting but they have so many other things they need to do."
RN 2	"New hires as orientees do not get log-ins for quite a while and that poses a problem for them that they could either do their patient care, or do their, you know look up their labs, and get in the systems. So, that they can actually look at orders without the preceptor actually doing it for them. I guess they could, the preceptor could log in but, I think I would say, the only benefit I could see for them doing this, is just for their ease of work. With the preceptor not doing all the pieces but I do know that there is a big challenge of getting people into the system to be able to join the system."

These clinical concerns impact immediate access to information, ability to provide clinical care, and employee participation as a team in information. Although these concerns might be considered frustrations to some they were very clearly and emotionally described as a concern, very differently than the frustraters. This theme was differentiated based on researcher notes and cues from interview that identified the content as a “concern” that would occur in the clinical area related to care and workflow processes related to direct care. The scholarly literature shows that Albarrak (2012) reported the password sharing at a rate of 33%, Fernández-Alemán et al. (2015) at a rate of 31.7 %, and Medlin et al. (2008) at a rate of 73%. In these three studies, sharing of passwords occurred with coworkers or colleagues and friends of their coworkers. In all of the quantitative studies there is no insight into the reasons for sharing passwords. The primary theme and subthemes reported here begin to reveal insight into the challenges faced in the process of password and account use and why password and account sharing might occur.

Primary Theme 3: Managing Password

Managing a password was reviewed in the scholarly literature as important to maintaining IT security. Albarrak (2012), Belanger (2011), and Medlin et al. (2008) each discussed the development of passwords and identified that users do not choose to create strong passwords even though they have the knowledge. User preference is “ease of use” (Belanger, 2011). In most situations, it is difficult to memorize a password that meets the definition of complex, this leads to easy or familiar password creation (Medlin et al., 2008). How RNs perceive the management of their password is important to understand based on the literature. This Primary theme contains the subthemes of password development, remembering password, change password how often, password support, action if someone knows password, worry about password.

Table 19

Primary Theme 3: Managing Password

Participant	Response
RN 6	"I think it's just remembering it and I wrote it in my phone. Because there are so many passwords you have to remember. I mean there is the pharmacy password, there is MyPay password, there is the TMS."
RN 8	"I don't give it out to anybody and most people are pretty good about when you're logging into the AcuDose they probably look the other way. They try to respect your, the privacy of your password or I try to shield it with hand, to shield with my body especially for things like narcotics."
RN 11	"I try to memorize it not write it down. I usually stick between 2 passwords. So, when I'm prompted to change it in the system I'll, you know won't forget if I change it to something totally different. I try to keep them like they pertain to my life like pets or family members or something like that."
RN 20	"Just remember it."

As described in several responses the RNs are trying to memorize the password, write it down, and protect it from visualization. In all cases, they try to protect the password in some way. Development descriptions were similar to those described in the literature. Each participant made their password something familiar to them that they would remember. They described that they would use something familiar, including names of spouse, child, or pet, dates of birth, and other specific personal information or a systematic approach that they would repeat. Several participants described following the system requirements while using familiar content. They reported that they would just use an uppercase letter at the beginning, and a number, or special character behind their familiar content.

Table 20

Password Development

Participant	Response
RN 3	"Whatever instructions I'm given, that's what I, how I change my password or develop it. That's another way I want to do it, but sometimes if it tells me I have to have it in capital I do that with some digits."
RN 6	"Digits, letters, characters, usually something that helps me, something that is easy for me to remember. Usually kind of a birth date, a name."
RN 10	"I try to make it something that I will remember. Usually some version of my initials or something that I've used in the past, like a version of something I've used in the past that reminds me my children or something. I only have like 3 that I alternate and I have to change things and it's always one of those 3 versions."
RN 15	"I came up with something that's in the category, let's say colors so say I decide to keep my base password, a color. So, it will be let's say blue. Then the next time I'll need to change it I'll make it red. Then next time, I'll change it to make it orange. So, it's always going to be a color, something like that. Then, if it asks me to change it'll be like capital B and then blue, you know because you have to have a capital and then blue. So, I know I'm stating in a color scheme. Then the number, I might make it, say the year, you know whatever year it is. Let's say its 2016 there will be blue 2016, but if it got, yeah blue 2016, or Blue16."

Remembering a password or committing it to a secure place for safekeeping is something that I was very interested to hear about as the participants began to discuss their approach to how they remember their password. The responses of committing the password to memory made me wonder about the complexity of the password but at no time during the interview did I ask for or probe for a password. There were a few times that I suspected a participant might share a password and I cautioned them that I did not want them to share their password I only wanted to talk about the password.

Table 21

Remembering Password

Participant	Response
RN 2	"Aside from writing it down, in the book that I carry in my pocket, I usually try to remember my password. It's usually when I come back or you know if I am on vacation it's when I have to try and remember it."
RN 3	"I have it written down, but it's kind of coded."
RN 4	"I do not write it down here where I work, it's not in my phone, it is written at home."
RN 9	"It's just in my mind."
RN 13	"I wrote it on the back on my badge so I don't forget."

Frequency of changing passwords contributes to overall security of an IT system. In this subtheme, the responses demonstrate what happens with changing passwords over time in the lived experience. 16 participants have not had to change passwords for long periods of time. Those who have had to change passwords report that it causes confusion because they have to use different passwords or variations then they have difficulty remembering the password.

Table 22

Change Password: How Often

Participant	Response
RN 4	“I don’t change it frequently because in this situation we’re not asked to change it frequently.”
RN 5	“Never.”
RN 7	“I don’t change it, because then I won’t remember it.”
RN 19	“Meditech you have to change it every couple of months. Regular computer we never have to change it. They don’t make us.”

RNs are clinical and sometimes need support. They discussed who they believe is the support they have for passwords when needed. As evidenced by one of the responses here they are not always sure what the problem is, PC, software, or password.

Table 23

Password Support

Participant	Response
RN 1	“I’ll call IT and they always give me a temporary one (password) and then I create a new one.”
RN 12	“Sometimes you can call the help desk and get it(password) that way, other times you have to go right through talk to somebody in IT security. So, it’s not always the same person or the same way that you go around to get a password.”
RN 15	“Sometimes IT help is needed to fix a password or computer or decide which is the problem.”

Other than purposefully sharing a password what would an RN do if they discovered that someone knew their password? What level of urgency would there be in an action? This subtheme provided insight into the actions that the RNs would take. Many of the participants would require assistance in knowing how to get a password changed.

Table 24

Action Taken if Someone Knows Password

Participant	Response
RN 1	"I will change it."
RN 6	"I probably won't take any action. Because it changes with every 3 months."
RN 15	"I would like to think that I would change it but then I don't know that I would. Like if a trusted friend I would probably just let it slide like I had given it out. Maybe I felt somebody was or I know somebody did it."
RN 18	"Not knowing who to even go to about changing my password, I'd probably alert my manager first to receive some guidance at least about where to go. So, that she was aware and look into possibly my password being used for things that I didn't do. But then IT would be contacted promptly to really send me password so that I can actually log on. That's a really tough one to think about because even if it's a night shift, so I figured out someone knew my password. I don't know if I would call my manager at the middle of the night so I may continue to chart with my password knowing that I could at least log in and know what I charted versus what someone else could have put in."

Fifteen of the participants would change their password either immediately or as soon as they could figure out how to make the change. The other five would not take action to change their password and considered it a low priority that did not seem to concern them. Given the concern for breach of password, potential for worry was a theme that rose from several participants but was related to external passwords not work related.

Table 25

Worry About Password

Participant	Response
RN 1	"I'm always on the lookout but I don't, I don't worry because I really do feel like people don't want you to take their passwords. So, I don't think they would want to take my password. I think it's a mutual understanding respect."
RN 3	"Yes, but it's, I worry about it but I know I have a secure password at least from what I feel. But I always know that somebody somehow could in some remote way still hack into an account that I have, even though I have a password for it that I feel secure."
RN 6	"I worry that I'll forget it, like after I'm off for an extended period of time then if you forget it you can't get in or else if that 3-month period has gone by and you're logged out and you can't remember it, you can always go to help desk."
RN 9	"For work, no, banking yes."

Fourteen of the participants do not worry at all about their passwords at work. Those who do worry about it have low levels of worry related to media publications and placed more worry on their personal accounts such as banking and credit.

Primary Theme 4: Orientation

The primary theme of orientation had four subthemes emerge that were analyzed including annual education, recent IT security, IT security talk on your unit, and participation in IT policy review on your unit.

Table 26

Primary Theme 4: Orientation

Participant	Response
RN 2	“In the orientation part of this you know that the flow of electronic medical records is really new. The overall orientation piece on the first orientation we did how do I track records. But as new systems come up we usually manage those. We are going to go through all the elements of those. So, I can say with each system I would probably have been oriented to that particular system and all you need to do will be getting in all of them. You know sometimes, especially with the when you first start using it, it’s difficult to know like exactly how you logged on. Sometimes you were just you know just take off, just log off like you would normally do with any other computer application without realizing its so different when you do that within the track records. So, I think it’s just plain orientations as you have new systems come up have them going and you have to get through too many systems. “
RN 5	“They do tell you to secure your stuff, don’t walk away from your computer, log off, but it’s not realistic.”
RN 6	“That you need to sign off when you walk away from the computer not to leave your PIV cards, not to leave your PIV card in the computer. It’s a personal identification vehicle or something like that and it has a chip in it or putting in the computer.”
RN 17	“Oh! Sure, I mean there is paper you have to sign understanding that this was to you and you are bound to maintain its privacy, you aren’t to give it to anyone. All that I remember that vividly it was ingrained. Then as layers have come on, we had to do that again. Like when AcuDose came in we had to sign another paper saying this is yours.”

Eight participants responded that there was no IT system when they started in nursing and the systems came along after they were working so they got oriented as the systems went live or they got no orientation and training. Two reported that they had more detailed orientations with med scanning and medical record review and the final 10 participants having reported that they had limited variations of password and or log-off security measures as their orientation. Annual education was reported as a frequent type of either IT education or IT security but was reported as brief in content. Participants described annual education and episodic education as more common and memorable.

Table 27

Education: Annual

Participant	Response
RN 1	"There are modules for annual training."
RN 5	"Each year there is some kind of on line training that has computer training or a refresher of some sort. I believe it talks about log-off."
RN 12	"But we do have each year, we have education that we have to do online regarding confidentiality of emails and your passwords and like IT kind of security. That's usually a yearly thing."

Recent IT security education was identified by seven participants, five who discuss on-line modules or ULearn type of education. The two RNs who mentioned they had mandatory education could not specify if there was IT security information within that education. Thirteen RNs had no recent education.

Table 28

IT Security: Recent

Participant	Response
RN 15	"The hospital has had us, I'd say in the past year do security education modules on the computer. Which requires a password that I can absolutely never, I can tell you the hospital tells you what your password is. It says, to put in your employee number then it tells you what your password will be by telling you to enter your hospital identifier code. Then your password and it's your social security so that's the password that you really don't have to remember because the hospital tells you what it is when you are entering in to that. But we have had education models on IT security."
RN 17	"The mandatory education that we do, that's all."
RN 5	"No, I don't think, there might have been a blurb about it in our chart nurse class, but I don't really remember it being anything significant."
RN 9	"Not to my knowledge, but there is a bunch of you learns going on right now that I haven't completed. So, sometimes that will capture something new that's happening."

RNs discussed the education of IT security, or the lack of such, and the unit talk of IT security. Fifteen participants had no talk on their units of IT security at all, five did have IT security talk creating this subtheme. One of those discussions was related to IT security frustrations.

Table 29

IT Security Talk on Your Unit

Participant	Response
RN 9	"Only when there was that pretty big breach a couple of years ago, and even that's the only thing that really brought it up. But it's not a daily conversation."
RN 5	"Yes, we have, there is one committee that deals with our IT staff, I've been able to call them. We get updates on that once a month in our emails and stuff and if anything changes we have education about that."
RN 12	"The only time it's talked about is if we have a new nurse or a traveler start and they don't have their IDs. Especially it's normally requested at least 2 weeks in advance. But the day they start they can't access anything and it takes hours to take their password up and running. It's especially difficult for travelers because they only get a 2-day orientation to the unit. They spend half their day trying to get their password and that's that time wasted."
RN 14	"Not really, not security so much as frustration of getting in and you know, getting in is a problem it's like you always have the log in, log in, log in. But there is no way around that. You know that's what it is. Our discussion."

Renaud and Goucher (2012) discussed that the likelihood of employees reading policies without encouragement and engagement by management is unlikely. Policy practice and implementation takes management interaction, education, and oversight and in many cases involvement to assure that the employee is engaged in the process and knows the information. In this subtheme, all participants share responses of no policy review for any kind of IT security or security practices for their unit. One participant responds that they make a periodic review in the department of an already established policy so that they are aware of the contents for appropriate cell phone use and other devices on work property.

Table 30

Participate in IT Policy Review

Participant	Response
RN 5	“No, I don’t even think that’s an opportunity for, I mean that I’m aware of.”
RN 10	“No, but I have been reporting the issues that are a concern that I have about or someone would have someone else’s password that could raise an issue for colleagues about that.”
RN 17	“No, just reviewing it with the staff because there were concerns about people sharing information on social media kind of stuff. I mean we’ve done that, we’ve done a staff review of about what you are allowed to have share and what you are not allowed to share. I guess some issues that were pretty good so, we have review policies as a unit, go over. Share what's identifiable, what it’s not.”

The participant responses related to orientation and each of the subthemes of education and policy participation represent many gaps in engagement with IT security. RNs respond with little experience or recall related to IT security detail in each of the themes.

Primary Theme 5: Call Who With IT Question

This primary theme identifies basic IT knowledge and engagement. The knowledge begins with the elements of simple connections to information of support for IT security to the clinical area and clinical personnel when needed. Do the RNs know who to reach out to when they have questions or concerns about IT security.

Table 31

Primary Theme 5: Call Who With IT Question

Participant	Response
RN 4	“I would call, we have a main help desk call or line we can call, it’s 24/7 would help me.”
RN 9	“I would probably call the help desk first. I know there is a security officer, I’d have to investigate on how to get a hold of them. But I really couldn’t tell you who it is.”
RN 15	“I know I should know this answer because it's part of the education module. But I don’t know very specific name or title at this point. I know yearly I do the module and then I quickly forget it because I never need to know it. But I would have, I would probably go to clinical director first to remind me who that person is or the director of our unit and then they will point me in the right direction. Or I could always call a help desk to, like if there is something later that I want to know immediately I'm sure they can point me in the right direction.”
RN 16	“I would call the computer tech person. I'm not sure what that person’s title is but I think maybe I think a computer tech person. I would call that person and ask him or her what to do.”

All participants would either call the help desk or IT personnel. There were four participants who were not completely sure who to call if they had concerns or a question and they deferred to their clinical leaders first for direction.

Table 32

Whose Role for IT Security

Participant	Response
RN 2	"I think it's really everybody's responsibility but if you see that there is an issue, they need you to confront it, or they need you to report it. So, I think it's kind of everybody's job but I know that there are some people that are ultimately responsible for that like the privacy officer in IT and those types of things. So, I think it's like everybody."
RN 11	"Definitely the IT department, clinical engineering. I'm sure help desk would probably be involved."
RN 1	"Well, I think it should be your hospital system, they have to make sure that it is able to be accessed by only authorized users. I think that it's my role to protect my actual access. But I think as a whole it should be your IT department from your hospital to prevent outsiders from trying to get in."
RN 7	"I don't know, we just call the helpdesk for everything. So, I'm not exactly sure who maintains the security but."

Participants responded in six categories for who was responsible for IT security and some included several within their same response. Responsibilities identified were for everyone (4), the hospital (2), IT (10), my responsibility (2), record security analyst (1), the RN (3), and not sure (1). Those who responded that it was "my responsibility" or the RN, suggested that it was their responsibility to maintain only their access with their password secure. During discussion of maintaining system security respondents identified various levels of concern that system is not secure.

Table 33

Concern System is Not Secure

Participant	Response
RN 1	“I was a little concerned when that breach did occur I don’t know the full details of it. I do know that it was one incident and not system wide. But I do think that the hospital took it extremely seriously and worked with caution in preventing it from happening again.”
RN 15	“Actually, it's secure, the only vulnerability I can see is just through human error you know that I'm probably guilty of is by leaving my computer open and that’s the only way I can think of. I don’t know how and it seems to me like I don’t know that it's or anything although I do know the physician can access all the information too. So, I guess it is open to the web so I guess it's technically open to vulnerability if it's on the web. But I assume we have now security team taking care of us.”
RN 18	“Sure yeah. Having some close family members in information technology that have been visited sometimes at work knowing that our operating system is a little bit older and isn’t supported at this point by Microsoft. That's a concern and that’s really the biggest one. Other than that, sometimes the badging situation can be of concern if people lend their badges out to go get coffees. Or lend their badges out to get to medication room or something like that. So, if they logged in once with their passwords that the badge can find into any computer with just tapping it on by the computer.”
RN 8	“I don’t know that any system is secure anymore, I mean everybody is getting hacked, I mean the big hospital system I work in was a victim of being hacked. Every time you turn around someone is being hacked. Or I don’t know, I think the more every security thing we develop there is someone who is just that much smarter and finds a way around.”
RN 9	“I don’t think anything is secure in today’s world anymore. Like my banking account got hacked, my credit card got hacked, my little kitty credit card hacked. I was having charges all over the place. So, I don’t think anything is really secure, I really don’t.”

Although the majority of participants (14) believed the system is secure. The six who were concerned about security of system had some experience wither directly or indirectly with a system problem or breach. If there was a concern or report of an IT issue was the participant's confidence maintained.

Table 34

Confidence That Concern is Taken Seriously

Participant	Response
RN 11	"Yes, they are very good with addressing any concerns that we have."
RN 17	"Oh! yeah. I felt that there was not the same timely response we would expect to issues. Because I thought that this was pretty serious like "Hair is on fire" we need to deal with this now and they were like, "Yeah we know."
RN 18	"Yes, every time we call them they actually have to open up a ticket and it gives us an email saying that the tickets' been opened. Then it'll tell us when the ticket's been closed meaning that everything should be resolved."
RN 20	"I think it depends on who answers the call on the help desk, it depends on the staff member that I would get in touch with."

Within this subtheme 19 participants expressed that they had confidence and one answered that "it depends on who answers at the help desk". The depth of the connection with confidence seemed to be at the help desk level. This is the level of connection for the RNs to IT security.

Primary Theme 6: Rate Security

Within this Primary theme of rate security, there are subthemes of are you expected to know IT security, is your job better with IT security, and what is your teammates practice. The perception of security level that the RN is exposed to along with sense of job improvement impact the expressed intention of the RNs application of IT security.

Table 35

Primary Theme 6: Rate Security

Participant	Response
RN 2	"I feel like that data is probably pretty secure but out and about I'm not sure. Because anyone can really look at the screens. I mean as you walk by if you really wanted to you can look at the things so something like that. You know based on, how kind of area that you're in, it's probably the level different levels things just on the screen. I think different places in the clinical area probably more secure like the conference rooms are fairly secure. The nurse's station, maybe a medium level because the traffic through there. You have different types of people who go through the nurses' station, nursing positions, different disciplines. They kind of walk through nurse's station and not the hallways, which I feel are pretty open with visitors and all types of persons. So, I think that's probably not as secure in the other areas."
RN 13	"I would say it's mid-scale."
RN 14	"I think 8 out of 10, the people that are being careful but they are not ultra-worried about it."
RN 18	"If 10 is very secure and 1 is not very secure I would say my unit would probably be 6 in my opinion."

Ratings have to do with location and access of unit. This perception is about real time access to computer screens and computers. Two respondents rated their unit at the highest rating saying they would be 10 out of 10 or most secure. All others (18) said they would be moderate to moderately high secure because they are very careful with HIPAA but they do leave their computers and they had not really thought about several aspects of password development prior to this interview. Consistent with the flow of discussion this subtheme of the RN being expected to know IT security emerged.

Table 36

Are You Expected to Know IT Security

Participant	Response
RN 7	"No, I mean not the details, nitty-gritty but I mean maintaining a password and making sure that no one has access and to that extend yes."
RN 8	"I think we should know the basics, how to protect yourself, you know, protect your patient's information."
RN 15	"I don't know that we need to know the ins and outs of it but I know we are expected to as far as we are concerned and using the system to try to keep it secure."
RN 19	"The only aspect that I would be expected to do is have a secure password and log off the stuff. Other than that, we wouldn't be required to know how to do it."

Eight respondents identified that they should know some IT security but did not or were not able to define what that would include. They suggested they should know some basics or password safety. I had wondered if that answer was based on the content of the interview. The remaining 12 respondents did not believe they had a need to know IT security.

Table 37

Is Your Job Better With More Security

Participant	Response
RN 6	"It doesn't make my job better but it keeps information private. I would think that the patient's information would be a better chance of it remaining private."
RN 13	"I feel like if it was more secure it would make my job harder, I would spend more time on that rather than patient care and that would not necessarily be better. But if there is a way they can make it secure and fast then it would be different."
RN 16	"I think I'd definitely feel more comfortable. I think feeling more comfortable will make me feel more confident and then I'll perform best I can."
RN 20	"I don't know if it would change specifically nursing practice just making things better, would make the patient safer so then, yeah, I would think that would make my job better."

None of the participants said that IT security would directly make their job better but eight said that it would make them more confident or make the patients safer and then indirectly make their job better. Given the perception of impact on their job because of IT security, the next subtheme that emerged impacting the RNs job was teammates practice.

Table 38

Teammates Practice

Participant	Response
RN 5	“Like I said before we all share our badges to sign on to the computers to chart stuff, work, we’re in the room and we’re already logged on and to our patients something is happening and you need more help in the room and they’ll come on, if I am already logged on because I’m in there, then they’ll just start charting under my account or something.”
RN 12	“I believe that if that would make our job easier, they would share them - I do share them.”
RN 17	“There might be a few that are careless because they are careless in many things.”
RN 20	“Right, yeah, I mean I’ve definitely overheard people sharing their information it’s not necessarily to log into the record, but its, “Hey, can you check my PTO or can you log in to check if my paycheck was deposited.” Usually the same log in you use for all of that is the same that you would use for the charting system. In theory, they could log in under you in the charting system too. So, it’s kind of a bridge.”

Responses include nine that identify they are aware of sharing among their peers, three that are aware of badge scanning shared accounts, and five that believe there is no sharing of passwords or accounts within their departments among teammates.

Primary Theme 7: Association With Hacking

There are three subthemes in the primary theme of association with hacking. The three subthemes are impact to employees, impact to patients, and impact to organizations. The standard responses within the primary theme of association with hacking seemed to be rambling intertwining information from personal concern to work and inclusive of mainstream media mania. Several participants admitted “I just don’t know…” as they discussed hacking.

Table 39

Primary Theme 7: Association With Hacking

Participant	Response
RN 15	“Somewhere I know like I said I don’t know how the ins and outs of system actually works. But I'm sure smarter minds of mine with more technical survey can maybe back engineer or reverse engineer into a system but I don’t know how that works. I don’t know how to do that myself.”
RN 16	“I mean we don’t really know everybody we work with, we think we might but you have to protect yourself at all times in the world we live in. I just think that it's just a responsibility of each person. If hacking happens I think some of these careless things could really cause that to go on. We have to be just cautious all the time.”
RN 17	“I don’t know enough about that hacking, how that occurs, I assume that if you are not careful it would be well likely that someone would use it. From a hacking perspective but I really think the hacker people aren’t like nurses taking care of patients in general but again maybe that’s the delusion.”
RN 18	“If another coworker knows someone else’s password, it could do a lot of detrimental things. Be it just sabotaging that nurse’s documentation or undoing documentation that was done. Or possibly charting things that weren’t true or weren’t done.”

Thoughts about hacking are not based on anything deeper than changing patient records or what is known about HIPAA and patient privacy. There was no response included about social engineering or actual hacking principles. With this as a premise the subthemes of impact developed related to hacking

Table 40

Impact to Employees

Participant	Response
RN 1	"I think the impact would be fear and I think that people would be probably a little more protective of their own private access, yeah."
RN 17	"I think it would be terrible. I think that I would just probably take the system down for a while and we are terrible at down time. Because we've got to rely so much on computer even though I liked paper. We are no longer set up to run in a paper world so it would be really hard. I get the extent of the hack would be, the extent of the effect. If it took the system down for days and that would be rebuilt from who knows where if we lost data, it's irretrievable as far as I could see. I could not have to chart on someone 2 days after I took care of them."
RN 18	"I think there could be disciplinary action up to termination depending on the circumstances of how the password got taken."
RN 19	"It depends on what information was hacked, you know if the get your financial stuff they can get information about your bank accounts, taxes. Most of us have direct deposits or even our social security numbers are in there too."

The RNs have a strong sense that there are consequences to hacking and are expressive that hacking is detrimental to employees. With continued discussions of consequences related to hacking the RNs passionately discussed aspects of potential impact to employees and patients as if they were intertwined. In several cases the RNs spoke about themselves using the hospital for themselves and their families for healthcare thus identifying the blurred lines between employee and patient as they see themselves as both within the same organization.

Table 41

Impact to Patients

Participant	Response
RN 3	"Very impactful, their medical record it's the highest regard of privacy and we should respect that and in no way, jeopardize their sense that their health information is secure."
RN 11	"Gosh! That would probably be a nightmare. As a nurse, you look at your orders and you go off of your orders. Say for example the hacker would get into e-record and put like this bogus orders and that can definitely put your patient at risk or some serious injury."
RN 14	"I guess they would be able to change records, you know to change your data. Would patients have confidence?"
RN 16	"Oh! I just think HIPAA would be out the window for one thing. Patient information would go to hands where it shouldn't be going. I think it would be disastrous."

Again, the RNs have a strong sense that there are consequences to hacking and are expressive that hacking is detrimental to patients. While their focus is on patient information and the consequence of hacking on patient information they did make a correlation to patient trust in the care givers and the hospital. The RNs also made a connection to the hackers' abilities to gain patient personal identifiers and being able to capture that information for use to gain the patient identity for misuse. Some expressed public concern for hacking similar to what Kwon & Johnson (2014) described about public awareness and concern of hacking are becoming more prominent.

The RNs expressed that the consequences to the organization would be significant and detrimental in all aspects including public relations, community, business, financial, health plan relationships, and many other aspects. Those who are employees to organizations who would face this type of hacking felt he or she would personally be affected. In all cases, they reported the effects would be disparaging.

Table 42

Impact to Organizations

Participant	Response
RN 3	"Very detrimental, its end results would be detrimental to the patients, to the staff and publicity wise it would be negative publicity."
RN 11	"I would definitely think, thinking the benefits I get from my hospital like healthcare, my salary if they were to kind of meddle with that in the public and community that could basically ruin my life. They would be stealing my salary and my healthcare benefits. So, it certain would be catastrophic."
RN 14	"It would be bad. Bad name. I can't think of the word, but bad PR or bad messages to the outside community that you know it's not safe."
RN 20	"Loss of trust from the community, because there is that expectation that their information is secure especially things like health information. So, you would definitely lose that trust from people."

Primary Theme 8: Other Security Thoughts

Other security thoughts came from an open-ended question that allowed the participants to discuss other IT topics that may be connected to this questionnaire or security of IT in general. There were no subthemes within this primary theme

Table 43

Primary Theme 8: Other Security Thoughts

Participant	Response
RN 1	"Well, I mean even like IT security nowadays people can badge in for the doors, for parking, for food. We actually had an incident where somebody lost their badge but it was still getting used. They actually tracked the doors it went through and that's how they ended up finding it. I guess it was somebody trying to get to the information desk. But they still used that badge."
RN 6	"I'm just kind of curious that you pick up the phone, you call someone and they get in on your account, there is no verification that who you're speaking with is actually someone legit."
RN 11	"I would just say maybe, like the point where I gave you where the people that have used to work on the unit now work elsewhere, but they still come back and work. If there could be some kind of, I don't want to say universal password, but they should still be able to come and get into the system if they come back to work, in their old unit."
RN 20	"I always wonder what, how they determine the amount of time between password changes, why do they say it needs to be every 35 days or why does it need to be every 60 days? I mean do they just pull that number out of the air or is that backed up by something? I always wonder that."

This category of thoughts was helpful to consider other security issues and serves to help with future research ideas and those security issues that bother nurses related to IT security. This category of information may be helpful in operational situations related to security gap assessments. Additional topics included point of care testing scanning and badge sharing for ease of use, mobile devices used in workflow and how they help or inhibit workflow, different vendor systems and how they do not interact (interoperability), and other badge access uses.

There were no identified discrepant cases that were factored into the analysis. Member checking, adequate analysis of data, absence of researcher bias, and minimizing conflict of interest reduce the opportunity for discrepant responses (Peredaryenko & Krauss, 2013).

Evidence of Trustworthiness

Credibility

The qualitative case study method allowed for construct validity to be established through evidence from the chain of sources described by Amerson (2011), including member checking, pattern matching, explanation building and using logic models. The participants' ability to discuss and reiterate the important aspects of the informed consent while meeting prior to the interview and the member checking activities were two very important aspects of credibility. Engagement was critical to a successful interview and part of my role was to take notes, of which the participant was notified prior to the start. If I noticed that the participant was distracted in any way by my notetaking, I would stop during the interview and later jot notes following the interview conclusion so as not to interfere with the participants thought and concentration. Immediately following each interview, I would make any notes required and record additional thoughts and impressions that I had gathered from my insights of responses that I might have had of the participants expressed feelings or engagement mannerisms so that I could apply that information into the memo section of NVivo v11. These notes served to help clarify accuracy in transcription and questions that arose during member checking by myself and the members.

Transferability

The interview questionnaire was submitted to an expert panel prior to use and was revised and validated for the study increasing the relevance to the study, appropriateness to the topic, accuracy in content, and clarity to the population. Bengtsson (2016) discussed the importance of validating the questionnaire through the use of an expert panel in the process of qualitative research, as it lends credibility to the process. The constructs of UTAUT served as the foundation for the research questions. The use of UTAUT allowed for an established protocol incorporated into the study design and became the supportive structure for external validity of this qualitative case study (Amerson, 2011). The framework of UTAUT and each of the constructs being used within this research study were established and validated and did support the work in this research study. Thomas and Magilvy (2011) discussed that transferability of a study is applying research findings from one group or population to another. The findings from this study are expected to have applicability to other clinical populations within the healthcare arena.

Dependability

Dependability was assured through comparative hand notes taken during the interview and the audio recordings that were recorded and transcribed verbatim with review following transcription. The researcher conducted repeated reviews of the audio recordings. The purpose of the repeated reviews was to improve interpretation and identify cues related to the lived experience that will be shared. These were compared to the notes related to expressed feelings and engagement attempting to capture the associated lived experiences that were not verbally described but were expressed nonverbally. All elements of data collected, researcher notes, audio recordings, and transcripts, were input to NVivo v11 software so that accurate and dependable results were analyzed.

Confirmability

Confirmability was maintained during the interview process, coding, and analyzing process of the study. The neutrality of the qualitative study, is achieved when each of the following have been addressed according to Noble and Smith (2015); (a) truth value, (b) consistency, and (c) applicability. This was often difficult to maintain during the interview process because of the casual nature of the interviews. Knowing the importance of confirmability, I would review ahead of each interview and remind myself to stay focused on the participant's story. This assisted me in maintaining my neutral position when topics arose with any link to a philosophical position, or experience that might be associated or similar to mine that triggered an instinct to discuss or respond. The multiple reviews of the recordings also helped to reveal, eliminate, or separate, any personal response during review, coding, or analysis of the data. Careful and thoughtful bracketing was used during the coding phase of data analysis. The bracketing for this study was conducted according to Tufford and Newman (2012), and Sorsa et al. (2015), on several different levels and very thoughtfully to allow for reflexivity and understanding. Each phase of the data analysis required a thoughtful and nonjudgmental processes to assure neutrality.

Saturation

The qualitative study is enhanced when internal validity is supported with saturation (Fusch & Ness, 2015). The population of this study included 20 participants. Data saturation occurred at participant 14 with emergence of common themes and subthemes concluding. According to Fusch and Ness, saturation is reached when there is no new information, no new coding, no new themes, and an ability to replicate the study. Although saturation had been reached at 14 participants the additional six participants enhanced the data rich responses obtained and became "balancers" of subthemes that had emerged. Meaning was enhanced because of the additional respondents in some categories to assure that they were subthemes rather than primary themes. The last six participants added to the responses equalizing and enhancing thematic developments.

Study Results

The eight primary themes and all subthemes that had emerged were discussed in the data analysis section above. Each of the first six primary themes have UTAUT constructs that are coordinated with that theme, see Figure 3. This study was designed to answer the overarching research question, what are RNs' perceptions, expressed intentions, and self-reported behaviors of IT security? I was able to answer this question by first answering each of the supporting questions.

RQ 1

RQ 1: What are RN perceptions, expressed intentions, and self-reported behaviors of the performance expectancy of IT security practice?

To answer this research question related to the performance expectancy the emerged primary and subthemes from primary themes 2, 3, 5, and 6 were used. The RN perceptions, expressed intentions, and self-reported behaviors include a mixed use of performance expectancy of IT security practice. The RNs self-reported role in the usage of security practices is dependent on the situation in the clinical environment. The RNs found it easy to use passwords but frustrating to repeatedly log-in using a password when required. The RNs did not share passwords but there was a subset that shared accounts through a modern method of sharing through badge swipe sharing. No password exchange is required but the badge, registered for authentication via single sign on (SSO), is shared between RNs for workflow efficiencies. The belief that the RNs' have is that the process will help them maintain aspects of their job that pertain to expediting the patient care process, enhance medical record documentation, and did not see it as a system security concern. The RNs did not identify that there would be a direct improvement in their job but they did describe that if security made things better for the patient then indirectly it would be better. Exploration of how the RNs' perceived their role in IT security showed that they were not well connected with the IT support and did not have a strong understanding of who was or should be responsible for IT security at the front line or at the organization. The perception of security was at least midlevel or higher in all work units even though RNs reported that their teammates shared passwords and did not log-off of their computers when they walk away. The use of security practices was described as relatively easy to use but were not put into place as part of the regular workflow. The workplace in each unit is influenced by the security practices and may be impacted by these practices.

RQ 2

RQ 2: What are RN perceptions, expressed intentions, and self-reported behaviors of the effort expectancy related to the IT security practice?

To answer this research question related to the effort expectancy the emerged primary and subthemes from primary themes 2 and 3 were used. Effort expectancy is associated with how easy it is to use the security practices. There were no aspects of security discussed by the participants that were described as difficult to use. There were aspects of inconvenience, frustration, interference with care, and plain annoying. The identified RN perception related to the security practices and ease of use have a direct correlation with the utilization of those security practices that describes the ability for reporting no sharing of passwords. Nineteen of twenty of the RNs reporting in this study use the SSO badge programed authentication for log-in. The SSO allows for ease of log-in for a large number of systems that the RNs access. The aspect of difficulty is accessing records and information as rapidly with multiple RNs while immediate or critical situations occur, those were the times when deviations from security practices were reported.

RQ 3

RQ 3: What are RN perceptions, expressed intentions, and self-reported behaviors of the social influence related to the IT security practice?

To answer this research question related to the effort expectancy the emerged primary and subthemes from primary themes 1, 2, and 6 were used. Social influence is the method for which the employee perceives their peers or significant other relevant professionals in the clinical environment believe they should be using the security practices. Within this study, the RNs described that the teammates they work with did walk away from their computers without log-off and they do share passwords, however they themselves discussed their behaviors which were different. The practice of walking away from the computer without log-off was described as a cultural norm. The RNs described that they would not personally share a password. The RNs' perception of social influence in the clinical setting related to varying levels of social support which permits a cultural norm of computer walk away with no log-off, mishandling of accounts by badge sharing, and other security issues.

RQ 4

RQ 4: What are RN perceptions, expressed intentions, and self-reported behaviors of the facilitating conditions of the IT security practice?

To answer this research question related to the facilitating conditions the emerged primary and subthemes from primary themes 1, 2, 4, and 6 were used. The RNs discussed the operational support of each other as a strong facilitating condition that led to breach of IT security. Facilitating conditions, as perceived by the RNs, included the technical methods that support using the security practices. The safeguards in place to protect security IT including the auto log-off on the computers for those who walk away without log-off was identified as an inhibitor to patient care because it required frequent log-in ultimately causing delays to care. The other facilitating condition that is applied to the IT security used by RNs is SSO. The emerged theme identified that SSO was used to breach IT security by sharing authenticated badges for account sharing, med room access, and facility purchases. Orientation and education were limited so would not be considered as a facilitation of conditions. The RNs did not participate and were not engaged in policy development. Overall engagement with IT for support was limited as well creating another aspect of limitation toward facilitating conditions.

RQ: Overarching

With each of the supporting questions answered, the overarching question can now be answered. What are RNs' perceptions, expressed intentions, and self-reported behaviors of IT security? RNs perceptions of IT security include a very basic level of what security definitions include aside from privacy and HIPAA. The expressed intentions of the RN population responding to this study included a positive desire to do what would protect themselves, the organization, and most importantly the patients they care for. The self-reported behaviors of the RNs included mishandling of IT security through walking away from the computer without log-off, poor development of passwords, lack of password change for long periods of time, sharing of accounts through SSO authenticated badges, and sharing log-on information for mobile and point of care equipment.

I have cross walked the UTAUT constructs used in this study along with the primary and subthemes that emerged from data analysis. By using this method, a robust review of the lived experience of the RNs' perceptions, expressed intentions, and self-reported behaviors of IT security practices was conducted. This review allows for insight into the security practice in the healthcare work environment.

The inquiry and collection of demographic data was specifically designed to align with the literature that has been established including variances between male and female, age, and educational preparation. In the literature review, each of these demographic items had been shown to have a relationship to adoption of technology and change (Venkatesh, 2003). These demographic items were not found in the data analysis to play a role in nor have a relationship to the emergence of the primary or subthemes within this study. I was unable to make any direct alignment from demographic data to the construct themes of UTAUT aimed toward use behavior.

Summary

Albarrak (2012) , Fernández-Alemán et al. (2015), and Medlin et al. (2008) each showed mishandling of IT security in their quantitative studies. The use of exploration with the case study format in this study allowed for findings that add to the knowledge of IT security handling in clinical settings. The RNs' perceptions, expressed intentions, and self-reported behaviors of IT security was able to be applied with insight into their lived experience of using the IT security within their clinical setting. A discussion of the interpretation of research findings, limitations of the study, recommendations for future research, and implications for positive social change is presented within Chapter 5.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this qualitative case study was to explore the perception of the registered nurse (RN) within four of the constructs of the unified theory of acceptance and usage of technology (UTAUT) that are specific to use behavior (Venkatesh et al., 2003). Insight into the lived experiences of RNs related to information technology (IT) security was the benefit of this study. The experiences and perceptions of the RNs were analyzed as they relate to the UTAUT constructs of performance expectancy, effort expectancy, social influence, and facilitating conditions. Using UTAUT as the theoretical framework, the following overarching research question was used for this study: What are RNs' perceptions, expressed intentions, and self-reported behaviors of IT security? The findings included that RNs' perceptions of IT security include a very basic level of IT security definition aside from privacy and HIPAA. Their expressed intentions included a positive desire to act in a manner that would protect themselves, the organization, and most importantly the patients they care for. The self-reported behaviors of the RNs include mishandling of IT security through several venues, including walking away from the computer without log-off, poor development of passwords, lack of password change for long periods of time, sharing of accounts through single sign on (SSO) authenticated badges and sharing of those authenticated badges, and sharing log-on information for mobile and point of care equipment. Within Chapter 5, I address the interpretations, implications, and potential applications of the findings along with limitations and conclusions of the work as well as avenues for future research. Finally, implications for social change are discussed.

Interpretation of Findings

The findings included that RNs' perceptions of IT security include a very basic level of IT security definition aside from privacy and HIPAA. Their expressed intentions included a positive desire to act in a manner that would protect themselves, the organization, and most importantly the patients they care for. The self-reported behaviors of the RNs include mishandling of IT security through several venues including walking away from the computer without log-off, poor development of passwords, lack of password change for long periods of time, sharing of accounts through SSO authenticated badges and sharing of those authenticated badges, and sharing log-on information for mobile and point of care equipment.

The RNs expressed trust of their teammates and offered discussion of protecting their environments, almost justifying no log-off and sharing of accounts or badges. This is consistent with research by Box and Pottas (2013) who discussed the general functioning of healthcare professionals is naturally within an honorable and trusting community. Those healthcare professionals, because of their trusting nature, have a low need for security sensitivity leaving them with a limited sense of need for IT security awareness.

The majority of RNs discussed the use of SSO. But even with SSO, they still had additional application for which they were required to have additional and separate passwords for authentication. Milenković et al. (2013), discussed the issue of users having to remember multiple passwords and that would most likely cause the creation of insecure passwords, forgetting passwords, or cause wasting time with multiple authentications. Findings supported this with identification of password development occurring from familiar categories with rare to no password change. Systems including Pixis and AcuDose, both dispensing systems most often used for medications, were reported to have 2-step authentication of password and biometric access (fingerprint). Password and biometric authentication were both methods described of gaining access to systems securely (Li et al., 2014).

Password sharing was not discovered within this study among the participants. However, they did share their lived experiences of password sharing scenarios having occurred on their units among teammates. They described actual workflow and patient situations that they believed might be a reason for password sharing. Albarrak (2012), Belanger (2011), Cazier and Medlin (2006), Rajarajan et al. (2014), Sharma and Sugumaran (2011), and Tam et al. (2010) all discussed the difficulty of protecting the organization relying on a password. They suggested that it is the people who must be the strength of the IT security. From an organizational perspective, the IT system is composed of three parts: technology, management, and the people (Cheng et al., 2013). The people or employees remain the weakest link in security and password management even though there have been strides in technology systems (Medlin et al., 2008; & Tam et al., 2010).

The RNs found it to be a cultural norm to walk away from a computer without log-off. They reported that not only did they do it to care for their patients and to do other clinical tasks but they also reported that their teammates within their unit do it. The front-line culture of the organizations represented in this study has either allowed or evolved to a position that there is a low-level response to IT security. Kwon and Johnson (2014) demonstrated that there were three levels of security practice adoption based on culture: leaders, followers, and laggers. Those identified organizations were noted as leaders were training and managing risk and breach incidents. The RNs in this study reported that they did not recall much IT security orientation, they have very little IT security training and education other than annual mandatory training for which they had little recall of the IT security within that training, and they had no talk of IT security on their units.

Evaluating and managing the human factors is one of the key aspects of IT security. Human factors are frequently mentioned in the literature when discussing IT security and often through history have been referred to as the weakest link (Arce, 2003, Ferguson et al., 2011, Tam et al., 2010). Negligence is often cited as a human factor that affects the organization. Negligence can fall into several categories of security risk. Kruger and Anschutz (2013) discussed the insider negligence at the root of data breaches. Kwon and Johnson (2014) discussed that the healthcare industry faces two weak links the internal threat and the external threat. Two weak links exist because healthcare has not adequately ramped up to deal with the security risks through investment allowing for remainders of uncertainty.

I found that the RNs had moderate awareness of IT security and that their awareness was targeted toward HIPAA and protecting the electronic medical record. They were certainly also aware that there was an obligation to authenticate through password or SSO to gain access to any application or the electronic medical record.

Harris and Furnell (2012) had previously identified the same that the employees of organizations have been found to have only moderate to low awareness when asked about behaviors required for security compliance. Albarrak (2012) found that nurses were deficient in security awareness and the importance of overall IT security in relation to patient data.

Throughout the preparation for this study, the design, and approval there were many discussions with colleagues, my committee, and experts in the field about the use of Simpson (1996) as a reference and citing the discussion related to the lack of policy and procedure, education, and oversight from leadership within the organizations that allow for breaches in the security. I have found that with this sample, even if there is policy out there, the RNs are not engaged, they have never participated in policy development for IT security, the orientation could not be recalled, and education was reported as limited if at all. Of the education that was reported very little could be articulated. Other than the RNs knowing that they needed to use a password, they knew very little about IT security.

The primary themes with subthemes and UTAUT constructs were each described in Chapter 4 and are further expounded upon in this chapter. In consideration of all findings and how actions in response to those findings might be applied to healthcare with associated impacts, I present the diagram in Figure 4. This diagram identifies the three aspects of the research question (a) expressed intentions, (b) perceptions, and (c) self-reported behaviors as they emerged from the findings. The influencing factors are identified at a conceptual level including (a) limited orientation and education, (b) lack of policy participation, (c) lack of understanding, and (d) workflow needs. Finally, the implicated risk of self-reported behaviors of IT security mishandling and the direct impacts.

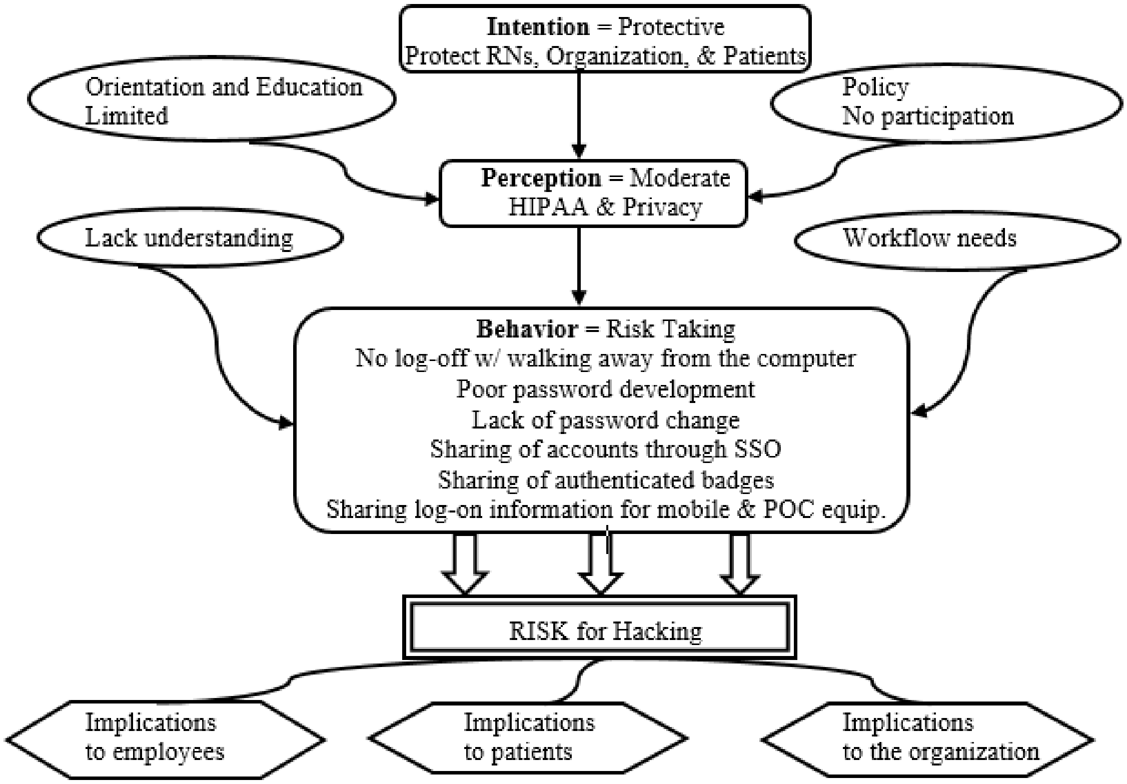

Intention = Protective
Protect RNs, Organization, & Patients
Orientation and Education
Limited
Policy
No participation
Perception = Moderate
HIPAA & Privacy
Lack understanding
Workflow needs
Behavior = Risk Taking
No log-off w/ walking away from the computer
Poor password development
Lack of password change
Sharing of accounts through SSO
Sharing of authenticated badges
Sharing log-on information for mobile & POC equip.
RISK for Hacking
Implications
to employees
Implications
to patients
Implications
to the organization

Figure 4. Diagram of findings. Reveals findings from *A Qualitative Exploration of the Security Practices of Registered Nurses* identifying emerged themes within the three aspects of the research question (a) expressed intentions, (b) perceptions, and (c) self-reported behaviors.

Limitations of the Study

Limitations of this study include that the study sample of RNs represented a single professional nursing organization and therefore lacks generalizability. The results from this population represent the security behaviors that can be provided in a limited descriptive presentation but do not become predictive of the future behaviors of other RN populations due to multiple contributing factors within each geographic region and organization. Additionally, the study participants were self-reporting. Limitations of self-reported results may contain bias, are not able to be verified, and are influenced by past or current situational experience (Brutus et al., 2013). The members may have experience with frequent surveying by their hospitals, other agencies, and other researchers of which I would have not known and that may create the limitation of a lower yield in an interest of participating in this study. The potential for eliminating a group who would normally participate in research due to over survey may have eliminated a specific subpopulation. Lastly, the RN's concern for the identification or potential for leakage of information potentially leading to disciplinary action due to variance from policy may yield false or dishonest response, limited response, or nonresponse to the questions within the interview process may be a limitation. The combination of self-report and fear of discipline might have skewed or influenced response honesty.

Recommendations

The outcomes of this cases study were different than I had anticipated as I had believed based on the literature that password sharing would become the primary area of IT security mishandling. Perhaps because of changing times and improvements in security and "ease-of-use" technology, the modern method of sharing accounts and expediting workflow is badge sharing with authenticated badges. The computer walkaway without log-off was another area of IT security mishandling that was prevalent in the clinical area. These two aspects of variance from IT security seem to be the result of mismatch with workflow for patient care and need for emergent or rapid documentation.

Future Research

The IT security mishandling behaviors of RNs provide fertile ground for future research in the areas associated with their work environment and practice patterns as they relate to IT security. These research studies could be done from several perspectives, including (a) observational workflows and associated IT security, (b) observations of what actually happens during the periods of mishandling, (c) timing of IT security processes used in the clinical setting, (d) actual nurse use of accounts and type of accounts with types of access to each account, and (e) comparative assessment of what IT believes is happening/management believes is happening/and what is really happening in the clinical area (perception/reality mismatch).

Orientation, education, and policy were identified as areas of weakness or not present. Future research in this area could include actual tracking of education and later evaluation of recall and assessment of usage. Inclusion of engagement of nursing within the unit environment or relationship between IT and nursing with metrics related to IT security knowledge and usage. Evaluation of nursing involvement in IT security policy development with comparison to the result of IT security implementation and usage in the clinical environment.

Future research in the area of hacking would be to better understand what RNs learn and understand about hacking or what actions might lead to hacking. In this study, they had a mindset on specific topics that may have limited their openness on the topic of hacking. In depth inquiry into effects of hacking might serve as an area of future research related to the populations that healthcare organizations support and serve.

Implications

Positive social change as it relates to IT security has the potential to make a substantial impact in the healthcare arena. Following the findings of this study it is evident that the implications for social change remain ever present as they had been described earlier, with an essential need for protection of systems, including patient information and employee information. Any loss of integrity to the healthcare electronic systems allows for the loss of confidence by the public. Chen et al. (2013) discussed the complexity in the healthcare systems as being the cause for a lack of security that may allow for risk behavior related to electronic medical record handling. I previously presented the concept of the public perception of the protected health information security and confidence of the security of their individual files being of high importance. In the findings of this study, I was able to identify that the employees had a concern over their employee information being maintained securely both as an employee and as a patient if they were insured and cared for by the same organization. Organizational leadership teams will need to strategically plan for IT security to be incorporated into frontline workflow so that everyone is part of security management.

Significance to Practice

The findings of this study substantiated that for the RNs, as with most individuals, healthcare providers, and administrators, the aspects of security include the electronic medical record and the aspects of HIPAA, but they do not often think of the operational systems and management objectives that are required to secure the systems. The IT security system for organizational information is large and complex. The RNs were not aware of the complexity of the systems. The workflows did not match the IT security processes. Organizational leaders must manage and safeguard the employee practices as they relate to IT security, including workflows and authentication practices. When this mismatch occurs, a gap analysis will be helpful to reestablish risk assessment. Insight into how RNs practice and relate to IT security influences the development and security of system builds. This stronger insight and understanding of the RNs' use of the security applications will allow administrative and IT oversight to create an opportunity for engagement of the RNs in the development of the policy and procedure. Engaging the RNs will provide for policies to become more nurse, clinician, employee, and patient care friendly so that the healthcare organizations are less susceptible to risk. Security compliance will increase if barriers to using the IT security can be minimized. Insight into the RNs' perception was gained during this study and will be helpful in developing stronger processes.

Significance to Theory

In the workflow of nursing practice, the role of maintaining IT security is an elemental part of the RN role and was expected to be a finding in this study. It was not one of the findings. Thus, I would recommend that actions be taken to incorporate measures into IT security processes and RN workflow to achieve this objective.

Venkatesh et al. (2003) discussed UTAUT and the constructs but did not connect the IT security practices of employees with the perceptions of the four constructs that contribute to use behavior. The RNs' expressed a lack of understanding of IT security in this study. If there were to be an increase in understanding of the UTAUT constructs in a meaningful way the IT security would become more applicable in the operational setting.

Out of this work, I have developed a framework for reducing barriers in security practices that are necessary within the RN workflow, decreasing risk of protected health information release, and decreasing security breach for the organization. This framework is produced by providing knowledge areas for improvement to the overall security practice at the front line. The framework for improving IT security at the frontline is presented for implementation in clinical environment locations (see Figure 5).

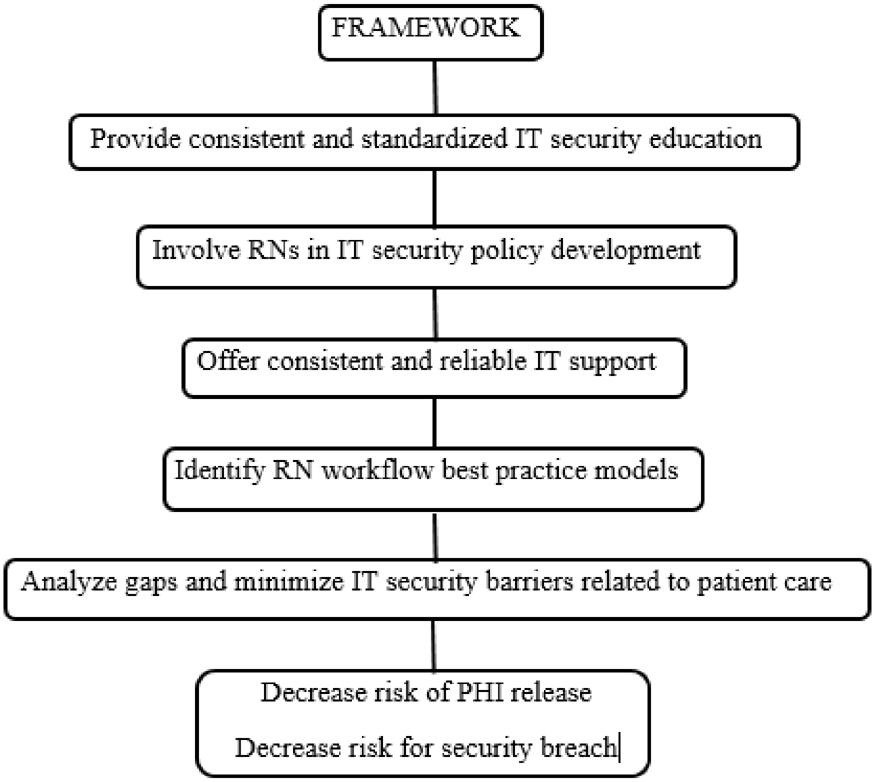

FRAMEWORK
Provide consistent and standardized IT security education
Involve RNs in IT security policy development
Offer consistent and reliable IT support
Identify RN workflow best practice models
Analyze gaps and minimize IT security barriers related to patient care
Decrease risk of PHI release
Decrease risk for security breach

Figure 5. Framework for IT security improvement. The healthcare clinical setting is unique with workflows that demand high level security processes, engaged and educated users.

Based on this work toward a framework, social change is likely to be promoted by helping employees to gain ease of use in the security practices. The change in the promotion of the security practices might be accomplished by minimizing barriers that will improve global security practice and reduce overall security breaches for the organization. Of importance to the clinical personnel, there will be an associated decrease for risk of protected health information release.

Significance to Social Change

Utilization behavior of the employee is determined through four of the constructs identified by Venkatesh et al. (2003). The purpose of IT security is only applicable if the employee perceives these to be important and purposeful for their practice. Identifying the gap between current theory and perception of RNs' related to IT security became evident in the findings of this study. These gaps will contribute to the knowledge contributions and implications for social change that can impact the healthcare industry. The security mishandling by nurses as described by both Albarrak (2012) and Medlin et al. (2008) in each of their respective studies was identified in an alternate style in this study along with other IT security mishandling situations. These security issues are occurring in a representative group from one of the largest subsets of the healthcare employees within healthcare organization thus creating exposure to risk.

Healthcare costs include the burden of technology costs, security, and breach recovery. Improvements in IT security processes within the healthcare arena would allow for a potential impact of cost reduction, patient safety, and patient satisfaction. Improving RNs' engagement within each of the constructs leading to improved use behavior would result in improved security protection and ultimately position healthcare for cost reductions as a result of the decreased breach and risk.

Maintaining the confidence of the general public and minimizing any concerns that they have related to potential security issues in an organization is important to the bottom line financially. Increasing the security within the healthcare organizations creates a more confident feeling for patients individually and extends to the global public. The work of identifying the RNs' perception with gained insight and potential for improvement of the IT security behavior and handling of security practices could become the catalyst to some of the change that is needed in healthcare security processes related to IT security and management. The changes that could be made as a result of the findings from this study are likely to extend to the community and promote increased patient confidence.

As the findings are disseminated, organizational leaders will implement change and include RNs in IT security planning. Confidence will grow. Two important aspects impact the research, positive social change may be fully realized as insights and recommendations are considered and adapted for the populations of clinical employees such as RNs. The first is that when users are more confident that information is secure they are more apt to use the electronic health record and with increased use, there is potential for maximizing healthcare delivery. Second, when organizations are able to reduce costs and resources used for security those resources can be deployed for other healthcare contributions such as providing additional disease prevention, community education, and further research toward healthcare advancements.

Conclusions

Albarrak (2012), Fernández-Alemán et al. (2015), and Medlin et al. (2008), each discussed the employee mishandling of IT security in their quantitative studies. There was a need to understand the lived experiences of those who use the IT security. In this study, I was able to hear the stories of what RNs experienced or believed about what their work was related to IT security. The interaction and observations that they had related to the topics of IT security were shared about situations and scenarios. The themes of data did identify sharing of accounts and lack of log-off when walking away from the computer. There was no report by any participant of direct sharing of passwords; however, there were consistent reports of awareness for teammates password sharing with a subset of participants' indirect involvement in that sharing practice within their respective work units. The summary of the RNs' shared information and experiences including that the patient care would always come first no matter what it takes to accomplish that mission. This was consistent with the findings that clinicians do not engage in IT security, including sharing passwords, before they allow harm to their patients (Koppel, Smith, Blythe, & Kothari, 2015). Ultimately, IT security will have to match the patient care workflow process or it will not be used.

References

Abelson, R, & Goldstein, M. (2015, Feb. 5). Anthem hacking points to security vulnerability of healthcare industry. *The New York Times*. Retrieved from http://www.nytimes.com/

Agaku, I., Adisa, A., Ayo-Yusuf, O., & Connolly, G. (2014). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association, 21*(2), 374-378. doi:10.1136/amiajnl-2013-002079

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams–Challenges in supporting the organisational security function. *Computers & Security, 31*(5), 643-652. doi:10.1016/j.cose.2012.04.001

Albarrak, A. I. (2012). Information security behavior among nurses in an academic hospital. *Health Med, 6*(7), 2349-2354. Retrieved from http://www.healthmed.ba/

Alsalamah, S., Gray, W. A., Hilton, J. C., & Alsalamah, H. (2013). Information security requirements in patient-centred healthcare supporting systems. *Studies in Health Technology and Informatics*, *192*, 812-816. doi:10.3233/978-1-61499-289-9-812

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). Towards a taxonomy of information security management practices in organisations. *ACIS*. doi:http://hdl.handle.net/10292/8174

Amerson, R. (2011). Making a case for the case study method. *Journal of Nursing Education, 50*(8), 427-428. doi:10.3928.01484834-20110719-01

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International Journal Internet and Enterprise Management,* 6, 279-310. doi:10.1504/ijiem.2010.035624

Arce, I. (2003). The weakest link revisited. *IEEE Security & Privacy*, *1*(2), 72-76. doi:10.1109/MSECP.2003.1193216

Baker, W. H., Goudie, M., Hutton, A., Hylender, C.D., Niemantsverdriet, J., Novak, C., … Tippett, P. (2011). "2011 data breach investigations report". Verizon RISK Team. Retrieved 9/4/2015 from: http://www.wired.com/images_blogs/threatlevel/2011/04/Verizon-2011-DBIR_04-13-11.pdf

Balbi, A. (2015). Massive cyber-attack at Anthem. *Strategic Finance*, *97*(3), 11. Retrieved from http://sfmagazine.com/

Balozian, P. & Leidner, D. (2016). IS security menace: When security creates insecurity. *AIS Electronic Library (AISeL)*. Retrieved from http://aisel.aisnet.org/icis2016/ISSecurity/Presentations/5/

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39*, 145-159. doi:10.1016/j.cose.2013.05.006

Bazeley, P., & Jackson, K. (Eds). (2013). *Qualitative data analysis with NVivo*. Thousand Oaks, CA: Sage Publications Limited.

Belanger, F. (2011). When users resist: How to change management and user resistance to password security. *Pamplin College of Business Magazine*. Retrieved from http://www.magazine.pamplin.vt.edu/fall11/passwordsecurity.html

Bernauer, J., Lichtman, M., Jacobs, C., & Robinson, S. (2013). Blending the old and the new: Qualitative data analysis as critical thinking and using NVivo with a generic approach. *The Qualitative Report*, *18*(31), 1-10. Retrieved from http://www.nova.edu/ssss/QR/QR18/bernauer2.pdf

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open, 2*, 8-14. doi:10.1016/j.npls.2016.01.001

Bigalke, J. (2009). Filling the healthcare IT gap by 2015. *Healthcare Financial Management: Journal of the Healthcare Financial Management Association*, *63*(6), 38-40. doi:19526817/196394293

Box, D., & Pottas, D. (2013). Improving information security behaviour in the healthcare context. *Procedia Technology*, *9*, 1093-1103. doi:10.1016/j.protcy.2013.12.122

Brutus, S., Aguinis, H., & Wassmer, U. (2013). Self-reported limitations and future directions in scholarly reports analysis and recommendations. *Journal of Management*, *39*(1), 48-75. doi:10.1177/0149206312455245

Cazier, J. A., & Medlin, B. D. (2006). How secure is your information system? An investigation into actual healthcare worker password practices. *Perspectives in Health Information Management/AHIMA, American Health Information Management Association*, *3*(8), 1-7. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2047302

Charles, D., Gabriel, M., & Furukawa, M. (2014, May). Adoption of electronic health record systems among U.S. non-federal acute care hospitals: 2008-2013, ONC Data Brief, no. 16. *Washington, DC: Office of the National Coordinator for Health Information Technology*.

Chen, Y., Nyemba, S., & Malin, B. (2012). Auditing medical records accesses via healthcare interaction networks. In AMIA Annual Symposium Proceedings (Vol. 2012, p. 93). *American Medical Informatics Association*. Retrieved from https://www.amia.org/amia2012.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447-459. doi:10.1016/j.cose.2013.09.009

Cheswick, W. (2013). Rethinking passwords. *Communications of the ACM, 56*(2), 40-44. doi:10.1145/2408776.2408790

Chopra, M. (2013). IT Security in hospital management. *Global Journal of Computer Science and Technology: Network, Web & Security, 13*(3), 1-7. Retrieved from http://computerresearch.org/stpr/index.php/gjcst

Clinician. (n.d.) In Merriam-Webster's collegiate dictionary. Retrieved from http://www.merriam-webster.com/dictionary/clinician

Crawford, M. (2014). Making data smart: Practical informatics is helping transform data into health intelligence, and now moving into day-to-day HIM work. *Journal of AHIMA*, 24-27. Retrieved from http://journal.ahima.org/2014/

Crowston, K., Allen, E. E., & Heckman, R. (2012). Using natural language processing technology for qualitative data analysis. *International Journal of Social Research Methodology, 15*(6), 523-543. doi:10.1080/13645579.2011.625764

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340. doi:10.2307/249008

Eddy, N. (March 19, 2014). Criminal attacks on health care organizations rise sharply. *Eweek*, Retrieved from http://www.eweek.com/it-management/criminal-attacks-on-health-care-organizations-rise-sharply.html

Ferguson, N., Schneier, B., & Kohno, T. (2011). *Cryptography engineering: Design principles and practical applications*. Indianapolis, IN: John Wiley & Sons.

Fernández-Alemán, J. L., Sánchez-Henarejos, A., Toval, A., Sánchez-García, A. B., Hernández-Hernández, I., & Fernandez-Luque, L. (2015). Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International journal of medical informatics*, *84*(6), 454-467. doi:10.1016/j.ijmedinf.2015.01.010

Finkle, J. (2014, April, 23). Exclusive: FBI warns healthcare sector vulnerable to cyber-attacks. Reuters. Edition: US. Retrieved from http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423

Fusch, P., & Ness, L. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9). Retrieved from http://tqr.nova.edu/

Gaunt, N. (2000). Practical approaches to creating a security culture. *Internal Journal of Medical Informatics, 62*, 51-78. doi:10.1016/s1386-5056(00)00115-5

Graham, C. (2010). HIPAA and HITECH compliance: An exploratory study of healthcare facilities ability to protect patient health information. *Proceedings of the Northeast Business & Economics Association*, 402-406. doi:10.2139/ssrn.2510105

Gunawan, J. (2016). Electronic health records in nursing practice: a concept analysis. *International Journal of Innovations in Medical Education and Research, 2*(1), 5-8. doi:10.5455/ijimer.2015.19082015012

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236. doi:10.2753/MIS0742-1222280208

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242-251. doi:10.1016/j.cose.2012.10.003

Halse, C., & Honey, A. (2014). Unraveling ethics: Illuminating the moral dilemmas of research ethics. *Signs, 40*(1). doi:10.1086/428419

Harper, M., & Cole, P. (2012). Member checking: can benefits be gained similar to group therapy?. *The Qualitative Report, 17*(2), 510-517. doi:10.1037/e530492014-001

Harris, M., & Furnell, S. (2012). Routes to security compliance: be good or be shamed? *Computer Fraud & Security*, *2012*(12), 12-20. doi:10.1016/S1361-3723(12)70122-7

Hebda, T., & Czar, P. (2013). *Handbook of informatics for nurses and healthcare professionals*. (5th ed). Boston: Pearson.

Hovenga, E. J. S., & Grain, H. (2013). Information security governance: A risk assessment approach to health information systems protection. *Health Information Governance in a Digital Environment*, *193*, 186. doi:10.3233/978-1-61499-291-2-186

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-660. doi:10.1111/j.1540-5915.2012.00361.x

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi:10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi:10.1016/j.im.2013.10.001

Institute for Health Care Improvement (IHI). (2015). *Improving patient safety*. Retrieved from http://www.ihi.org/IHI/Topics/PatientSafety/SafetyGeneral

Kashiwagi, D. T., Sexton, M. D., Graves, C. E. S., Johnson, J. M., Callies, B. I., Roger, C. Y., & Thompson, J. M. (2016). All CLEAR? Preparing for IT Downtime. *American Journal of Medical Quality*, 1062860616667546. doi:10.1177/1062860616667546

KFF. (2015, October). Total number of professionally active nurses. Kaiser Family Foundation. Retrieved from http://kff.org/other/state-indicator/total-registered-nurses/

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal*, 2014. Retrieved from http://www.hindawi.com/journals/tswj/

Kirby, S.B. (2015). Informatics leadership: The role of the CNIO. *Nursing 2015*, 21-22. doi:10.1097/01.NURSE.0000462394.23939.8e

Koivunen, M., Niemi, A., & Hupli, M. (2014). The use of electronic devices for communication with colleagues and other healthcare professionals–nursing professionals' perspectives. *Journal of Advanced Nursing*. doi:10.1111/jan.12529

Koloroutis, M. (2004). *Relationship based care: A model for transforming practice.* (Koloroutis, Mary, Ed.). Minneapolis: Creative Health Care Management, Inc.

Koppel, R., Smith, S. W., Blythe, J., & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: you want my password or a dead patient?. *Studies in health technology and informatics*, *208*, 215. doi:10.1007/978-3-319-20765-0_6

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics, 38*(2), 143-154. doi:10.1016/j.apergo.2006.03.010

Kruger, D., & Anschutz, T. (2013). A new approach to IT security. *Healthcare financial management: Journal of the Healthcare Financial Management Association, 67*(2), 104-6. doi:23413677/1313524602

Kwon, J., & Johnson, M. E. (2012). Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*. doi:10.1136/amiajnl-2012-000906

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *Mis Quarterly*, *38*(2), 451-471. Retrieved from http://www.misq.org/

Landolt, S., Hirschel, J., Schlienger, T., Businger, W., & Zbinden, A. M. (2012). Assessing and comparing information security in swiss hospitals. *Interactive journal of medical research, 1*(2):e11. doi:10.2196/ijmr.2137

Li, X., Wen, Q., Li, W., Zhang, H., & Jin, Z. (2014). Secure privacy-preserving biometric authentication scheme for telecare medicine information systems. *Journal of medical systems, 38*(11), 1-8. Retrieved from http://www.springer.com/public+health/journal/10916

Liu, C. H., Chung, Y. F., Chen, T. S., & Wang, S. D. (2012). The enhancement of security in healthcare information systems. *Journal of medical systems, 36*(3), 1673-1688. doi:10.1007/s10916-010-9628-3

Marshall, C., & Rossman, G. B. (2016). Designing qualitative research (6th ed.) [Kindle version]. Retrieved from http://www.amazon.com

Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of U.S. hospitals to social engineering attacks: How many of your employees would share their password? *International Journal of Information Security and Privacy*, *2*(3), 71-83. doi:10.4018/jisp.2008070106

Merriam, S. B. (2014). *Qualitative research: A guide to design and implementation*. San Fransisco, CA: John Wiley & Sons.

Milenković, I., Latinović, O., & Simić, D. (2013). Using Kerberos protocol for single sign-on in identity management systems. *Journal Of Information Technology & Applications, 3*(1), 27-33. doi:10.7251/JIT1301027M

Murphy, J. (2011). The nursing informatics workforce: Who are they and what do they do? *Nursing Economics, 29*(3), 150-153. Retrieved from http://www.nursingeconomics.net/cgi-bin/WebObjects/NECJournal.woa

n.a. (2015, May 7). Criminal attacks are now leading cause of data breach in healthcare, according to new Ponemon study. [Whitepaper] Ponemon Institute. Retrieved from http://www.ponemon.org/news-2/66

n.a. (2015, October). State of cybersecurity in local, state & federal government. [Whitepaper] Ponemon Institute. Retrieved from https://fcw.com/whitepapers/2015/10/hpsp-state-cybersecurity-government-100115/asset.aspx?tc=assetpg

n.a., (2014, December 9). *National health expenditures 2013 highlights*. Centers for Medicare and Medicaid Services. Retrieved from http://www.cms.gov/Research-

Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsHistorical.html

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence Based Nursing, 18*(2), 34-35. doi:10.1136/eb-2015-102054

O'Harrow, R. (2012, December 25). Health-care sector vulnerable to hackers, researchers say. *The Washington Post*. Retrieved from http://www.washingtonpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html

ONC. (2015). Health IT quick stats. *Health IT. gov: Dashboard*. Retrieved from http://dashboard.healthit.gov/quickstats/quickstats.php

Peredaryenko, M. S., & Krauss, S. E. (2013). Calibrating the human instrument: understanding the interviewing experience of novice qualitative researchers. *The Qualitative Report, 18*(85), 1-17. Retrieved from http://www.nova.edu/ssss/QR/QR18/peredaryenko85.pdf

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, 63, 539-569. Retrieved from http://www.annualreviews.org/journal/psych

Rack, L., Dudjak, L., & Wolf, G. (2012). Study of nurse workarounds in a hospital using bar code medication administration system. *Journal of Nursing Care Quality. 27*(3), 232–239. doi:10.1097/ncq.0b013e318240a854

Rajarajan, S., Prabhu, M., Palanivel, S., & Karthikeyan, M. P. (2014). GRAMAP: Three stage graphical password authentication scheme. *Journal Of Theoretical & Applied Information Technology, 61*(2), 262-269. Retrieved from http://www.jatit.org/

Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership?. *Information Management & Computer Security*. *20*(4), 296-311. doi:10.1108/09685221211267666

Rogers, E. M., (2003) *Diffusion of innovations*, (5th ed.). New York, NY: Free Press. 1995.

Rogers, E. M. (2004). A prospective and retrospective look at the diffusion model. *Journal of Health Communication*, *9*(S1), 13-19. doi:10.1080/10810730490271449

Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal*, *42*(6), 32-38. Retrieved from ProQuest. doi:14872/227758486

Salmela S., Eriksson K. & Fagerstrom L. (2012). Leading change: A three dimensional model of nurse leaders' main tasks and roles during a change process. *Journal of Advanced Nursing. 68*(2), 423–433. doi:10.1111/j.1365-2648.2011. 05802.x

Schwartze, J., Haarbrandt, B., Fortmeier, D., Haux, R., & Seidel, C. (2014). Authentication systems for securing clinical documentation workflows. *Methods of Information in Medicine, 53*(1), 3-13. doi:10.3414/ME12-01-0078

Seidman, I. (2013). *Interviewing as qualitative research: A guide for researchers in education and the social sciences*. Teachers college press.

Sethi, N., Lane, G., Newton, S., Egan, P., & Ghosh, S. (2014). Disaster easily averted? Data confidentiality and the hospital desktop computer. *International Journal of Medical Informatics*. *83*(5), 385-91. doi:10.1016/j.ijmedinf.2014.02.002

Sharma, S., & Sugumaran, V. (2011). A framework for enhancing systems security. *Journal of Information Privacy and Security*, *7*(4), 3-22. doi:10.1080/15536548.2011.10855921

Simpson, R. (1996). Technology: nursing the system. Security threats are usually an inside job. *Nursing Management*, *27*(12), 43. doi:10.1097/00006247-199612000-00010

Sochalski, J., & Weiner, J. (2011). Health care system reform and the nursing workforce: Matching nursing practice and skills to future needs, not past demands. *The Future of Nursing: Leading Change, Advancing Health*, 375-398. Retrieved from http://veterans.iom.edu/~/media/Files/Activity%20Files/Workforce/Nursing/Health%20Care%20System%20Reform%20and%20the%20Nursing%20Workforce.pdf

Sockolow, P. S., Rogers, M., Bowles, K. H., Hand, K. E., & George, J. (2014). Challenges and facilitators to nurse use of a guideline-based nursing information system: Recommendations for nurse executives. *Applied Nursing Research*, *27*(1), 25-32. doi:10.1016/j.apnr.2013.10.005

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302. doi:10.1016/j.im.2011.07.002

Sorsa, M. A., Kiikkala, I., & Astet-Kurki, P. (2015). Bracketing as a skill in conducting unstructured qualitative interviews. *Nurse Researcher*, *22*(4), 8-12. doi:10.7748/nr.22.4.8.e1317

Tam, L. L., Glassman, M. M., & Vandenwauver, M. M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233-244. doi:10.1080/01449290903121386

Thomas, E., & Magilvy, J. K. (2011). Qualitative rigor or research validity in qualitative research. *Journal for Specialists in Pediatric Nursing*, *16*(2), 151-155. doi:10.1111/j.1744-6155.2011.00283.x

Tufford, L., & Newman, P. (2012). Bracketing in qualitative research. *Qualitative Social Work, 11*(1), 80-96. doi:10.1177/1473325010368316

Umphress, E. E., & Bingham, J. B. (2011). When employees do bad things for good reasons: Examining unethical pro-organizational behaviors. *Organization Science, 22*(3), 621-640. doi:10.1287/orsc.1100.055

U.S. Census Bureau. (2010). *Aging boomers will increase dependency ratio.* U. S. Census Bureau Projects. Accessed June 28, 2015 from http://www.census.gov/newsroom/releases/archives/aging_population/cb10-72.html

Vance, A., Lowry, P., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263-290. doi:10.2753/MIS0742-1222290410

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management science*, *46*(2), 186-204. doi:10.1287/mnsc.46.2.186.11926

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478. doi:14872/218137148

Welton, J. (2011). Hospital nursing workforce costs, wages, occupational mix, and resource utilization. *Journal Of Nursing Administration*, *41*(7/8), 309-314. doi:10.1097/NNA.0b013e3182250a2b

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science & Technology, 58*(2), 212-222. doi:10.1002/asi.20474

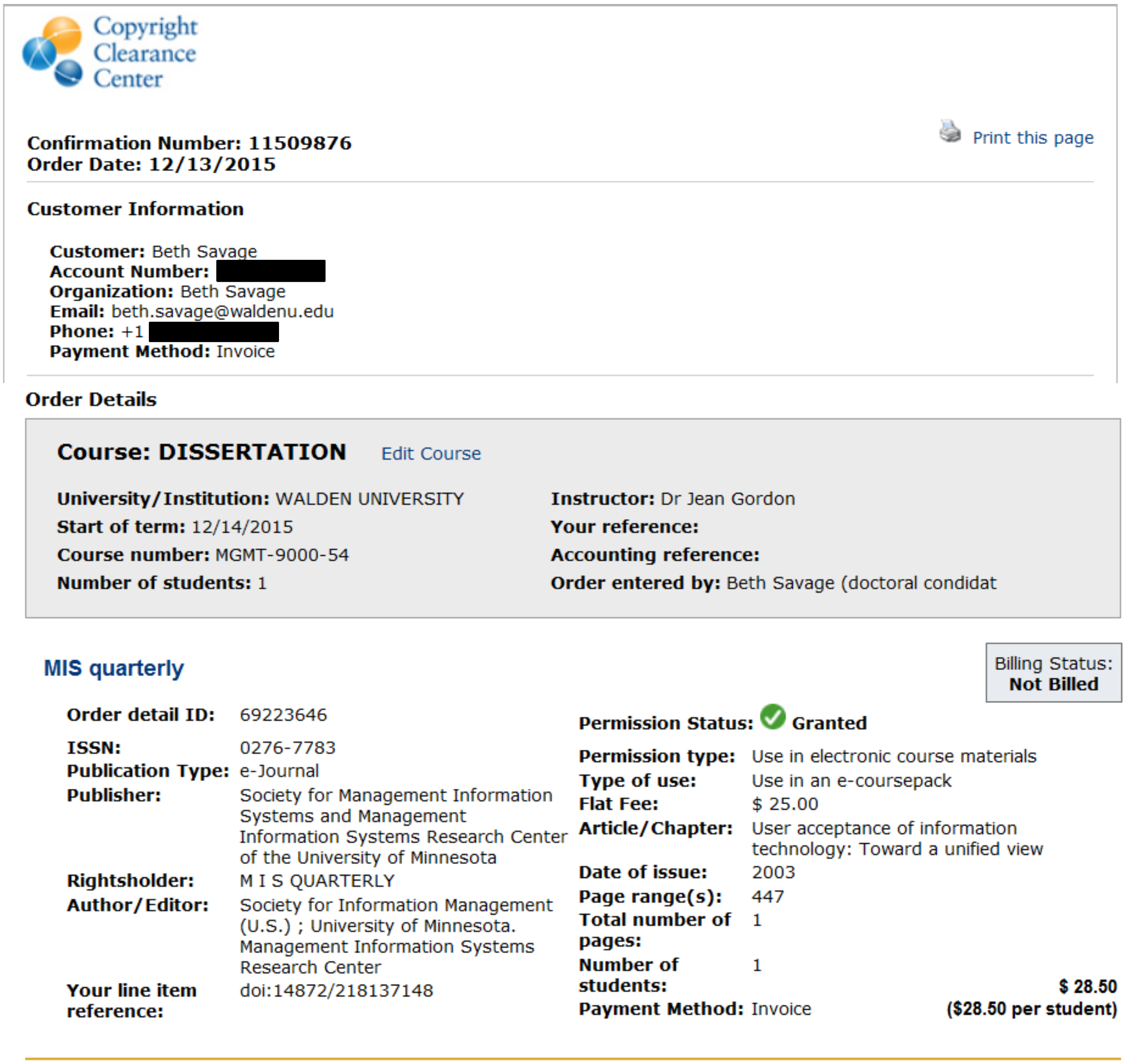
Workman, M., Bommer, W., & Straub, D. (2009). The amplification effects of procedural justice on a threat control model of information systems security behaviours. *Behaviour & Information Technology*, *28*(6), 563-575. doi:10.1080/01449290802556021

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. Information Technology & People, *26*(4), 401-419. doi:10.1108/ITP-12-2012-0147

Zafar, H., Ko, M. S., & Clark, J. G. (2014). Security Risk Management in Healthcare: A Case Study. *Communications of the Association for Information Systems, 34*(1), Article 37. Retrieved from http://aisel.aisnet.org/cais/

Zheng, K., Haftel, H. M., Hirschl, R. B., O'Reilly, M., & Hanauer, D. A. (2010). Quantifying the impact of health IT implementations on clinical workflow: A new methodological perspective. *Journal of the American Medical Informatics Association*, *17*(4), 454-461. doi:10.1136/jamia.2010.004440

Appendix A: Permission for Use of Figure 1



Copyright Clearance Center

Print this page

Confirmation Number: 11509876
Order Date: 12/13/2015

Customer Information

Customer: Beth Savage
Account Number: [redacted]
Organization: Beth Savage
Email: beth.savage@waldenu.edu
Phone: +1 [redacted]
Payment Method: Invoice

Order Details

Course: DISSERTATION Edit Course

University/Institution: WALDEN UNIVERSITY	**Instructor:** Dr Jean Gordon
Start of term: 12/14/2015	**Your reference:**
Course number: MGMT-9000-54	**Accounting reference:**
Number of students: 1	**Order entered by:** Beth Savage (doctoral condidat

MIS quarterly

Billing Status:
Not Billed

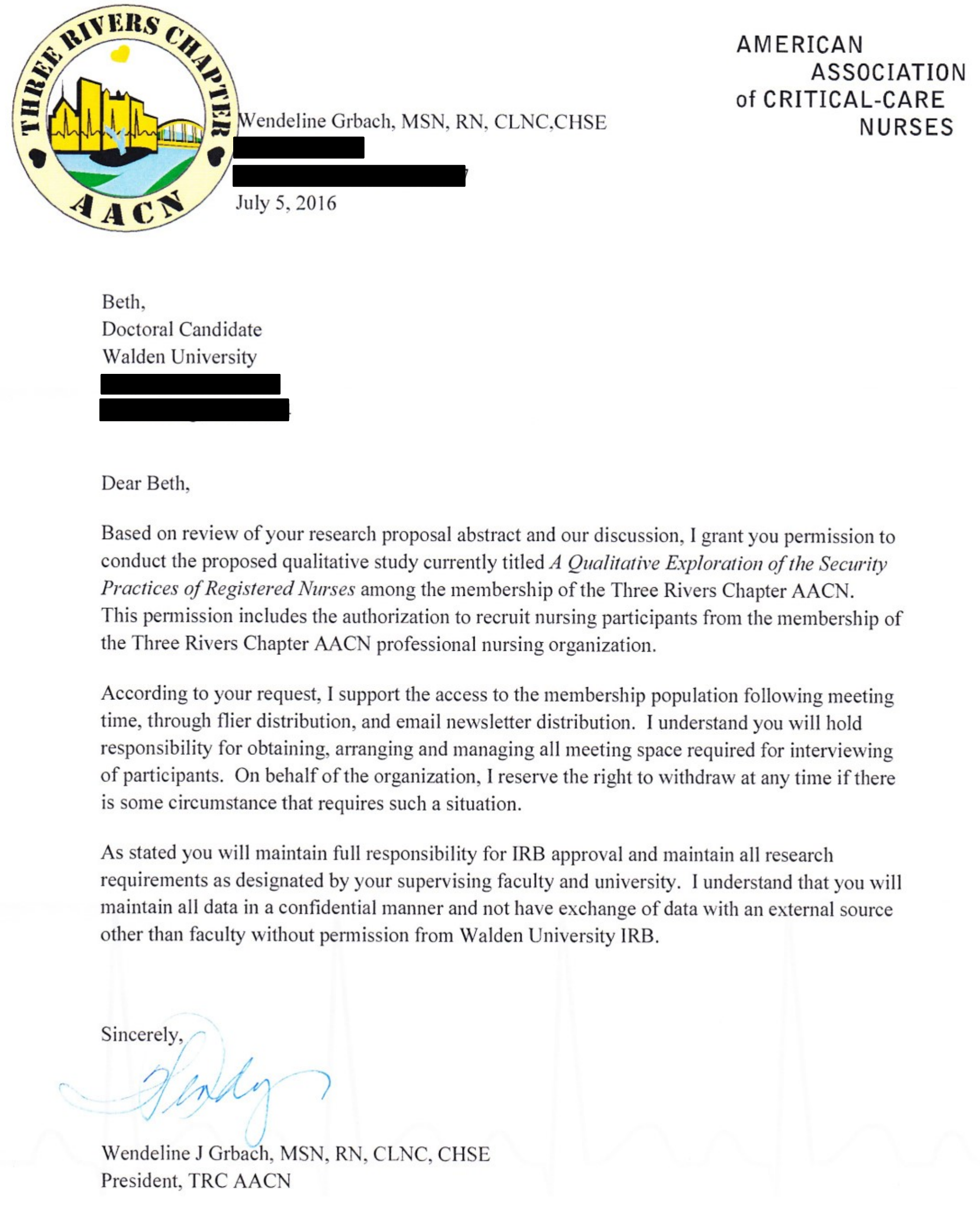
Order detail ID:	69223646
ISSN:	0276-7783
Publication Type:	e-Journal
Publisher:	Society for Management Information Systems and Management Information Systems Research Center of the University of Minnesota
Rightsholder:	M I S QUARTERLY
Author/Editor:	Society for Information Management (U.S.) ; University of Minnesota. Management Information Systems Research Center
Your line item reference:	doi:14872/218137148

Permission Status: ✓ **Granted**

Permission type:	Use in electronic course materials
Type of use:	Use in an e-coursepack
Flat Fee:	$ 25.00
Article/Chapter:	User acceptance of information technology: Toward a unified view
Date of issue:	2003
Page range(s):	447
Total number of pages:	1
Number of students:	1
Payment Method:	Invoice

$ 28.50
($28.50 per student)

Appendix B: Letter of Agreement



THREE RIVERS CHAPTER AACN

Wendeline Grbach, MSN, RN, CLNC,CHSE
[redacted]
July 5, 2016

AMERICAN
ASSOCIATION
of CRITICAL-CARE
NURSES

Beth,
Doctoral Candidate
Walden University
[redacted]

Dear Beth,

Based on review of your research proposal abstract and our discussion, I grant you permission to conduct the proposed qualitative study currently titled *A Qualitative Exploration of the Security Practices of Registered Nurses* among the membership of the Three Rivers Chapter AACN. This permission includes the authorization to recruit nursing participants from the membership of the Three Rivers Chapter AACN professional nursing organization.

According to your request, I support the access to the membership population following meeting time, through flier distribution, and email newsletter distribution. I understand you will hold responsibility for obtaining, arranging and managing all meeting space required for interviewing of participants. On behalf of the organization, I reserve the right to withdraw at any time if there is some circumstance that requires such a situation.

As stated you will maintain full responsibility for IRB approval and maintain all research requirements as designated by your supervising faculty and university. I understand that you will maintain all data in a confidential manner and not have exchange of data with an external source other than faculty without permission from Walden University IRB.

Sincerely,

Wendy

Wendeline J Grbach, MSN, RN, CLNC, CHSE
President, TRC AACN

Appendix C: Expert Panel Participation Request Email

Title: Expert Panel Participation Request

Dear [Participant Reviewer],

I am currently a doctoral candidate in the College of Management at Walden University studying Information Management Systems. I am conducting a dissertation study titled *A Qualitative Exploration of the Security Practices of Registered Nurses*. I would be very appreciative if you would assist me in the evaluation and validation of the qualitative interview tool for use in this research.

The purpose of this interview is to explore the lived experiences of the nurse related to Information Technology (IT) security. The interview is constructed to correlate with the unified theory of acceptance and usage of technology (UTAUT) constructs to identify the registered nurses' perceptions, expressed intentions, and self-reported behaviors of IT security.

The Interview Questions and Critique Form are attached for your review. Following my receipt of all edits and comments, I will forward a final revised copy to you for review. Please feel free to contact me with any questions at XXX XXX-XXXX or email beth.savage@xxxx.xxx.

I look forward to your participation in creating a quality interview tool. Thank you.

Beth Savage

Attachments

Interview Questions
Critique Form

Appendix D: Interview Questions

I. Can you tell me about a time during your workday, if any, when you have walked away from the computer without logging off?
   a. Do you know if anyone has ever used your account?
   b. Are you aware of any safeguards in place to protect you when you walk away without logging off?
   c. Is it a norm in your unit to log-off or not log-off when walking away from the computer?

II. What challenges, if any, have you had related to your password?
   a. How easy is it for you to use your password?
   b. Have you ever shared your account/password with coworkers?
   c. In what clinical situations, if any, would sharing your account/password occur?
   d. What benefit or reward is there to sharing an account/password?
   e. Do passwords support your workflow?

III. What measures do you take to manage your password?
   a. When you develop or change your password what is it composed of? (i.e. digits, letters, symbols, minimum eight characters?)
   b. What do you do when someone else knows your password?
   c. How do you remember your password?
   d. How often do you change it?
   e. Do you ever worry about your password?

IIII. Can you tell me about your orientation, unit education, or hospital policies related to IT security?
   a. Do you recall anything specific in your orientation?
   b. Have you been to any recent education for IT security?
   c. Does anyone on your unit talk about IT security?
   d. Have you participated in a policy review for IT security?

V. Can you tell me who, if anyone, you would call if you had questions about the security of your password or your account?
   a. Do you have confidence that your concerns would be taken seriously?
   b. Are you, or have you ever been concerned that your system is not secure?
   c. Whose role is it to maintain the security of the electronic system?

VI. As you perceive different levels of IT security, very secure to not secure, is there a difference in your work environment?
   a. If the system is more secure, does that make your job better?
   b. Do you believe you are expected to know IT security as part of your job?
   c. What do you believe is the practice of your teammates when handling passwords and sharing accounts?

VII. In what way, if any, do you believe that the employees' actions at the computer or with a password has any association when hacking occurs in an organization?
   a. In what ways could the password handling lead to hacking?
   b. What, if any, would the impact be to the employees?
   c. What, if any, would the impact be to the patients?
   d. What, if any, would the impact be to the organization?

VIII. What do you perceive as other aspects of IT security that I should be aware of from your experience with IT security in your work?