

Molloy College

DigitalCommons@Molloy

---

Theses & Dissertations

---

5-3-2018

## Health Information Security and Privacy: A Social Science Exploration of Nurses' Knowledge and Risk Behaviors with Security and Privacy Issues Focusing on Mobile Device Usage

Keith Richard Weiner

Molloy College, [kweiner1@molloy.edu](mailto:kweiner1@molloy.edu)

Follow this and additional works at: <https://digitalcommons.molloy.edu/etd>



Part of the [Nursing Commons](#)

This Dissertation has All Rights Reserved. [DigitalCommons@Molloy Feedback](#)

---

### Recommended Citation

Weiner, Keith Richard, "Health Information Security and Privacy: A Social Science Exploration of Nurses' Knowledge and Risk Behaviors with Security and Privacy Issues Focusing on Mobile Device Usage" (2018). *Theses & Dissertations*. 75.

<https://digitalcommons.molloy.edu/etd/75>

This Dissertation is brought to you for free and open access by DigitalCommons@Molloy. It has been accepted for inclusion in Theses & Dissertations by an authorized administrator of DigitalCommons@Molloy. For more information, please contact [tochter@molloy.edu](mailto:tochter@molloy.edu), [thasin@molloy.edu](mailto:thasin@molloy.edu).

Molloy College

Barbara H. Hagan School of Nursing

PhD in Nursing Program

HEALTH INFORMATION SECURITY AND PRIVACY: A SOCIAL SCIENCE  
EXPLORATION OF NURSES' KNOWLEDGE AND RISK BEHAVIORS WITH SECURITY  
AND PRIVACY ISSUES FOCUSING ON MOBILE DEVICE USAGE

a dissertation

by

KEITH RICHARD WEINER

submitted in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

May 3, 2018

© Copyright by KEITH WEINER

All Rights Reserved

2018

MOLLOY COLLEGE

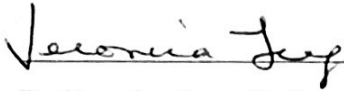
THE BARBARA H. HAGAN SCHOOL OF NURSING

The dissertation of Keith Richard Weiner

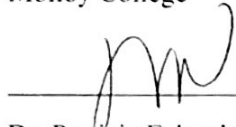
Entitled HEALTH INFORMATION SECURITY AND PRIVACY: A SOCIAL SCIENCE EXPLORATION OF NURSES' KNOWLEDGE AND RISK BEHAVIORS WITH SECURITY AND PRIVACY ISSUES FOCUSING ON MOBILE DEVICE USAGE in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

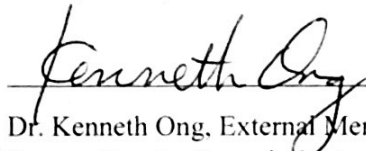
In The Barbara H. Hagan School of Nursing has been read and approved by the Committee:



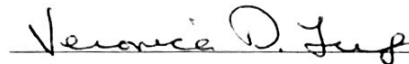
Dr. Veronica Feeg, Chairperson  
Professor, Barbara H. Hagan School of Nursing  
Molloy College



Dr. Patricia Eckardt, Member  
Associate Professor, Barbara H. Hagan School of Nursing  
Molloy College



Dr. Kenneth Ong, External Member  
Former Deputy Commissioner of Disease Intervention, New York City Department of Health  
Former Member Board of Directors, Healthcare Information and Management Systems Society  
Former Chief Medical Informatics Officer, NewYork-Presbyterian/Queens



Veronica D. Feeg, PhD, RN, FAAN  
Associate Dean and Director  
PhD Program in Nursing

Date: May 3, 2018

## Abstract

**Background.** Health information system security and privacy are critical issues that impact the wide use of the Electronic Health Record (EHR) in healthcare including hospitals, providers and health systems (Breaches Affecting 500 or More Individuals, 2017). These issues have been researched from a technology standpoint in this era of accelerated electronic health record adoption, but less has been done related to the EHR users in the United States. Most of the literature related to security and privacy explores research topics, peripheral and direct, regarding policy adherence mechanisms. Yet to be studied is a social science exploration of nurses' risk knowledge and risk behaviors associated with security and privacy issues.

**Purpose.** This dissertation examines characteristics related to cybersecurity practices of new nurses a year following graduation from nursing school where they may have been prepared to work in environments with EHRs. The study will explore their understanding of cybersecurity as it relates to use and protection of the sources of information in the EHRs, and their own personal risk behaviors with mobile technologies that may put them at risk to outside hacking or misuse of information. The questions that drive the study are the associations with nurses' knowledge of information system security, risk behaviors specifically with mobile device use, and their threat appraisal that may influence their personal habits and their concern for potential misuse of their own electronic health information.

**Method.** A web-based survey was emailed to a sample of new graduates who completed the National Student Nurses' Association (NSNA) Annual Survey and gave their permanent email address voluntarily to be contacted again for additional surveys. The survey designed in SurveyMonkey®, the same approach used with this sample in prior studies, was sent to a list of 3,000 addresses. The variables of interest are *Knowledge of Information System Security (KISS)*,

*Risk Behaviors (RB), Personal Technology Practices (PTP), Mobile Device Habits (MDH), Threat Appraisal (Internal and External), Concern for Information Privacy (CFIP), and Information Privacy Protection Response (IPPR).*

**Pilot Testing.** Several measures developed for the study were tested on a sample of senior graduating nursing students (n=167) to assess their validity and reliability, including KISS, RB and PTP. Prior to data collection, the new items were assessed for content validity by five judges in preparation to be tested for reliability analysis. A paper-pencil version of the new items was distributed to the nursing students just prior to their graduation. Their responses were entered and analyzed using SPSS, which yielded a final set of items with acceptable reliability ( $\alpha = .700$ ). These new items were combined with the other variables of previously studied items, slightly modified, for integration on the final tool. Additional demographic questions and mobile device usage were added.

**Procedures.** The final survey was distributed to the list of participants (n=3,000), anticipating a 10 - 20% return rate that would yield 300 - 600 subjects. A reminder was sent every 2 weeks for 6 weeks while the study remained open. Participants were offered an incentive of being eligible for a \$250 drawing at the conclusion of the study.

**Analysis.** The first level of analysis included an extensive descriptive analysis of the frequencies and measures of central tendency for subject self-reported mobile device frequency and types of use. The subsequent analysis included a series of correlations calculated on the variables of interest to determine the relationships of predicted relationships. The model did not support the predictions and an adjusted model was proposed for future studies on the measured variables and demographic variables of interest.

**Limitations.** The pilot study was distributed in a paper format whereas the proposed format for the national study used an electronic medium.

**Conclusions.** This study provided information about the relationship between the core variables and demographic components. These findings could inform educators and employers about new nurses' knowledge and risk behaviors related to information system security.

*Keywords:* Electronic Health Record, Protection Motivation Theory, Security, Privacy, Informatics, Meaningful Use, ARRA, HITECH, Cybersecurity, Risk

## Acknowledgements

I would like to acknowledge all of my family, friends, colleagues, teachers, students, acquaintances, and other kind souls who have in effect been mentors guiding me through my journey. I recognize the importance of those who have contributed to our body of knowledge through the ages and of those who will make great strides in the future. I am also eternally grateful for those who selflessly work toward making their part of the world a better place whether through education, research, healthcare, charity, or other means.

Specifically related to this dissertation, I would like to thank the National Student Nurses' Association and its members for their collaboration, the researchers who granted permission to build upon their work, my esteemed committee members (Drs. Veronica Feeg, Patricia Eckardt, and Kenneth Ong), and the people who make Molloy College a truly majestic institution.



# Table of Contents

Abstract.....	i
Acknowledgements .....	iv
Table of Figures.....	ix
Table of Tables .....	x
Chapter 1: Introduction.....	1
Background of the Problem .....	3
Background: Knowledge and Risk Behaviors.....	4
Significance of the Problem .....	7
Problem Statement.....	10
Study Aim.....	11
Purpose .....	11
Research Questions .....	12
Proposed Model for the Study .....	13
Concern For Information Privacy Subscale Definitions .....	14
Conceptual Definitions of Variables .....	15
Conceptual Definitions of Dependent Variables .....	16
Summary.....	16
Chapter 2: Review of Literature .....	17
Introduction .....	17
HIPAA Rules In Action.....	18
Security Breach – Privacy Violations.....	21
Social Engineering Behaviors – For Bad and For Good .....	23
Theoretical Framework: Rogers’ Protection Motivation Theory .....	29
Violation of Information Privacy Responses .....	31
Medical Students’ Knowledge of Privacy and Security.....	34
Fuzzy Logic of Cyber Security Knowledge .....	37
Social Engineering.....	39
Systematic Technical Perspective Review of Electronic Health Record Systems .....	42
Nursing Education: National Student Nurses’ Association (NSNA) .....	44
Nursing Education: National Council of State Boards of Nursing (NCSB) .....	45
Summary.....	46
Chapter 3: Methods .....	47
Introduction .....	47

The Pilot Study to Develop the Measures – Study Variables .....	47
Pilot – Data Collection .....	49
Sample .....	49
Design and Instrument Development .....	50
Procedures .....	51
Content Validity Index and Item Elimination Process .....	51
Knowledge Instrument Item Elimination .....	52
Human Protection .....	53
Reliability Statistics Methodology .....	54
Reliability Statistics – Knowledge Test .....	54
Reliability Statistics – Risk Behaviors .....	54
Reliability of Investigator Developed Measures .....	54
Reliability Statistics – Concern for Information Protection (CFIP) Total and IPPR .....	56
Reliability Statistics – CFIP Subscales.....	56
The Full National Study .....	56
Sample .....	57
National Student Nurses Association Membership .....	57
Method.....	58
Population Studied.....	58
Sample .....	58
Recruitment Method.....	59
Variables Specified – Instrument Items (Appendix I – Survey Instrument (National Survey)).....	59
Relational Variables .....	61
Procedure .....	61
Data Collection Methods .....	61
Hypotheses .....	61
Hypothesis Statements.....	62
Threat Appraisals – Stated in the Null .....	64
Ethical Consideration and Consent – Human Subject Protection .....	64
Chapter 4: Findings .....	66
Introduction .....	66
Characteristics and Demographics .....	67
Phone Characteristics .....	70
Descriptive Findings of The Study.....	72

Mobile Application Use .....	72
Security Practice Results .....	74
Level of Knowledge .....	76
Level of Risk .....	79
Information Privacy Protection Responses and Concern For Information Privacy .....	82
Reliability of All Measurement Scales .....	83
Reported Threat Appraisal – “Worry” About a Consequence – Ranked Groups .....	84
Question: Is Knowledge a Predictor of Risk and Concern for Information Privacy Total and Factors?.....	86
Knowledge Related To Risk.....	87
Knowledge Related To Concern For Information Privacy.....	88
Question: Are Risk Behaviors Related to Concern for Information Privacy Total and Factors?.....	89
Question: Is Threat Appraisal Associated with Knowledge, Risk, Concern for Information Privacy Total and Factors, and Personal Protective Responses? .....	91
Threat – Internal and External .....	92
Threat of Nurse Fine.....	92
Threat of Job Loss .....	94
Threat To Patient Privacy .....	95
Threat of Hospital Fine.....	96
Hypothesis Testing: Demographic Variables .....	97
Differences in Knowledge, Risk, and Concern for Information Privacy and Protective Responses .....	97
Age Related To Knowledge, Risk Behaviors.....	98
Age Related To Time Spent Using Mobile Device .....	100
Age Related To Activity Type .....	100
Education Related To Knowledge, Risk Behaviors, CFIP, and IPPR.....	101
Conclusion .....	103
Chapter 5: Discussion.....	105
Introduction .....	105
Characteristics and Demographics .....	105
Phone Characteristics .....	109
Descriptive Findings of the Study .....	111
Mobile Application Use .....	112
Security Practice Results .....	113

Level of Knowledge .....	114
Level of Risk .....	116
Information Privacy Protection Responses and Concern for Information Privacy .....	118
Reliability of All Measurement Scales .....	119
Reported Threat Appraisal – “Worry” About a Consequence – Ranked Groups .....	120
Question: Is Knowledge a Predictor of Risk and Concern for Information Privacy Total and Factors?.....	120
Knowledge Related To Risk.....	120
Knowledge Related To Concern For Information Privacy .....	121
Question: Are Risk Behaviors Related to Concern for Information Privacy Total and Factors?.....	121
Question: Is Threat Appraisal Associated with Knowledge, Risk, Concern for Information Privacy Total and Factors, and Personal Protective Responses? .....	122
Threat – Internal and External .....	122
Hypothesis Testing: Demographic Variables .....	123
Differences in Knowledge, Risk, and Concern for Information Privacy and Protective Responses .....	123
Age Related To Knowledge, Risk Behaviors .....	123
Education Related To Knowledge, Risk Behaviors, CFIP, and IPPR.....	124
Limitations.....	125
Conclusion .....	126
References .....	131
Appendix A – Study Permission Fuzzy Logic .....	137
Appendix B – Fuzzy Logic Materials .....	138
Appendix C – Study Permission Violation of Information Security .....	139
Appendix D – Molloy College Institution Review Board Approval.....	140
Appendix E - Pilot Survey .....	141
Appendix F – Abbreviation Definitions .....	153
Appendix G – National Student Nurse Association Social Media Guidelines .....	154
Appendix H - Content Validity: Student Nurses’ Knowledge of Information System Security and Risk Behaviors.....	155
Appendix I – Survey Instrument (National Survey).....	164
Appendix J – Knowledge Test and Results Key .....	182
Appendix K – Survey Raffle .....	188

## Table of Figures

Figure 1 Information Privacy Protective Responses Pathway .....	14
Figure 2 Key Endeavors of Healthcare Organizations and Practices Information Systems Managers (Ong, 2015) .....	20
Figure 3 Sample - Levels of Administrative Safeguards (Ong, 2015) .....	25
Figure 4 Sample - Levels of Physical Safeguards (Ong, 2015) .....	25
Figure 5 Sample - Levels of Technical Safeguards (Ong, 2015) .....	26
Figure 6 Office for Civil Right Facilitates Privacy and Security (Ong, 2015).....	27
Figure 7 Elimination of Knowledge Items .....	53
Figure 8 Descriptive Variables and Aggregate Measures .....	60
Figure 9 Knowledge Score Frequency Chart .....	79
Figure 10 Risk Habit Score Frequency Distribution .....	82
Figure 11 Permission: Fuzzy Assessment of Health Information System Users Security Awareness Survey and Study .....	137
Figure 12 Permission: Fuzzy Assessment of Health Information System Users Security Awareness Survey and Study With Materials .....	138
Figure 13 Permission: How Patients Respond To Violation of Their Information Privacy .....	139
Figure 14 Molloy Institution Review Board Approval Letter .....	140
Figure 15 NSNA Social Media Guidelines .....	154

## Table of Tables

Table 1 Threat Appraisal Taxonomy .....	55
Table 2 Sample Characteristics .....	69
Table 3 Phone Operating System .....	70
Table 4 Phone Manufacturers .....	71
Table 5 Smart Phone Use By Feature .....	73
Table 6 Practice Results (By Percentage) .....	74
Table 7 Knowledge Score Descriptive Statistics .....	76
Table 8 Knowledge Results .....	78
Table 9 Risk Behavior Score Descriptive Statistics .....	80
Table 10 Risk Behaviors Results .....	81
Table 11 CFIP and IPPR Descriptive Statistics .....	83
Table 12 Instrument Reliability - Pilot and Current Study .....	84
Table 13 Threat Appraisal Taxonomy .....	85
Table 14 Threat Rankings – Frequency of The Responses .....	85
Table 15 Risk Behaviors Related To Knowledge .....	87
Table 16 Knowledge related to CFIP and IPPR .....	88
Table 17 Risk Behaviors related to CFIP and IPPR .....	90
Table 18 Threat of fine ranks on differences in knowledge, risk behaviors, IPPR, and CFIP .....	93
Table 19 Threat of fine level related to knowledge scores .....	93
Table 20 Threat of job loss ranks on differences in knowledge, risk behaviors, IPPR, and CFIP .....	94
Table 21 Threat to patient privacy related to knowledge, risk behaviors, IPPR, and CFIP .....	95
Table 22 Threat of hospital fine related to knowledge, risk behaviors, IPPR, and CFIP .....	96
Table 23 Age related to knowledge, risk, concern and personal protective responses .....	99
Table 24 Age related to time spent using mobile device .....	100
Table 25 Age activity for significant correlations .....	101
Table 26 Age activity for non-significant correlations .....	101
Table 27 Education type effects on knowledge, risk behaviors, IPPR, and CFIP .....	102
Table 28 School type effects on knowledge, risk behaviors, IPPR, and CFIP .....	103

## Chapter 1: Introduction

Medical informatics has entered a new age. Resistive holdouts notwithstanding, electronic health records (EHRs) are nearly omnipresent in the American healthcare system. Legislation and government programs are guiding and accelerating the adoption of EHRs. There are boundless benefits to providers, healthcare systems, governments, and consumers. However, securing the right of protection of healthcare information is at an increasing risk as electronic health records become more entrenched in our society. Examples of breaches, nefarious and otherwise, are plentiful. Adopters are those hospitals, healthcare providers, practices, and other segments of the healthcare delivery system that have adopted the use of an electronic health record certified by a federal government sanctioned organization for the federal government's "Meaningful Use" program. "Meaningful Use" is a method of measuring for the purpose of financial incentives the adoption and usage of a certified electronic health record under the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the 2009 American Recovery and Reinvestment Act (ARRA). Adopters of healthcare technology may be held financially liable for breaches. These adopters are compelled to enter into incentive programs introducing risks for which they may not adequately be able to mitigate. To add further insult to injury, the adopters arguably do not receive adequate government or vendor support to prevent catastrophic breaches (Ong, 2015).

As good stewards of the dignity of healthcare consumers, healthcare institutions are burdened with painstaking measures to fortify their efforts in the prevention of sensitive information leakage in the new age of pervasive medical informatics. Under threat of crippling fines, healthcare entities such as hospitals and providers must be vigilant in safeguarding precious data while the threat of possible data leakage looms in part beyond their control.

Overall, this new paradigm presents a paradox of data liberalization for the benefit of patients with an increased risk of harm to the patients' detriment.

Health Information Technology (HIT) has lagged far behind the technology of other industries such as those in the financial sector. Speculatively, perhaps this lag may be in part due to healthcare technology being classification as a cost within a healthcare business model. In financial sectors, technology is a requirement to thrive or even survive. Financial database systems have competed for the financial prize by edging out one another over milliseconds in transactional speeds. Even the financial systems within healthcare are typically antiquated in comparison to technology typical of the financial industry. To add additional pressures to the mix, The Administrative Simplification Compliance Act of 2001 required that all Medicare claims must be done electronically ("Medicare Mandates Electronic Claims," 2003). This transformational piece of legislation forced even the financial portion of healthcare to advance into embracing modern information technology. In doing so, this legislation sparked a huge wave in the transmitting of electronic protected health information (ePHI).

Electronic healthcare systems have evolved considerably since the inception in the latter half of the twentieth century which saw the use of mainframe style systems, huge overhead and very limited capabilities. These early systems were often limited to finances, registration, and very few clinical components. The traditional paper chart remained in place for the most part during this era while antiquated systems prevailed in pervasiveness. As the personal computer started to become commonplace in the 1990s, so did its prevalence in hospitals to varying degrees. According to Tuttle (1997), the 1990s saw a need in healthcare for computer systems but a fragmented market coupled with a lack of scalable software.



Very clumsy clinical applications began appearing moreover at the turn of the century. Many of these early pioneers have their footprints in the applications of larger companies that consumed them over the years. These systems were painful to interface with other proprietary systems. Hospitals began adopting a “best of breed” approach by acquiring a mismatched set of proprietary systems, which did not work well in an interoperable manner. Others took a more uniformed approach selecting a single vendor for as many services and departments of the hospital as possible. Using a single vendor approach for multiple system often resulted in a wide spectrum of quality among these system modules as some portions of the product were the result of a quick acquisitions to complete a vendor’s portfolio. Clinicians outside of hospital systems were spared this experience generally, for the pen and paper were always 100% backwards compatible with all prior systems. Today, however, this paradigm is rapidly changing.

### Background of the Problem

A review of contemporary literature reveals that while there is an abundance of studies on the impact of health information technology in healthcare, there is little focus on the understanding of the safeguarding of electronic protected health information. There is a paucity of literature that directly addresses the nurses’ information system security knowledge. None of the studies reviewed makes subsequent associations with the personal characteristics of nurses that would make them to be sufficiently motivated to protect information the way they protect patients’ wellbeing in general. Understanding what motivates users to be protective – and therefore vigilant in maintaining secure and confidential processes in their routines – may be a precursor to their practices with using the EHRs and other patient-identifiable technologies in clinical care. Protection Motivation Theory, a theoretical framework may appropriately serve in the study of healthcare behavior but has not been applied to health care providers in this way as it

has been to health care recipients related to their personal self-care activities. Furthermore, the prevalence of mobile device use in the healthcare settings with nurses has not been factored in risk behavior studies. Where studied, the mobile device portions of the survey instruments were found to contain elements not relevant to commonplace usage in the United States and lacked the smart technologies that creep into everyday use that are prevalent today.

Based upon the gaps found in the literature review, this author has developed a study based upon both the use of existing instruments textured with the construction of a new instrument in order to measure variables not previously reported in the body of available literature.

#### Background: Knowledge and Risk Behaviors

To study nurses' knowledge of security and risk behaviors, it is less important to know about the security and encryption literature which is extensive and highly technical, and more essential to examine a way to understand human behavior as it applies to taking risk in general. Background literature for this study includes an examination of existing reports of knowledge, risk behaviors, and responses to the threat of security violations of users of HIT. Specifically, a significant segment of healthcare breaches affecting 500 or more individuals has been attributed to incidents with mobile devices. Between 10/21/2009 and 2/23/2017, 472 of the 1,847 large reported breaches had a mobile component involved in the incident (calculated from Breaches Affecting 500 or More Individuals, 2017). Further exploration specific to nurses' knowledge of information system security, risk behaviors with mobile device use, threat appraisal of their breaches in security, and their own sense of protection in response to the use of their own electronic health records, i.e. personalizing their understanding of confidentiality and security, is a framework to connect what nurses know and how they behave relative to their mobile devices.

This model may inform healthcare entities how to minimize violations of security or external infiltrations into their EHRs.

Rogers' Protection Motivation Theory has been well applied in the context of patient care in that the "fear appeal" may invoke a protective response (Rogers, 1975). Rogers' theory may be applicable to the healthcare practitioner experiencing a protective response to a fear of maleficence such as the inappropriate disclosure of protected health information. Such a fear appeal should be based upon the recognition that certain behaviors may increase the likelihood of such a negative occurrence.

In Protection Motivation Theory, the subject must analyze the existence of a hazardous condition, have a perception about the efficacy of the prescribed course of action, and based upon this threat appraisal elicit a protective response. In the case of nurses, the threat is the potential unauthorized use or misuse of electronic protected health information. The efficacious course of action would be the sound use of mobile devices. The protection response would be their sentiment in the case of their electronic health information being potentially misused. This is known as Information Personal Protection Responses, or the response to the threat appraisal (Rogers, 1975).

For the subject to have a response, they must first recognize a threat and the efficacy of the prescribed course of action. The method by which the threat and efficacy was evaluated is by way of a knowledge survey. A study of medical students' knowledge of cybersecurity was examined in the context of mobile devices, rapidly becoming a fixture in the healthcare industry (Whipple, Allgood & Larue, 2012). The study addressed the need to examine healthcare professionals' use of mobile devices and the associated risk behaviors that put protected health information at risk. However, in so examining humans as the weakest link in the security chain

the largest group of healthcare professionals was not in the scope of study. This study prompted this author to develop an instrument for the purpose of studying nurses' knowledge and associated risk behaviors of mobile device use, a specific area of study not observed having been examined in the body of reviewed literature. The areas to be explored were also influenced by a study conducted in Turkey, reported as an assessment survey, administered to determine cybersecurity awareness related to health information systems (Aydin & Chouseinoglou, 2013). The questions driving this dissertation were based on the authors' personal experience in cybersecurity and the general need to know what new nurses learn in their education, what electronic devices they may use in their clinical work, and what personal protective habits related to security they may have adopted or not. Assessing their knowledge of cybersecurity is fundamental to predicting their personal technology practices.

The knowledge level of nurses will establish a baseline for their understanding of the threat appraisal and efficacy of their response to mitigate the threat to the proper use of electronic health information. If these do not adequately mitigate their risk behaviors, it may be explained by their personal sense of privacy or lack thereof. Whether or not a nurse treats a patients' information the way they would want their own information to be treated could weigh into the consideration of risk behaviors. Do nurses have concern about protecting patient information? Do they respond in a way that is congruent with their own beliefs about protection of their own information?

To evaluate the subjects' Concern for Information Protection and their Information Privacy Protective Responses as Rogers' Protection Motivation mechanism, a study based upon patients' perceptions was used as the basis for the instrument. Kuo, Ma, and Alexander's 2014 study on patient responses to violations of their protected health information protection demonstrated a

predicted connection between one's "concern" with one's "protective responses." By using this parallel idea, assessing these concepts in nurses may provide insight on nurses' motivation to be vigilant in their personal technology habits related to patient information. This notion serves as a basis for studying nurses' responses to the threat appraisal of their own health records being at risk. Furthermore, the study's relationship among the elements of Information Privacy Protective Responses and Concern for Information Privacy may serve in the overall model to uncover the aspects of cybersecurity risk that nurses could be taught or motivated to minimize their risk behaviors.

This study will examine the nurses' knowledge of information security systems, their habits with mobile device use, and the threat appraisal (internal and external) that may motivate them as they relate to the subjects' self-report of risk behaviors and/or safeguarding private information as if it were their own health information. This will lay the framework for studying nurse risk behaviors and the antecedents that may be ameliorated through an educational intervention.

### Significance of the Problem

The American Recovery and Reinvestment Act (ARRA) of 2009 included stipulations for improving the United States' health technology infrastructure. As part of ARRA, The Health Information Technology for Economic and Clinical Health (HITECH) Act provides financial incentives for providers and hospitals, herein referred to as adopters, to adopt and implement electronic medical record technology. Conversely, significant penalties exist for those who choose to not adopt the technology. Computerizing patient data increases the risk of privacy breaches for which severe financial penalties exist. Those adopting the technology may be ill prepared to address privacy risk and are vulnerable for incurring substantial penalties. New rules imposed from the phases of "meaningful use" now mandate institutions to demonstrate vigilant

risk assessments and policies to manage numerous breach incidents. According to a 2012 Ponemon Institute study, 94% of hospitals surveyed experienced at least one data breach.

Under the HITECH Act portion of the 2009 American Recovery and Reinvestment Act, hospitals and providers face incentives to adopt and penalties for the failure to adopt an electronic health record. Furthermore, they must demonstrate “meaningful use” in stages. The current stage 2 of “meaningful use” requires hospitals to show that 5% of discharges must use the patient portal.

The patient portal potentially increasing the risk of a breach as protected health information and personally identifiable information is now mandated to be displayed in a customer-facing, publically-accessible system. Any mistakes such as inappropriate disclosures has the possibility to become calamitous. Between business associates, such as the patient portal vendor and the healthcare entity (hospital or practitioner), HHS has mandated agreements which could potentially reduce the liability of the healthcare entity. Potentially adding to the increase in risk, electronic health record vendors had to rush to meet the “meaningful use” stage 2 specification deadline and bring these features to market. Hospitals then rushed to implement and meet a goal that the majority of the nation’s hospitals failed to do. Following this rush, CMS (Centers for Medicare and Medicaid Systems) delayed the requirement. However, many institutions produced hastily-implemented systems across the country. Statistics of breaches resulting from the patient portal are not available as CMS will only publish those settled cases with 500 or more disclosures. Therefore, smaller breach episodes resulting from such hasty activities have yet to be realized.

Mobile applications increase the risk of breaches for the simple reason that they are mobile. Such devices are more readily lost or stolen than desktop devices and have the potential

to expose large amounts of sensitive information. A significant portion of non-paper based breaches of 500 or more individuals as reported by CMS indicates that mobile devices are most often the culprit. Approximately one of every three non-paper large breaches involved a mobile device (Breaches Affecting 500 or More Individuals, 2017). The common theme is that these lost or stolen mobile devices were not encrypted. Appropriately implemented encryption provides a covered entity with a “safe harbor” provision essentially considering a breach highly unlikely and therefore not reportable. Unfortunately, encryption is not a default standard configuration of the most common laptop operating systems.

Tablets and smart phones may or may not be protected. Apple’s iOS is encrypted by default, but controls may not be set up correctly to prevent disclosures. Android, the other prevalent mobile operating system, varies from manufacturer to manufacturer and only in the future will these devices be encrypted by default. Even Android encryption has been broken by a variety of mechanisms including deep freeze – which actually requires one to freeze the phone to a certain temperature before loading a ROM package. Apple’s latest offering supposedly cannot even be undone by the company themselves even in the case of a law enforcement request. However, without the mandated use of mobile device management solutions, the variety of configurations leaves mobile devices at risk. According to a 2012 Ponemon Institute study, 60% of all workplace mobile phone users circumvent their devices’ security features. Therefore, human behavior must be eliminated from the equation where possible to diminish the risk of a breach.

## Problem Statement

Nurses, the largest group of healthcare professionals in the United States, use electronic health records containing patients' sensitive information. As employee mistakes rank among the top sources of healthcare data breaches, nurse information system security knowledge and behavior should be studied to possibly mitigate security risks and ultimately safeguard a vulnerable population's sensitive information entrusted to healthcare entities. Data breaches can result in harm to patients by way of identity theft and fraud. Institutions may suffer financial penalties and harm to their reputation. Such instances have been frequently reported by news outlets (Ong, 2015). If health information system security knowledge can be improved through intervention and it has any influence on nurses' risk behaviors using mobile technologies, then untoward consequences can be prevented rather than prosecuted. In other words, an effective way of maintaining compliance with information system security practices may be to improve the knowledge of the subjects and find methods to encourage such practices rather than endure consequences to either personnel, the institution, and/or the patients. This content might be taught before the new graduate nurse becomes employed. However, standardized specific instruction on cybersecurity may be an elusive goal for nurse educators in the United States as the variations of EHRs, with associated security features continue to proliferate and students continue to use the latest electronic devices on the market. According to Gardner and Jones (2012), nursing schools have by and large not integrated the EHR into their curricula. The American Association of Colleges of Nursing (2008) offers in its latest guidelines for baccalaureate nursing education elements about the use of clinical informatics systems without mention of either privacy or security of the electronic information. According to available



literature, there is a prevalent lack of standardized cybersecurity practices in undergraduate nursing programs in the United States.

### Study Aim

The aim of this descriptive study is to explore level of new nurses' information system security and mobile device risk behaviors along with their Information Privacy Protective Responses, looking for patterns of relationships in users' protection motivation and their potential for breaches through risk behaviors related to health information technology (HIT) in general and EHRs specifically. This study will provide information related to a currently unstudied area of HIT security risk behaviors among nurses in preparation for future research on information system security training in nursing programs.

### Purpose

The purpose of this descriptive study is to explore in a national sample of new nurses one year after graduation in their HIT knowledge about security and risk behaviors in their use of portable electronic devices, their knowledge of information system security, and the influence, if any, of their personal protective motivation to protect patient care information. This sample of nurses that are homogeneous with respect to experience will provide a focus on how they were prepared in their nursing education in relation to information system security in order to inform educators in the future.

## Research Questions

The main question for the study is as follows:

What kind of activities do new nurses engage in with mobile technologies, including frequency of use, types of activities, and habits or behaviors that make them vulnerable to security risk?

This overall question driving the study can be broken into a series of questions related to the new nurses' specific cybersecurity knowledge, risk, and personal characteristics including:

1. What is the level of knowledge of new nurses' information system security (KISS) related to patient privacy, security rules, and vulnerability to breaches or threats to exposing protected health information (PHI)?
2. What is the nurses' level of personal or mobile device risk behaviors and types of personal technology practices which may pose a risk to health information systems?
3. What is the reported level and type of nurse mobile application use?
4. What is the level of new nurses' Information Privacy Protective Responses (IPPR) and Concern for Information Privacy (CFIP) factors?
5. What nurses' characteristics and behaviors predict their Information Privacy-Protective Responses (IPPR) based upon the Concern For Information Privacy (CFIP) factors including:
  - a. medical facilities errors (ME)?
  - b. unauthorized access to medical information (UA)?
  - c. medical facilities secondary use of medical information (SU)?
  - d. personal collection of medical information (CO)?
6. What are the predominantly reported threat appraisals (internal vs external)?

7. How do nurses' threat appraisals mitigate their Knowledge of Information System Security, their Privacy Protective Responses or their Risk Behaviors?

#### Proposed Model for the Study

The theoretical framework of Rogers' Protection Motivation Theory (PMT) is a suitable foundation to evaluate the Information Privacy Protective Response (IPPR) as the subjects' reaction component to their Concern for Information Privacy (Rogers 1975, 1983). The PMT is commonly used a framework for the study of patient responses to health threats as found in a survey of literature. Essentially, the patient must have knowledge of a risk. The patient develops a sense of a "fear appeal" (threat appraisal) or trepidation of said risk being realized along with the negative aspects of the risk in question. The patient then has a sense of belief as to whether the ascribed treatment would be efficacious. The patient would then adhere to the ascribed treatment to varying degrees or perhaps non-adherence based upon their knowledge, fear appeals, and belief in the efficacy of treatment.

Similarly, applying this to the proposed study, users of EHRs need knowledge about security risk to promote their compliance with cybersecurity practices. This knowledge lays the groundwork for behaviors that are influenced by the forces that shape their technology practices, secure or risky. These forces may be personal motivation such as concern for information protection, their information protective responses, their motivation externally or internally (threat appraisal) to being compliant, and their increased use of their mobile devices. A potential archetype for this can be seen in the figure below Information Privacy Protective Responses Pathway. The participants were be assessed for their knowledge, their individual protective response as attributed to Rogers' PMT, their fear appeal is their own CFIP index in whole and in part as subscales of the CFIP and their self-reported practices and risk behaviors. This study

examines correlations between knowledge, risk behaviors, CFIP, and the IPPR response to the CFIP as Rogers’ “fear appraisals” as they may be mediated by the threat appraisal of punishments to self (internal) or causing harm to others (external).

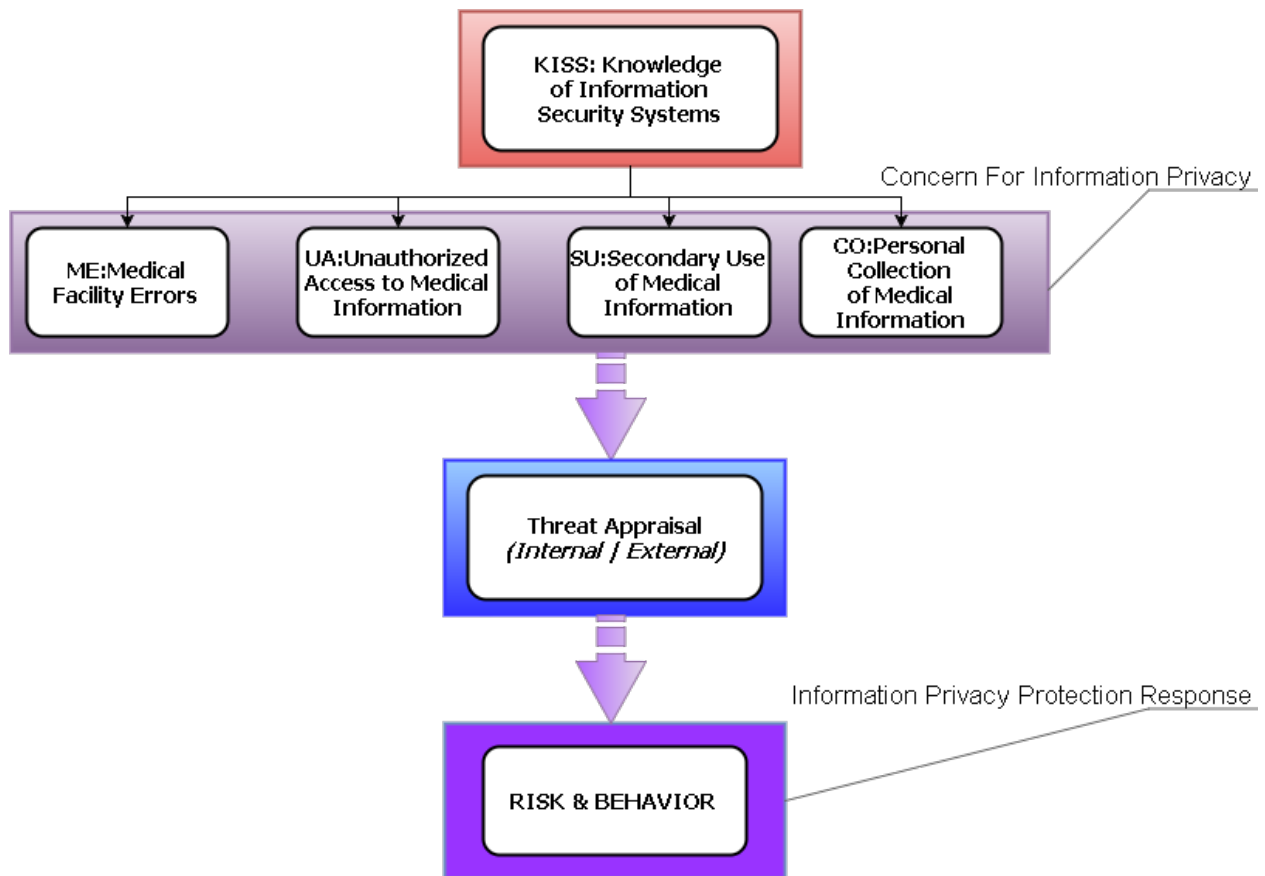


Figure 1 Information Privacy Protective Responses Pathway

Concern For Information Privacy Subscale Definitions

The Concern for Information Privacy (CFIP) index includes the subscales of Medical Facility Errors (ME), Unauthorized Access to Medical Information (UA), Secondary Use of Medical Information (SU) and the Personal Collection of Medical Information (CO) as its subscales (Smith, Milberg & Burke, 1996). The subscales are considered as the various factors of concerns to individuals that contribute to their overall concern for information privacy. The

CFIP serves as the conceptual framework for the study. Subjects' CFIP is evaluated using a survey to determine their sentiment or concern for the usage of their own medical information based upon the subscales which contribute to their overall concern.

### Conceptual Definitions of Variables

- Knowledge of Information Security Systems Index: This index measurement determines the degree to which a subject has knowledge of information system security (KISS).
- Concern For Information Privacy Index (CFIP): This index comprised of the below subscales determines the degree to which a subject has concern for the protection of information privacy; either their own or that of another subject.
  - Medical Errors (ME): Errors may exist in the electronic health record. An example may include mistyped information, another patient's data, or a system processing issue resulting in incorrect information present in an electronic health record.
  - Unauthorized Access of Medical Information (UA): This pertains to the condition whereby individuals not authorized by the patient for access to the electronic health record may obtain access. An example may be an institution workforce member obtaining access to an electronic health record without a clinical or business purpose. Another example may be the breach of electronic health record system resulting in the leakage of electronic health information to potentially nefarious actors.
  - Secondary Use (SU): Electronic health record data may be stored by, manipulated by, or transported to systems aside from the primary electronic health record. An example may be the transfer of information to a shared healthcare network database. Another example may be either prospective or retrospective research.
  - Personal Collection of Medical Information (CO): The personal collection refers to the gathering of electronic health information by an individual for personal use outside of clinical or business needs. An example may be the printing of electronic health information for potentially nefarious use.
- Threat Appraisal: This is the perception of a threat and motivation to take action as a result of this threat perception. An issue must be determined by a subject to be threatening and the action must be understood to have efficacy as a mitigating factor

against such a threat. This concept is operationalized into categories of “internal” threat to self (job, fines) and “external” threat/harm to others (hospital, patients).

### Conceptual Definitions of Dependent Variables

- Cyber Security Risk Behaviors (RB): This index measurement determines the professional behaviors undertaken by a subject which could present a risk to the protection of electronic information; either their own or that of another subject.
- Information Privacy Protection Response (IPPR): This response to the Concern For Information Privacy represents the intended activities to be taken by the subject to protect the electronic information, health record or otherwise, against undue privacy infringements.

### Summary

In summary, this chapter has outlined the problem of increased electronic health record prevalence in the United States as an increased security risk adjoined with employee mistakes as a leading cause of security issues in healthcare organizations and practices with nurses representing the largest segment of healthcare personnel and since mobile devices are becoming ubiquitous. To decrease the human risks to protected health information, it is essential to understand what nurses know about information system security and their motivation to protect information as it relates to their risk behaviors. The descriptive study provides information about new nurses in the United States with respect to their information system security knowledge, risk behaviors associated with mobile device use, their concern for information privacy as indicated by their own information privacy protective responses, and threat appraisal.

## Chapter 2: Review of Literature

### Introduction

This chapter provides an overview of literature with selected studies on the security of health information that are less technical and more based upon human behaviors. It begins with a background about HIPAA legislation and the mandates for EHR administrators that followed, including a general description about expectations that are technically implemented and regulations with punishments that were advanced for breaches in confidentiality. The chapter also includes a description of the Protection Motivation Theory as the dissertation theoretical framework, information system security knowledge studies, a foundational study on Information Personal Protection Response, a social engineering review, and a brief literature review of technical perspectives related to electronic health record privacy and security.

Health information system security and privacy have been researched in this era of accelerated electronic health record adoption in the United States. This literature review explores such research topics, peripheral and direct, regarding policy adherence mechanisms. There is a large body of literature on the impact of health information technology and related electronic health records (EHR), but less on the users of these healthcare organizations and practices and even less on the new era of mobile devices. Yet to be studied is a social science exploration of nurses' knowledge and risk behaviors with security and privacy issues with the focus on what they have learned in the nursing program and how much they bring to their new role as RNs. This section will also examine the literature pertinent to this study including medical students' cybersecurity knowledge, Rogers' Protection Motivation Theory, response to information privacy, response taxonomy, fuzzy logic, and social engineering.

In an effort to diminish the risk to protected health information in healthcare organizations and practices, this study should inform nursing educators within the healthcare organizations and practices as well as educational institutions about the knowledge of new nurses, their risk behaviors with mobile devices, and motivation for preventing incidents related to information system security.

### HIPAA Rules In Action

The 1996 Health Insurance Portability and Accountability Act (HIPAA) legislated the protection of health information privacy (Gilley, 2009). This Act permitted Health and Human Services to enact the Privacy and Security Rules of 2003 (“HHS delegates security rule authority to OCR”, 2009). Health and Human Services’ Office for Civil Rights (OCR) is tasked with enforcing these rules. Both the rules and the enforcement capabilities have been further strengthened under the HHS Final Rule of 2013 (Strauss, 2013). The OCR conducts periodic audits of healthcare entities, responds to reports of potential healthcare-related privacy and security issues, invokes penalties, and provides remediation guidance for breaches and infractions (HCPro, 2013).

HIPAA has placed a layer of rules that users in healthcare organizations and practices of health information data and personal health information, especially physicians and nurses, must heed in their active provider roles. On the HHS.gov Health Information Privacy website (April 16, 2015), The Department of Health and Human Services summarizes the HIPAA Privacy Rule as follows:



*“The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.”*

Paper-based systems could be easily tucked away from prying eyes with little chance of exposure en masse. Traditionally, charts could be copied, faxed, tampered with or viewed without the likelihood of access being tracked. While this modality seems safe contrasted against a backdrop of sensational cybersecurity headlines, large and small, paper-based breaches have occurred and continue to remain a risk. But these pale in comparison with the proliferation of new technologies and social media activities where providers such as physicians and nurses, who are human, interact with mountains of protected health information (PHI) and its electronic versions (ePHI) that may be vulnerable to security breaches and privacy violations. Healthcare organizations and practices now have the added responsibility of oversight of the wide range of computerized technologies in health and the ubiquitous systems of tracking health information. Their key endeavors in an era of regulation and “meaningful use” now include active risk assessment with the traditional maintenance and incident response/management of system disasters. The figure “Key Endeavors of Healthcare Organizations and Practices Information Systems Managers” shows some mainstay efforts of institutions to protect clinical systems.

These include risk assessments, encryption for both information at rest and in motion, as well as disaster recovery strategies.

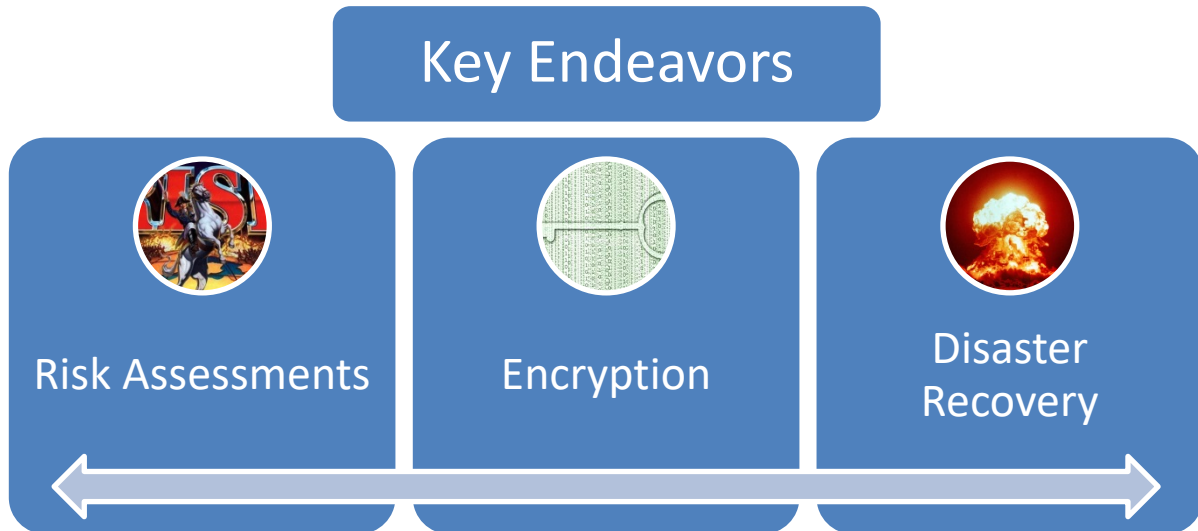


Figure 2 Key Endeavors of Healthcare Organizations and Practices Information Systems Managers (Ong, 2015)

With the electronic health record, data is available via multiple sources, people and systems. Along with this liberalization of information and massive accessibility come the mechanisms by which to track, restrict access, and monitor for inappropriate access. It's a brave new world with an increase in both benefits and risks. Furthermore, emerging programs and technology changes the manifestation of electronic health record usage and changes how newfound risks may surface. For example, the 21st Century Cures Act (H.R.6 - 21st century cures act, 2015) calls for EHR vendors to:

*“publish application programming interfaces and associated documentation, with respect to health information within such records, for search and indexing, semantic harmonization and vocabulary translation, and user interface applications; and... demonstrate to the satisfaction of the Secretary that health information from such records are able to be exchanged, accessed, and used through the use of application programming interfaces without special effort, as authorized under applicable law”.*

Such legislation leads to the use of application programmer interfaces which essentially requires vendors to open a portal into the electronic health record to other vendors. This changes the expression of risk to ePHI and how controls to mitigate such risk must be considered.

#### Security Breach – Privacy Violations

Data security has at times been front and center on the news and on the minds of the general public. Headline after headline, we are reminded of the potential pitfalls of living in a connected world. American intelligence agencies have accused the Russian government of hacking and other activities to influence the United States’ 2016 Presidential election (Shane, Sanger, & Kramer, 2017). Prior to such revelations, the National Security Agency (NSA) contractor turned whistleblower Eric Snowden exposed some of the NSA’s massive surveillance activities. These disclosures have shaken the foundations of international relations and help to create a narrative that America’s own government may be spying on their citizens. When combined with the sensitive nature of one’s private health information disclosed to providers with expectation of privacy, the public’s trust is threatened if that information appears to be available for others to see.

The following selected list suggests considerations related to the practices of securing ePHI:

- How is ePHI access logged? Is there remote access by healthcare personnel, vendors, and other business associates? Does anyone review or become alerted to potentially inappropriate access? Remember that even trusted employees have been known to have inappropriately disclosed information. Countless examples exist of information sold for a variety of reasons. People have been jailed even after making only a scant profit.
- Is information segmented in a fashion that limits access based on job role or even physical location? Maybe one hospital unit should not have access to another's. Maybe a physician sees a different set of information than a clerk.
- Is there an education program for the workforce to help in the understanding of legislation and organization policies to which they must adhere? Are there supplementary security awareness reminders? While ignorance is no excuse for the law, HIPAA does compel entities to keep its workforce informed.
- Is there a limitation on administrative access or even any access that goes unlogged?
- Can tampering of information be prevented or at least be discovered?
- What mechanisms are in place to prevent leaks from nefarious sources? (i.e. viruses, hackers, scammers)
- How secure is the information against damage – physical or otherwise? Are there contingency plans in place for periods of inaccessibility?
- Is there a disaster recovery, business continuity, and backup plan? Have you tested these plans? Careers have been cut short in disaster scenarios when untested backups fail.
- What mechanisms prevent accidental disclosure? Is there a data leak prevention system – either comprehensive through a vendor or otherwise via piece-meal? Can employees send patient files over email – internally and externally – where they reside ad-infinitum in wait for a potential hacker to come along?
- Is all sensitive data encrypted both at rest and in motion? An inadvertent disclosure could be as simple as a download to USB thumb drive that gets lost or an unencrypted stolen laptop. Stolen laptops are a huge source of breaches according to the Office for Civil Rights. Proper encryption means the would-be thief just inherited a brick-shaped laptop for all intents and purposes.
- Are the security mechanisms reasonable to implement? If not, workforce members will circumvent them. Anecdotally, one company made everyone change their passwords every day. The employees would gather every morning to choose the group password. Only their username was different. In the case of extremely complicated passwords and

different usernames for various systems, employees tend to place notes under their keyboards or tape them to their monitors.

- Is there an identity and access management solution in place? While this topic is complex, consider how to ensure that only those with authorization obtain access. The solutions may be technological in nature (single sign-on, self-service password resets) or administrative (activation and termination notification).

Identity theft companies promote their services in light of these new menacing headlines. The sensitivity of one's health information makes privacy in the EHR even more important to consumers. For example, a television advertisement shows a physician accidentally leaving a patient data-rich laptop in a cab while rushing to a meeting. Of course, the identity theft protection service thwarts the efforts of the thief who just happens to take the same cab immediately thereafter. But the potential consequences of a health data breach are being highlighted to the public. In this connected age of well-publicized data breaches, the general public has become more aware of the threat to their privacy, sacred health information, and finances. These create a suspicious consumer – and the health care workers using the information need to fully appreciate the great responsibility placed in their trust. Yet nurses, the largest single provider group using the healthcare organizations and practices' electronic technologies, are often perpetrators knowingly or unknowingly of vulnerabilities to the protections in place in the EHR.

### Social Engineering Behaviors – For Bad and For Good

Within the context of the information age, Social Engineering is the concept by which individuals or groups are manipulated into disclosing information such as access credentials or persuaded to elicit specific behavior responses (Greavu-Servan & Serban, 2014). A term historically associated with social sciences, social engineering has become the subject of concern in the computer security industry (Anderson, 2008, p.17). As diverse is the landscape of

available information, a wide spectrum of potential effects and bounty resulting from social engineering incidents may too be vast.

Identity theft, one prominent bounty of social engineering, often involves the use of others' names, banking information, social security numbers, and birthdates without the people's knowledge or permission (Hadnagy, 2010, p. 17). Medical theft involves the unauthorized use of health data also known as protected health information which may possibly be obtained through social engineering alone or in combination with other tactics. According to a 2012 study by the Ponemon Institute, the economic impact of such theft in the United States is \$41.3 billion per year up 33.66% from the year prior.

It has become necessary for hospitals and health care entities to put technological protections, educational interventions, and punitive policies to address the need to protect patient information and to be in compliance with regulatory expectations. These efforts combine people and products, designed to prevent, intercept, or threaten punishment of breaches in security. The figures below show samples of how a covered entity (health organization) may implement from a policy perspective the Health and Human Services guidelines for the administrative, technical, and physical controls of the HIPAA Security Rule. In these samples, every segment of each safeguard category has an associated institution policy indicating how elements of the rule are addressed.

ADMINISTRATIVE SAFEGUARDS				
Standards	Sections	Implementation Specifications R=Required, A=Addressable	Policy Number	Policy Name
Security Management Process	164.308(1)	Risk Analysis	R 9100-204	Risk Analysis
		Risk Management	R 9100-032	Security Management Process
		Sanction Policy	R 9100-032	Security Management Process
		Activity Review	R 9100-032	Security Management Process
Assigned Security Responsibility	164.308(2)		R 9100-033	Assigned Security Responsibility
Workforce Security	164.308(3)	Authorization and/or Supervision	A 9237(100-131 and 700-702)	See: Human Resources Policies On Intranet
		Workforce Clearance Procedure	A 9237(100-131 and 700-702)	See: Human Resources Policies On Intranet
		Termination Procedures	A 9237(100-131 and 700-702)	See: Human Resources Policies On Intranet
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Functions	R 9100-034	Isolating Health Care Clearinghouse Functions
		Access Authorization	A 9100-035	Access Authorization
		Access Establishment and Modification	A 9100-036	Access Establishment and Modification
Security Awareness and Training	164.308(a)(5)	Security Reminders	A 9100-037	Security Reminders
		Protection from Malicious Software	A 9100-004	Protection from Malicious Software
		Log-in Monitoring	A 9100-038	Log-in Monitoring
		Password Management	A 9100-205	Password Management
Security Incident Procedures	164.308(a)(6)	Response and Reporting	R 9100-039	Response and Reporting
Contingency Plan	164.308(a)(7)	Data Backup Plan	R 9100-040	Contingency Plan
		Disaster Recovery Plan	R 9100-040	Contingency Plan
		Emergency Mode Operation Plan	R 9100-040	Contingency Plan
		Testing and Revision Procedures	A 9100-040	Contingency Plan
		Applications and Data Criticality Analysis	A 9100-040	Contingency Plan
Evaluation	164.308(a)(8)		R 9100-042	Evaluation
Business Associate Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement	R 9200-331	Business Associate Agreements

Figure 3 Sample - Levels of Administrative Safeguards (Ong, 2015)

PHYSICAL SAFEGUARDS				
Standards	Sections	Implementation Specifications R=Required, A=Addressable	Policy Number	Policy Name
Facility Access Controls	164.310(a)(1)	Contingency Operations	A 9100-044	Contingency Operations
		Facility Security Plan	A 9100-015	Facility Security Plan
		Access Control and Validation Procedures	A 9100-030	Access Control and Validation Procedures
		Maintenance Records	A 9100-045	Maintenance Records
Workstation Use	164.310(b)	Acceptable Use Policy	R 9200-385	Acceptable Use Policy
Workstation Security	164.310(c)		R 9100-041	Workstation Security
Device and Media Controls	164.310(d)(1)	Disposal	R 9100-031	Device and Media Controls
		Media Re-use	R 9100-031	Device and Media Controls
		Accountability	A 9100-031	Device and Media Controls
		Data Backup and Storage	A 9100-031	Device and Media Controls

Figure 4 Sample - Levels of Physical Safeguards (Ong, 2015)

TECHNICAL SAFEGUARDS				
Standards	Sections	Implementation Specifications R=Required, A=Addressable	Policy Number	Policy Name
Access Control	164.312(a)(1)	Unique User Identification	R 9100-043	Unique User Identification
		Emergency Access Procedure	R 9100-047	Emergency Access Procedure
		Automatic Logoff	A 9100-219	Automatic Logoff
		Encryption and Decryption	A 9100-029	Encryption
Audit Controls	164.312(b)		R 9100-048	Audit Controls
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	A 9100-046	Mechanism to Authenticate Electronic Protected Health Information
Person or Entity Authentication	164.312(d)		R 9100-049	Person or Entity Authentication
Transmission Security	164.312(e)(1)	Integrity Controls	A 9100-050	Integrity Controls
		Encryption	A 9100-029	Encryption

Figure 5 Sample - Levels of Technical Safeguards (Ong, 2015)

In support of these sample endeavors is a matrix illustrating how the Health and Human Services Office for Civil Rights facilitates the privacy and security undertakings of covered entities in pursuit of compliance with the HIPAA Security Rule. The agency holds a balance between privacy and security, a public access arm, tools to facility compliance, and an enforcement segment.



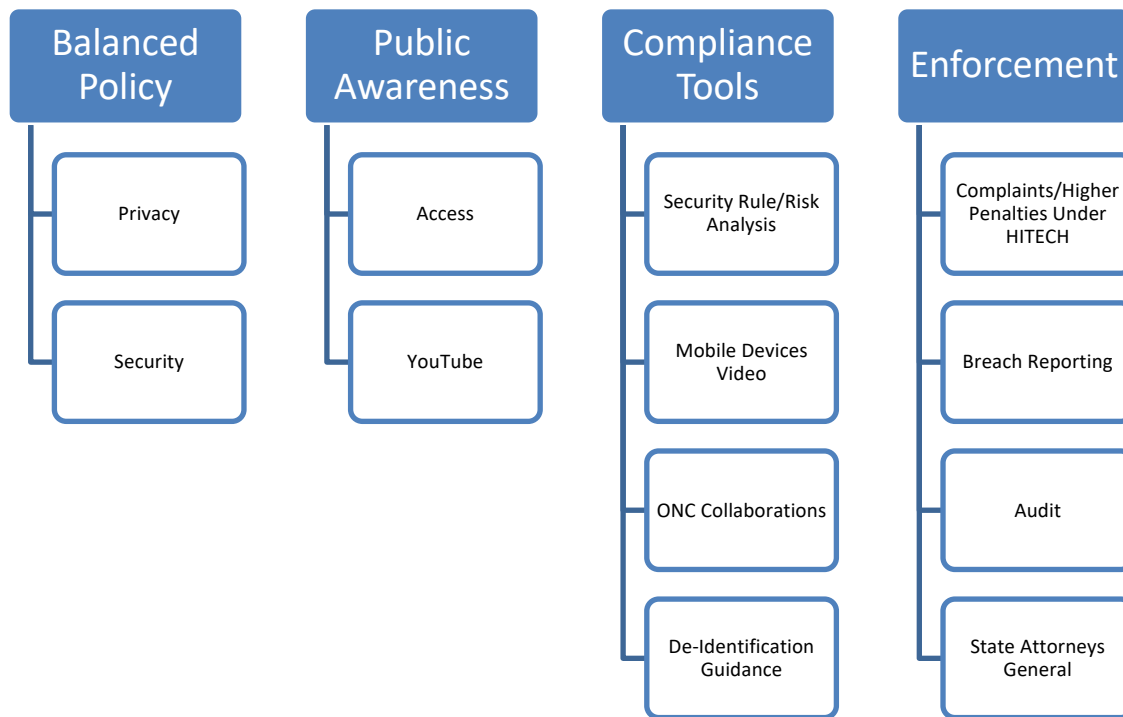


Figure 6 Office for Civil Right Facilitates Privacy and Security (Ong, 2015)

Social Engineering by design involves the manipulation of human behavior (Greavu-Servan & Serban, 2014, P. 5). The HIPAA Security Rule (Administrative Safeguards, § 164.308(a)(5) 45 CFR Subtitle A, 2003) addresses this vulnerability by requiring healthcare entities to “Implement a security awareness and training program for all members of its workforce (including management).” Using the notion of Social Engineering in reverse, perhaps efforts can be constructed to positively influence people who are frequent users to internalize and protect patient information as part of their work life. By recognizing the predictors of motivation to protect information, interventions aimed at users may be constructed.

These new efforts must take into account the multiple potential entry points with the growing proliferation of mobile devices and social access to a wide range of tools and information that

may be useful and/or purely social. These boundaries have become less clear. In order to plan for and develop interventions that address future breaches, it is important to study the knowledge and behavior of those who are vulnerable to inadvertent or intentional threats to patient privacy. Nurses represent the largest group of healthcare professionals according to a July 13, 2015 United States Department of Labor report (TED: The Economics Daily Image, 2015) and therefore represent the largest workforce group mandated to receive security awareness training. Furthermore, the growth and adoption of population health endeavors may speculatively seem a changing role for nurses potentially increasing their use of technology and their oversight of information in healthcare spaces such as primary care.

As part of an overall effort to minimize breaches and exposure of patient sensitive health information, this study will explore the user side of EHR security and the variables that may be pivotal in risk behaviors or susceptibility, knowing that mobile devices will continue to grow and be part of the healthcare systems currently in place. The Concern for Information Privacy (CFIP) theoretical framework from Smith et al (1996) based upon the Rogers (1975, 1983) “Protection Motivation Theory” (PMT), this study focuses on nurses one year after graduating from nursing school, to determine their knowledge, risk behaviors, and personal beliefs related to privacy. This group may give insights into what nurses learned in their education as it carries into their first year of work. It seeks to explore the information privacy-protective responses (IPPR) of nurses (the largest single user group who access protected patient health information routinely) and how it might predict their likelihood of risk behaviors of security breaches related to their increase use of mobile devices. Knowing what predicts the likelihood of risk behaviors of security breaches including the nurses’ susceptibility and/or lack of knowledge, the researcher was able to develop an intervention that combines education with social engineering strategies to

produce users of EHRs and other healthcare technologies who internalized motivation to protect ePHI.

### Theoretical Framework: Rogers' Protection Motivation Theory

The theoretical framework of this dissertation is centered on Ronald Rogers' Protection Motivation Theory (PMT). This theory may be considered chiefly pragmatic for studies pertaining to subjects' recognition of health consequences resulting in a fear appeal and their associated response mechanisms (Rogers, 1975, 1983). This new nurse study uses the same protection motivation and fear appeals mechanism in overlaying the new nurse's sentiment of protecting their own sensitive information with the relationship of protective responses vis à vis the subjects' information system security risk behaviors.

In Rogers' 1975 article "A Protection Motivation Theory of Fear Appeals and Attitude Change" along with his 1983 revision "Cognitive and Physiological Processes In Fear Appeals and Attitude Change," a concept was formulated describing the relationship between fear and the reaction to this given recognition of fear. Initiating the process is the components of the fear appeal as magnitude of noxiousness, probability of occurrence, and efficacy of recommended response. In other words, the motivation for protection originates at the recognition that an event is perceived with a potential degree of harm at a particular degree of likelihood and that the recommended response is calculated with a certain degree of effectiveness. For example, a patient must appreciate that non-adherence to a prescribed diet may have likely concrete consequences which would be significantly averted by adherence to the recommended regimen. Based upon these factors, the patient may elicit a protective response.

In the Cognitive Mediating Process, the fear appeal is evaluated. The noxiousness is appraised. The probability is evaluated as the expected likelihood of the event's occurrence.

The efficacy of the recommended treatment is deliberated as a possible coping response. These factors lead to the protection motivation (Rogers, 1983).

Categorically, the fear appeal and cognitive mediating processes lead to an attitude change. In the above instance, the patient may make the determination that the diet will work and thus adopt an adherence to said regimen.

Rogers discusses the fear appeal process in the context of the power of persuasion. He issues a disclaimer of his theory's limitations. There are vast arrays of confounding variables which could potentially affect the response outcome. Applying this notion to fear appeal as it relates to how nurses appraise the noxiousness of a breach in security from a few perspectives: (a) a personal protection motivation that connects the breach of security for one's own information and how that information might be abused; (b) an internal threat that a breach will result in something bad happening to oneself such as punishment or loss of job; (c) an external threat that a breach will result in harm to one's patient or the hospital. In this study, new nurses as subjects self-report their behaviors using mobile devices and their secure practices to protect access to their own or hospital information. While the fear emotion may not be adequately conveyed through a survey, the nurse assessment was based upon considering themselves as the affected victims of potential breaches in cybersecurity and how this may or may not influence their secure cyber practices.

## Violation of Information Privacy Responses

The violation of information privacy protective responses was a study conducted in Taiwan with patients. Elements of the study and the results shaped the development of examining nurses' information privacy protective responses and concern for information privacy as variables in the dissertation that may predict risk behaviors, particularly with mobile devices.

In Kuo, Ma, and Alexander's 2014 study on patient responses to violation of information privacy, the taxonomic structure of Information Privacy Protective Responses (IPPR) operated as the unifying resultant of factors such as Collection (CO), Unauthorized Access (UA), Secondary Use (SU) and Medical Errors (ME) within the framework of Rogers' Protection Motivation Theory. The Taiwan-based study was conducted in a hospital with patients in the investigation of their concerns for information privacy and resulting protective responses in reaction to factors which may lead to the invasion of patients' privacy. The study cited reasons for the increasing pervasiveness of the electronic health record in the health industry leading to the foreseeable accompaniment of the healthcare entities' ethical dilemmas and patients' privacy concerns. The variables were found to be factors that were interrelated and predictive of the participants' reported protective responses. By using this structure and known relationships, this dissertation modifies the elements to apply to the nurses themselves, interpreting the questions as if the information in the EHRs was their own.

By applying this study to the dissertation focusing on new nurses in the United States as subjects with whom the Information Privacy Protective Response mechanism can be explored, a potential motivating factor of shaping safe, secure practices might contribute to behaviors in addition to the knowledge nurses might have about cybersecurity. The Kuo study refers to the plethora of sensitive information held by the electronic health record and the potentially

devastating consequences to the affected patient population should an unauthorized disclosure or breach occur. Medical data can be considered as quite sensitive and harm can ensue if mishandled. The authors go on to infer that the risk increases as data accumulates over time. The study's purpose is to assist those entities in a position to improve the mechanisms designed to protect patients' private information.

The authors specify that only a scarce, limited amount of studies regarding patient concerns for their information privacy have been completed. Their study uses the Protection Motivation cognitive appraisal of threat in the context of perceived risks to the electronic medical record privacy and the Information Privacy Protective Responses as the Protection Motivation resultant effect. These findings are specific to the population studied but may be useful to other populations such as nurses themselves. These authors present the notion that the perceived threat to the security of the electronic health record should result in a decrease in risk behaviors contributing to the likelihood of such threats being realized and thereby considering the attitude change as a privacy protection behavior by means of the protection motivation conduct.

The study selected a Southern Taiwanese hospital that provides medical services with nearly 1300 inpatient beds and a near average of 5000 outpatients seen daily. Four interviewers recruited a convenience sample of subject by what the authors describe as approaching patients "randomly" to conduct in-person interviews for 5 to 10 minute periods. In research, randomness typically refers to the random assignment of treatment. Random selection would be the use of selecting from an available pool of subjects. This study in effect used a convenience sample of subjects who self-selected to partake in the study upon approach of recruiters.

The survey collected demographic information in the first section coupled with the second section of privacy concerns and subsequent protective responses. Using a 5-point Likert scale,

measures from prior empirical studies were translated into Chinese and categorized into collection, secondary use, unauthorized access, and medical errors. The Concern for Information Privacy (CFIP) scale involving these factors was modified to suit the context of the electronic health record. A group of ten patients served as a pilot study for the purpose of eliminating extraneous or otherwise unsuitable elements.

The Structured Equation Model (SEM) was used to test the hypotheses using the partial least square (PLS) as no distributional assumptions were made. The results included 204 subjects out of 300 invitees with demographic details congruent with the general population of Taiwan only slightly younger and more educated.

Reliability and validity were tested in confirmation of the measurement model. The measurement items within the constructs were scrutinized as confirmatory by factor analysis resulted in three of the twenty-one items being discarded. The construct validity testing resulting in all approved items receiving a Cronbach's alpha statistic estimate of at least 0.7.

Bootstrapping was performed using 1000 re-samples showing support for the four hypotheses save for the link of unauthorized access link to the Information Privacy Protective Response.

According to the study, subjects seemed to feel that too much of their patient information was collected by medical facilities thereby causing some discomfort. The authors suggest that only a minimal data set of information should be retained by the medical facility. The subjects did not seem concerned with the potential for unauthorized access. The authors attribute this phenomenon to patient familiarity with the medical staff. Perhaps the sample contained individuals who were more educated than the general population and had confidence in healthcare staff as possible peers. The subjects did, however, express concern over secondary use of information beyond the intended purpose. Secondary use is required for billing,

insurance, and pharmaceutical payers among other recipients. The authors suggest limiting secondary disclosures where applicable and having prior approval before the release of information could take place. Regarding errors, subjects showed concern over the potential inaccuracy of their medical information and effect on patient safety. The authors suggest that patients cannot review their data for accuracy and that medical facilities must take it upon themselves to protect electronic health records from alterations and inaccuracies. Please note that in the United States, regulations require healthcare entities partaking in the “Meaningful Use” incentive program to not only provide a patient portal but are required to have a percentage of their population log in as well. Therefore, patients in the United States may review a subset of their chart and potentially request corrective action as warranted.

The study examined the breadth of patient privacy concerns and their responses. The study sought to suggest increases in lacking protections as the proliferation of the electronic record continues over time. The study did not connect the concept of access by individuals outside of the medical facility, a factor of concern in the era of regularly reported breaches of medical information. The authors implore medical facilities and government entities to develop mechanisms to reduce patient privacy concerns related to the electronic health record. The study has expanded the use of the Concern For Information Privacy framework to the electronic health record paradigm and validated the instrument in the context of the healthcare setting thereby narrowing the gap of information found in the body of pertinent literature.

#### Medical Students’ Knowledge of Privacy and Security

In another non-technical study on information system privacy and security, third year medical students of a Midwestern university in the United States were surveyed for their knowledge of information system privacy and security. Their reported activities using mobile



devices was found to be in near ubiquitous use among the sample representative of the institution (Whipple, Allgood, & Larue, 2012). This rapid increase in mobile technologies appears to be worldwide and notably among young people, including students.

The researchers found the students' knowledge of information system privacy and security to be lacking and therefore sought to establish a baseline of their familiarity with this essential subject matter particularly with mobile device use. A set of 67 respondents were provided with clinical situations to determine their concern for information privacy.

The results showed that all respondents used their phone for voice communication and 94% for text messaging. Respondents noted only 76.9% used the internet. Due to the subjects' interpretation of the question and gap in their knowledge of the technology, this author would suggest the number is likely to be 100%. The interpretation of several results such as internet use suggests that there are significant knowledge gaps and/or perhaps limitations in the manner in which survey questions were constructed.

Consistent with results conducted by the Ponemon Institute (2012) with workforce members, these students bypassed a key security mechanism on their phones more than half the time. The author noted the same with the "PDA" (Personal Data Assistant), a term that fell out of use roughly a decade prior to their study but suggestive of perhaps tablet use in its place. However, the institution in question also used this outdated PDA technology to operate a software package. Given the availability of advances in technology in the mobile device sector, one may presume that these functionally-limited PDA devices were likely used almost exclusively for work-related purposes. Scenarios included the sharing of information via the YouTube video sharing service and Facebook, the predominant social media service. As infractions of protected health information have been reported in the media by way of both of

these services, the use in scenarios provides for a realistic conduit by which to comprehend medical student mobile behavior which may place the privacy and security of patient information at risk for inappropriate and potentially unlawful disclosures.

The forty question Mobile Device Questionnaire (MDQ) was provided to 67 students at the commencement of their third year of medical school in attendance of an intersession activity. Only a single student claimed to not have a mobile phone. The survey was initiated with demographic details followed by mobile devices use, security knowledge, and concluding with clinical scenarios issues. The authors concluded that more education needs to be provided to medical students regarding information system security and privacy due to the ease at which data may be shared through mobile devices both purposely and inadvertently.

A principal focus of the finding is centered on the students' lack of mobile device locking. (This author notes that the major vendors of such devices have increased security mechanisms and encouraged the use of said mechanisms as default configurations over the years since this study was conducted. Furthermore, mobile device management solutions requiring the locking of devices with complex passwords have been created and available to institutions to safeguard such devices.) While still a relevant area of study, the period of time and sample studied may not be indicative of the experience of new nurses from across the United States in the year 2016.

Some of the survey questions in the MDQ were used by this author to develop items for the dissertation. Several items required adaptation to suit the target nurse audience and with clarifications or modifications reflective of technology in modern use. For example, "Notepad" is vendor-specific application available on a specific mobile device operating system found to be in near obscurity at the time of this dissertation draft. "Address Book" is merely a contact list that all participants likely use with every interpersonal interaction. Responses to the question are

likely to be more indicative of respondents' awareness of how the technology is used rather than whether or not the technology is in use by the subject. These were all considered in the development of the survey for this study.

Most telling and arguably of foremost value is the subject responses to scenarios indicative of behavior, possibly putting sensitive information at risk. Such scenarios served as models for the instrument directed at nurses with the goal of similarly identifying and describing nurse risk behaviors. In the Whipple et al. (2012) study, more than a quarter would leave their device unprotected and alone for up to an hour. More than half did not take issue with sending protected health information to a professor via email and reading such content submitted to them via email on their mobile devices. Depending upon institutional policies and protection mechanisms in place, such activities may be considered as contributory to mobile device risk behaviors and therefore certainly revealing of a likely educational opportunity for these student programs.

The authors concluded that third year medical students are far enough along in their program to have hopefully been exposed to information protection education in having had exposure to the clinical setting. Their study may be informative to those studying mobile security risk behaviors in other populations and serve as a basis for further study in other populations of interest in the contemporary healthcare and technology worlds.

#### Fuzzy Logic of Cyber Security Knowledge

Cybersecurity knowledge was studied as Başkent University in Ankara, Turkey and analyzed using fuzzy logic. Participants included 86 administrative subjects, 69 physicians and 86 students with various unspecified categories of health-related studies. The study provided

results, interpretation of the survey outcomes, and guidelines for the application of fuzzy logic to other healthcare institutions (Aydın, & Chouseinoglou, 2013).

The article provides a compelling account of the significance of cybersecurity mechanisms in health information systems and the rationale for student subjects as “digital natives” expected to be the predominant information system user base within the upcoming decade. The persuasive explanation of cybersecurity risk is detailed as a rationale for conducting such an investigation of cybersecurity habits.

The authors outline a precedence for the use of fuzzy logic in healthcare research. Defined therein is fuzzy logic as a linguistic methodology for qualitative modeling thereby deducing human knowledge to a mathematical elucidation. Results are not considered a constant, but rather gradually measured and without certitude. For the results, researchers had determined a baseline of information system training finding the vast majority of students and physicians not having received any, while roughly two-thirds of administrative staff had this deficiency. The amount of time spent on the internet seemed to influence the degree of risk behaviors and potential for information security incidents.

A five-point Likert scale with 80 questions out of a total of 89 was applied to 470 subjects using an instrument tested by 62 experts for reliability and validity judgment with a Cronbach’s alpha statistic estimate of 0.935. Rich data consisting of upper and lower limits by demographic category and instrument item were yielded.

The instrument items contributed in the development of this researcher’s new nurse survey. However, either perhaps due to the translation from native Turkish into English or through the choice of terms invoked by the translators, this author’s sentiment is that the articulation of several objects’ phrasing could better be served to invoke the intended inquiry of the subject.

Furthermore, some of the technology described therein the study was found to either be obscure or otherwise outdated such as the LimeWire application. Other items such as “citizenship number” may be considered as regional-specific and perhaps substituted with an item of similar concern for subjects within United States. The same regional-specific applicability would apply to technologies perhaps more prevalent in Turkey than in the United States such as the use of Skype as a chat service.

The authors noted that while their study could provide some insight into risk behaviors with users of health information system, the results should be considered as specific to the institution in Turkey. Results may differ among studied populations. However, a principal goal of this study is to serve as a model or framework for further studies using fuzzy logic in the context of safeguarding health information systems.

### Social Engineering

Within the context of the information age, Social Engineering is the concept by which individuals or groups are manipulated into disclosing information such as access credentials or persuaded to elicit specific behavior responses (Greavu-Servan & Serban, 2014). A term historically associated with social sciences, social engineering has become the subject of concern in the computer security industry (Anderson, 2008, p. 17). As diverse is the landscape of available information, a wide spectrum of potential effects and bounty resulting from social engineering incidents may too be vast.

Identity theft, one prominent bounty of social engineering, often involves the use of others’ names, banking information, social security numbers, and birthdates without the people’s knowledge or permission (Hadnagy, 2010, p. 17). Medical theft involves the unauthorized use of health data also known as protected health information which may possibly be obtained through

social engineering alone or in combination with other tactics. According to a 2012 study by the Ponemon Institute, the economic impact of such theft in the United States is \$41.3 billion per year up 33.66% from the year prior.

Kevin Mitnick and William Simon (2003) echoed a dire warning of how even the most stringent of traditional security mechanisms may be thwarted by unsuspecting individuals performing their duties in good faith.

*“A company may have purchased the best security technology that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business. That company is still totally vulnerable. Individuals may follow every best-security practice recommended by the experts, slavishly installed every recommended security product, and be thoroughly vigilant about proper system configuration and applying security patches. Those individuals are still completely vulnerable.”*  
(p. 3)

Following upon the premise styled by Kevin Mitnick that humans are likely to be the source of breaches in the milieu of most strident security mechanisms, Aydın and Chouseinoglou (2013) likewise identified health information system users as the Achilles’ heel of information security. Researchers cited sources supporting the assertion that risks from inside the organization, both accidental and purposeful, produced the key offenders of security. As a result, these researchers focused their study on newly graduated subjects from Turkey in the evaluation of their security awareness using a fuzzy analysis, a system with precedence in studying health information systems. The purpose of this study was to evaluate the security awareness of health

information system workers in Turkey with varying degrees of information system knowledge and experience. In doing so, the researchers have developed a gauge to determine areas of deficiency necessitating further intervention.

Social Engineering by design involves the manipulation of human behavior (Greavu-Servan & Serban, 2014). The 2003 Security Rule addresses this vulnerability by requiring healthcare entities to “Implement a security awareness and training program for all members of its workforce (including management).” Nurses represent the largest group of healthcare professionals in this workforce according to The United States Department of Labor (2015). Therefore, nurses speculatively would be expected to be a proportionally significant recipient of such training. This study examines the security awareness, social engineering aspects of Registered Nurses in the United States, in healthcare organizations and practices of all sizes and configurations across the country, with the common aspect that they all graduated less than one year prior to the study from an accredited institution.

Social engineering has garnered a reputation as a deceptive force of nefarious intent in the context of elaborate and high-profile information systems theft. However, social engineering theories such as Roger’s Theory of Protection Motivation may be germane to the preservation of information system privacy and security.

According to Rogers (1975):

*“A protection motivation theory is proposed that postulates the three crucial components of a fear appeal to be (a) the magnitude of noxiousness of a depicted event; (b) the probability of that event's occurrence; and (c) the efficacy of the protective response. Each of these*

*communication variables initiates corresponding cognitive appraisal processes that mediate attitude change.” (P. 93)*

In other words, appealing to subjects’ nature that severely adverse events are likely to occur in a particular instance should increase the protective responses in these subjects. Rogers (1983) later introduced the concept of “fear appeals.” A modern example might be a commercial showing young drivers briefly texting and seemingly a moment later being airlifted for medical treatment as a deceased friend remains by the tragic accident.

Kuo, Ma, and Alexander (2014) referred to the theory of protection motivation in studying a patient population in Taiwan to find a relationship between their healthcare information privacy concerns and protective responses. In doing so, researchers discovered the specific matters of importance were related to collection, possible inaccuracies, and additional uses of their private health information. Unauthorized access by staff members did not elicit protective responses. This study served as a barometer reading for hospitals to appreciate patient concerns in the context of preserving a positive standing while commissioning the use of an electronic health record. In this context, the protection response mechanism is the dependent variable being measured in a population of Taiwanese patients and may or may not be generalizable to the population in the United States.

#### Systematic Technical Perspective Review of Electronic Health Record Systems

Rezaeibagha, Win and Susilo (2015) performed a systematic, technical review of electronic health record systems examining elements of privacy and security using grading criteria based upon industry standards.

The systematic review explicitly omitted the element of mobile devices as stated in the authors’ exclusion criteria. Mobile device use as a potential risk factor in maintaining the



privacy of EHR information is a key element in this dissertation study. The omission in the technical review further builds a case for the need to explore an element of healthcare technology that is rapidly increasing in prevalence. In addition to the absence of mobile device use, the authors note the study limitation exclude factors such as administrative and organizational aspects of electronic health record data safeguards.

The authors used the International Organization For Standardization (ISO), International Electrotechnical Commission (IEC) standardized elements to review the security and privacy components of various electronic health records to evaluate the security and privacy elements of the system described therein the literature examined literature reviews. The ISO standards used include ISO/EIC 27002:2013 and 2900:2011. Findings were outlined in the review and included a matrix of each system graded against multiple elements of the ISO/EIC standards.

Rezaeibagha et al. (2015) summarized their investigation findings of the technology-based evaluation and highlighted the following determination:

*“Our findings demonstrate, regardless of the enormous effort required, well defined access control policies should be mandated in order to provide patient privacy by limiting the access rights to patient data with proper access control policy language and standards. Applicability of privacy and security rules and scalability of EHR system implementations can be provided with proper architectures and frameworks, cryptography techniques and policies.” (p. 30)*

In other words, the authors stress the imperative of invoking technical safeguards for the protection of electronic health record systems. The various implementation manifestations of

such safeguards, while imperative to address the international standards, may diminish but do not eliminate the human behavior risk factors examined in this dissertation.

This meta-analysis surveyed literature reviews of electronic health record systems from a technical perspective using international standards as evaluation criteria. The authors expressed study limitations related to mobile device use and administrative controls which are associated with human risk behaviors. These study limitations are explored by way of this dissertation study.

#### Nursing Education: National Student Nurses' Association (NSNA)

The National Student Nurses' Association provides cybersecurity guidance for its members in part to protect the privacy of patient information. This information has been made available on the NSNA website page section titled "Recommendations for: Social media usage and maintaining privacy, confidentiality and professionalism".

The NSNA highlights risk to the safeguarding of patient information related to student nurses' use of social media outside of the work and school settings. The guidelines state that although institutions may provide guidance in their setting, student nurses' behaviors can pose a risk to the integrity of patient privacy and ultimately pose a risk of sanctions to themselves, especially when common practices of sharing information with peers electronically is commonplace. Healthcare organization and practice policies demand vigilance in protecting the privacy of patients and abhors sharing information outside of sharing with other providers who have a right to that particular information. Such verbiage lends itself well to the "threat appraisals" portion of Rogers' Protection Motivation Theory in that the threat and consequences are provided to the subject for appraisal.

The scope of social media includes the use of both web-based and mobile social platform and outlines contemporary social media services as examples of platform types. The guidelines not only provide context by referencing HIPAA and examples of how social media activity may lead to breaches, but also discuss the protection of the public perception of nurses. The guidelines do not only provide verbiage of caution to its members, but they also tout the virtue of social media when used appropriately.

The National Student Nurses' Association members have been provided with social media guidelines in an effort to protect patient privacy. The information contained therein the guidelines are particularly suitable to include in this literature review as the targeted membership audience services in part as the subjects of this dissertation study thereby providing a contextual backdrop of education germane to the study (Recommendations for: Social media usage and maintaining privacy, confidentiality and professionalism.2018).

#### Nursing Education: National Council of State Boards of Nursing (NCSB)

Like the National Student Nurses' Association (NSNA) guidelines for its members' social media use, the National Council of State Boards of Nursing (NCSBN) provides a similar direction (White paper: A nurse's guide to the use of social media.2011). These guidelines point out the beneficial uses of social media while cautioning about its pitfalls which could lead to the improper disclosure of patients' protected health information. This document provides education on social media use in the context of federal regulations such as HIPAA and site fictitious examples of how improper use made lead to inappropriate disclosures.

The document also provides information about consequences to the patient as well as the nurse. As with the National Student Nurses' Association guidelines, these consequences are in alignment with the dissertation's theoretical framework of using Rogers' Protection Motivation

Theory “threat appraisals.” The nurses should understand the threat and the perceived efficacy of the treatment to mitigate the identified threat. In other words, the guidelines show the threat of consequences and provide the means by which to mitigate such consequences.

In both social media document guidelines, the threat of nurse-invoked breaches is placed into the context of social media use, but such guidelines are applicable as general safeguards in the workplace. These documents serve as a reference for the type of educational material nurses may receive in safeguarding protected health information by decreasing risk behaviors with the use of electronic devices.

### Summary

In summary, this chapter explored pertinent literature regarding the technical safeguards, baseline education of nurses in behavior-based threats to patient privacy, social engineering, cyber-security knowledge, mobile device use, and the theoretical framework of Rogers’ Protection Motivation Theory.

Through the literature review, gaps in the literature have been identified thereby necessitating the need for a national study of new nurses one year post-graduation to determine their information system security knowledge, mobile device use, risk behaviors, Concern for Information Privacy, level of Information Privacy Protection Response, the internal or external threat appraisal, and associations among these factors.

## Chapter 3: Methods

### Introduction

This chapter provides an overview of the study, research design, study population, sample and sampling procedures. With two new measures developed for the study and several existing measures modified for the national study, a full description about the instrument development in stages and pilot study data analysis are described.

### The Pilot Study to Develop the Measures – Study Variables

This study examines the associations between variables in the proposed model of nurses' knowledge, concern for information privacy, threat appraisal, risk behaviors, and information privacy protective responses. The following variables are operationally defined.

Risk Behaviors (RB): The information system risk behaviors factors associated with mobile device use amongst new nurses are variable results in the measurement of an overall risk score. These self-reported behaviors were compiled by the investigator, derived from several sources in the literature and developed into a measure (RB) of 21 items that are summed to yield a score from 0 to 21. These items and the resulting measures were assessed for content validity and reliability in the pilot study.

Knowledge of Information System (KISS): The knowledge of information systems security factors are variables presented to the subjects on the questionnaire. The level of nurses' information system security knowledge is a score from the survey questionnaire items resulting in an overall score that measures their information system security knowledge. The items were influenced from and authored similarly to studies conducted to assess medical students' knowledge of patient privacy and security issues concerning mobile devices (Whipple, Allgood, & Larue, 2012); health information system users' awareness of security issues (Aydın &

Chouseinoglou, 2013); but essentially authored by the investigator. The items selected for use in the survey were compiled by the investigator into a Knowledge of Information System Security (KISS) score ranging from 0 to 28 which was later slated for reduction to a range of 0-24 following the item elimination process. Each multiple choice item was considered as a single point in value with one point yielded per each correct response. These items and the resulting measures were assessed for content validity and reliability in the pilot study.

Concern For Information Privacy Index. (CFIP): The protection response mechanism of the use of the nurses own electronic health record is based upon the Concern For Information Privacy CFIP. This instrument was modified from the study by Kuo, Ma and Alexander (2014), incorporating additional items by Smith, Milberg and Burke (1996). It is composed of several subscales. The instructions for the items were changed to capture the nurses' response about his or her own personal information. The CFIP sum scores range from 0 to 15. The reliability was assessed in the pilot study.

CFIP Subscales: The subscales of the CFIP include the factors medical errors (ME), unauthorized access of medical information (UA), secondary use (SU), and personal collection of medical information (CO). The CFIP sum scores range from 0 to 12.

Mobile Device Practices: The level of nurses' information system security risk behavior and personal technology habits with mobile devices is another variable. The sum risk behavior scores range from 0 to 10 with the higher score indicating riskier behavior practices.

Information Privacy Protective Responses: Measuring the nurses' response to how they would feel about their own electronic health record use or information privacy protective responses (IPPR) mechanism is a dependent variable. Examined are the associations between

risk behaviors with the CFIP and IPPR. The sum scores of the IPPR range from 0 to 8 for the pilot.

Threat appraisal: This is the perception of a threat and motivation to take action as a result of this threat perception. This variable is operationalized into categories of “internal” threat to self (job, fines) and “external” threat/harm to others (healthcare institutions, patients). The four items are rank ordered by the respondent and sorted by rank in to threat groups.

### Pilot – Data Collection

Prior to data collection, the investigator developed new items for the *Knowledge and Risk Behaviors* measures based on the literature and the investigator’s professional experience. These items were presented to five judges with advance information system and/or security knowledge in order to assess for content validity. See the Appendix H - Content Validity: Student Nurses’ Knowledge of Information System Security and Risk Behaviors. Items were revised to consensus of form and wording. These were supplemented by the modified items on a questionnaire used in the pilot data collection.

On March 16, 2016, a pilot survey was distributed to Molloy College nursing students in advance of the subsequent nation-wide survey to be conducted with National Student Nursing Association member participants. This class of seniors completed the survey in paper-pencil form with all of the items on one questionnaire. These preliminary items were assessed for reliability based on the data collected.

### Sample

A sample of 167 third year Molloy College nursing students attending a scheduled group scholastic event served as subjects for the pilot study. With IRB approval for the pilot study as shown in Appendix D – Molloy College Institution Review Board Approval, this convenience

sample completed the survey and delivered them to the researcher in unmarked envelopes to maintain anonymity.

The Molloy College graduating nursing students completed all the items on the paper-based survey. The descriptive, correlational study was intended to assess participants' knowledge, information security risk behaviors with mobile devices and information personal protection responses to inform the researcher. The full study recruited new nurses one year following graduation from nursing school to obtain a national sample of volunteers who were members of the NSNA and had previously agreed to be surveyed in the future about their new jobs. Using this homogeneous group related to education as a criterion negates the possible influential factors deriving from a plethora of circumstances and involvements in subjects' occupational experiences. While subjects may vary in age, their nursing practice would be held constant to interpret the findings closer to issues related to their recent education than their life experiences in multiple healthcare institutions, controlling somewhat for education across all respondents.

### Design and Instrument Development

The survey consists of demographic details, an information systems security knowledge assessment section, appraisal of risk behaviors and information privacy protective responses. The demographic section blended SurveyMonkey® certified items with population specific interest items to inform the researcher. The knowledge section was entirely developed solely by the principal investigator. The information privacy protective responses section used items modified from the Kuo, Ma, & Alexander study ( 2014). This collective instrument was evaluated by a jury of five subject matter experts and modified to suit the elicited feedback. The fuzzy logic study from Aydın and Chouseinoglou (2013) spurred the development of the risk



behavior elements of the instrument's development. Many of this study's elements in many respects referred to technology that is either currently not trending in usage or not relevant to the population in question being studied. Therefore, elements were selected where relevant and altered to reflect the current information technology landscape and perceived potential usage among the population of interest. The knowledge survey was also developed by the dissertation author and submitted to the same jury of experts during the same period that the risk behavior elements were distributed for evaluation. See Appendix H - Content Validity: Student Nurses' Knowledge of Information System Security and Risk Behaviors for details.

The demographic information included on the survey was drafted to be congruent with the National Student Nurse Association annual survey questions. The pilot study demographics were not used in the analysis.

### Procedures

The investigator-developed measures were first assessed for content validity and prepared for data collection to assess reliability.

### Content Validity Index and Item Elimination Process

The knowledge and risk behavior portions of the survey instrument were developed in advance for the pilot through validation of five expert jurors. Following the content validity analysis, the survey was prepared for distribution.

The surveys were distributed to 167 senior nursing students as a convenience sample. The surveys were delivered as paper-pencil instruments by two Molloy College professors. Three \$25 Amazon gift cards were offered via a raffle and participation in whole or in part was not deemed to be a requirement for entry into the raffle. Students were instructed that their responses were to be kept anonymous and no identifiable data was requested. Students were

permitted to abstain from part or even all the survey responses. Students submitted the paper responses to the professors who collected and delivered the responses to the study investigator for evaluation.

### Knowledge Instrument Item Elimination

The sample results served to finalize the knowledge instrument. One subject was eliminated due to minimal participation in the survey. Others who did not respond to a question were graded as incorrect for that question. Those elements which received less than 50% correct response from the subjects were considered as eliminated for the instrument to be used for the national survey.

Furthermore, items were examined for the percentage correct by all pilot subject and graded on a shaded scale shown in the figure Elimination of Knowledge Items as either above, below, or near the 50% mark. All items found to be below the 50% mark were eliminated as part of an item discrimination and difficulty index manner of assessment for item elimination and retention.

Question	Percent Correct	Above 50%	Below 50%		
Question 10	87.4251497	x			
Question 11	83.85093168	x			GUIDE
Question 12	75.47169811	x			Near 50%
Question 13	90.3030303	x			Above 50%
Question 14	28.125		x		Below 50%
Question 15	78.91566265	x			
Question 16	96.40718563	x			
Question 17	43.29268293		x		
Question 18	60.47904192	x			
Question 19	16.16766467		x		
Question 20	72.12121212	x			
Question 21	88.41463415	x			
Question 22	64.84848485	x			
Question 23	68.90243902	x			
Question 24	66.66666667	x			
Question 25	100	x			
Question 26	14.81481481		x		
Question 27	54.81927711	x			
Question 28	21.81818182		x		
Question 29	69.6969697	x			
Question 30	96.95121951	x			
Question 31	64.81481481	x			
Question 32	91.41104294	x			
Question 33	80.24691358	x			
Question 34	89.63414634	x			
Question 35	47.5308642		x		
Question 36	94.51219512	x			
Question 37	80.86419753	x			
Question 38	94.44444444	x			
Question 39	74.375	x			
Question 40	88.88888889	x			

Figure 7 Elimination of Knowledge Items

### Human Protection

A Molloy College Institution Review Board application was filed and approved prior to conducting the survey process. Subjects were advised that participation was completely voluntary and without coercion. A statement to the voluntary nature of the survey was placed upon each page header along with the option to omit part or all the survey item responses. In addition, the header stated that all survey submission information would remain anonymous and participants' names were not requested. Three Amazon gift card valuing \$25 USD were awarded by a random raffle conducted by instructors with the explicit understanding that survey

omissions, in whole or in part, would not have been considered disqualifiers for participating in the award activity. The principal investigator maintained an active Collaborative Institutional Training Initiative Graduate Nursing Biomedical certification throughout the survey collection process.

### Reliability Statistics Methodology

The reliability statistics elimination process incorporated psychometrically sound steps involving the reduction of items that did not support the intended scale and subscale measurements.

### Reliability Statistics – Knowledge Test

The knowledge questions were tallied for each subject to produce an overall knowledge score. With 28 items, an N=126, and an exclusion of 40 participants, the Cronbach's alpha statistic estimate was .769. A reduction of items to 24 provided a Cronbach's alpha statistic estimate of .775 and those items could be used for the nationwide survey. In the final survey, 27 items were selected for use based on the item content (See Appendix H - Content Validity: Student Nurses' Knowledge of Information System Security and Risk Behaviors).

### Reliability Statistics – Risk Behaviors

A total of 10 participants with incomplete data were removed leaving an N=157. A Cronbach's alpha statistic estimate of .728 was obtained following the elimination of 5 of the 21 items thereby leaving 16 items remaining for the nationwide study.

### Reliability of Investigator Developed Measures

Using a thorough process of examining each item for its item discrimination index, difficulty index and coefficient alpha analysis, items were eliminated. The *Knowledge of Information System Security* (KISS) received a Cronbach's alpha statistic estimate of .775 after

eliminating four items and leaving 24 remaining. The *Risk Behaviors* (RB) score received a Cronbach’s alpha statistic estimate of .728 after eliminating five items and leaving sixteen remaining. These revised and finalized items were included on the SurveyMonkey® survey to the participants in the full study.

Threat Appraisals

The Threat appraisals (Internal and External) are 4 statements where respondents are asked to rank order them in the order of how much they perceive them as a threat, or in other words would “worry about” the consequence. These rankings are mutually exclusive. The statements were developed to yield assigned “threat” ranks to each respondent for the four items representing “internal” (I) or “external” (E) threat groupings. The statements were operationally defined by the rank of the perceived threat for respondents, yielding a grouping for each threat and differentiated as “internal threat appraisal” (i.e. an undesirable consequence that affects the self, such as losing a job, position, or being fined) and “external threat appraisal” (i.e. an undesirable consequence that affects others including hospital fined or patients’ privacy exposed). The survey included these four statements with the following instruction:

To measure Threat appraisal (I) and (E):\_Which of the following statements reflects your motivation to keep your patient information on the EHR secure? Rank order from lowest (least worry) to highest (most worry) (1 to 4).

Table 1 Threat Appraisal Taxonomy

INTERNAL THREATS	<input type="checkbox"/> I would worry about fines on me or my loss of position. <input type="checkbox"/> I would worry about my loss of employment.
EXTERNAL THREATS	<input type="checkbox"/> I would worry that my patients’ privacy would be exposed. <input type="checkbox"/> I would worry that my hospital would be fined.

### Reliability Statistics – Concern for Information Protection (CFIP) Total and IPPR

- The Cronbach's Alpha for all CFIP factors, including the IPPR, was found to be .890 with an N=153 after 14 participants had been excluded due to insufficient participation in this section of the survey.
- The Cronbach's Alpha for IPPR was .704 for 6 items, an N=156, and an exclusion of 11 participants.

### Reliability Statistics – CFIP Subscales

- The Cronbach's Alpha for UA, a subscale of the CFIP index, was found to be .861 with 3 items, and N=163, and after 4 participants had been excluded.
- The Cronbach's Alpha for SU was .883 for 3 items, an N=161, and an exclusion of 6 participants.
- The Cronbach's Alpha for ME was .875 for 3 items an N=159, and an exclusion of 8 participants.
- The Cronbach's Alpha for CO was .887 for 4 items, an N=159, and an exclusion of 8 participants.

### The Full National Study

The main question to be answered by the national study includes: What kind of activities do new nurses engage in with mobile technologies, including frequency of use, types of activities, and habits or behaviors that make them vulnerable to security risk? With the pilot study complete and a final survey instrument refined based on the pilot data, the full study was done on a national sample of new nurses in the United States. This descriptive, correlational study was done using an electronic version based upon the original paper survey and distributed via SurveyMonkey® to a list of 4,352 students from the National Student Nurses Association (NSNA) database of student members who graduated in 2016 and voluntarily provided their email addresses for follow-up.

## Sample

The National Student Nurses Association (NSNA) database was used to derive roughly 4,352 email contacts of RNs throughout the nation who have granted permission for follow-ups from past surveys. An approximate 30% of responses was anticipated to provide a samples size of approximately 1000.

Per a 2009 Economic Modeling Specialists International report, an estimated 190,615 individuals completed a nursing program. Without considering factors precluding graduates from being registered nurses one year later and assuming the 2009 figures are roughly an indicator of current graduation trends, the estimated sample size accounts for 0.53% of the population of all newly registered nurses. This study was estimated to have a 0.8 sufficient power and a medium size significance at  $\alpha = 0.05$ . With a 95% confidence interval and 5% accepted margin for error, a population size of 190, 615 and 50% response distribution would require a sample size of 384.

Therefore, an estimated sample size of 1000 would exceed the required 384 as a sufficient sample size.

## National Student Nurses Association Membership

Per the NSNA website, this nonprofit organization was founded in 1952 for enrolled nursing students with a dedication to fostering the professional development of nursing students. With over 60,000 members, this organization has representation through the United States including all fifty states, the US Virgin Islands, Guam, Puerto Rico and the District of Columbia. Its mission is “to mentor students preparing for initial licensure as registered nurses, and to convey the standards, ethics, and skills that students will need as responsible and accountable leaders and members of the profession.” (NSNA, 2015).

According to Feeg and Mancino (2015), this organization has conducted annual web-based surveys over the past seven years including recently graduating past members who agree to receive follow-up surveys.

### Method

A sample of new nurses with approximately one year of experience completed a web-based survey. The descriptive, correlational study acquired participants' educational experiences to inform the researchers. Using the limited experience among nurses as a criterion reduces the possible influential factors deriving from a plethora of circumstances in subjects' occupational activities, including likely limiting the exposure to security awareness training through the employer. The HIPAA Security Rule requires workforce awareness training for covered entities such as hospitals and physician practices. Therefore, reducing work experience limits the subjects' likely exposure to employer training. Subjects may vary in age while the analysis of the data reflects that the work experience factor is controlled.

### Population Studied

The population consists of new nurses throughout the United States who were members of the National Student Nurse Association. This database provides the investigator with a national sample of nurses from all types of hospitals or health care organizations with similar experience at the time of the study. These individuals gave their permanent email addresses for future studies. They had graduated approximately one year prior.

### Sample

The sample drawn from a list of more than 4,000 past members of the National Student Nurse Association who willingly agreed to volunteer for surveys by giving their email addresses.



## Recruitment Method

The NSNA has a database of members, a subset of which are graduates who have agreed to receive surveys. The NSNA had permitted the distribution of surveys although they retained control over the distribution and at no time did the principal investigator have access to the member database or the ability to distribute the surveys. The SurveyMonkey® application allows for blinded email addresses to receive the survey with assurance of anonymity. Each invitation had information about the survey, estimated time of duration to complete the survey, and an option to be eligible for a \$250 drawing. Using the Dillman, Smyth, & Melani (2008) method of distribution, subjects were recruited and reminded with subsequent mailings.

## Variables Specified – Instrument Items (Appendix I – Survey Instrument (National Survey))

### *Descriptive Variables*

- Demographics – Items 1-5
- Personal Use of Mobile Devices (PUMD) – Items 8-11
- Personal Technology Practices (PTP) – Items 12-15
- Mobile Device Habits (MDH) – Item 16

### *Aggregate Measures*

- Knowledge of Information System Security (KISS) – Items 18-44
- Risk Behaviors (RB) Score – Item 17
- CFIP: Concern for Information Privacy – Items 6, 7g-j)
- Subscales of CFIP:
  - UA: Unauthorized Access to Medical Information (6a-c)
  - SU: Secondary Use of Medical Information (d-f)
  - ME: Medical Facility Errors (g-i)

- CO: Personal Collection of Medical Information (7g-j)
- IPPR: Information Privacy Protective Responses, a response to the CFIP – Item 7 (c-h),  
Items 7a-b omitted to elevate the coefficient alpha=.758 with 6 items
- Threat Appraisal as a measure of statements (Internal and External) – Item 45

Refer to corresponding items as listed in Appendix I – Survey Instrument (National Survey).

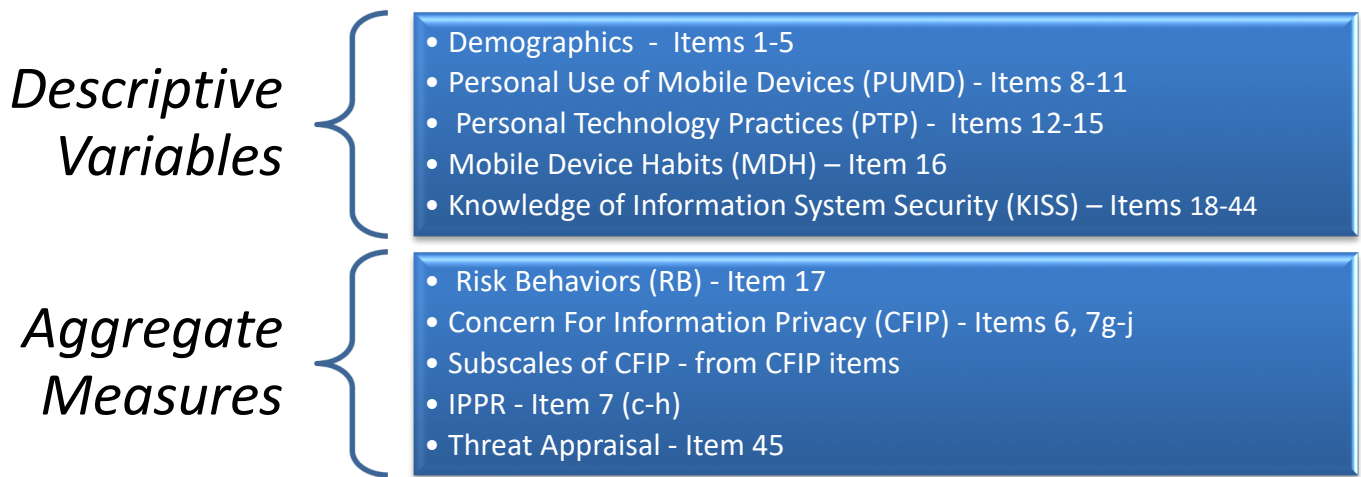


Figure 8 Descriptive Variables and Aggregate Measures

### Relational Variables

The variables studied in relation to the CFIP include the information system security behaviors of the subjects specifically with mobile devices. Examined are the relationships between this behavior and the CFIP. Knowledge is considered to be the precursor and another variable for which relations with other variables were examined. Threat appraisal may play a mediating role. Particular demographics may influence risk behaviors as well and is also tested.

### Procedure

The survey was sent via SurveyMonkey® to the eligible list of subjects' email addresses with a statement of informed consent and information to proceed. The list was supplied by and the delivery managed by the National Student Nurse Association (NSNA). Subjects were instructed that their participation was voluntary, and responses considered to be anonymous. An incentive of a \$250 gift card raffle was offered to a single participant selected at random out of those who voluntarily include their email address for follow-up on the raffle results. This information was technically de-identified from the response set of answers to the survey questions. Participants were informed that their email addresses collected for the raffle and survey responses would be collected and kept separate.

### Data Collection Methods

The data were collected electronically via SurveyMonkey® and sent without subject-identifying factors to the principal investigator.

### Hypotheses

A series of hypotheses were tested on the variables of interest. A correlation matrix for selected variables were done to determine where and if relationships among the variables exist.

The preliminary correlation analyses allowed further consideration of specific tests of models derived from the literature and theory. These focused on the following hypotheses tested:

### Hypothesis Statements

H<sub>0</sub>: An increase in Information Privacy Protective Responses does not result in a decrease in identified risk behaviors.

H<sub>1</sub>: An increase in Information Privacy Protective Responses results in a decrease in identified risk behaviors.

H<sub>0</sub>: An increase in information system security knowledge does not result in a decrease in identified risk behaviors.

H<sub>2</sub>: An increase in information system security knowledge results in a decrease in identified risk behaviors.

H<sub>0</sub>: An increase in information system security knowledge does not result in a decrease in Concern for Information Privacy.

H<sub>3</sub>: An increase in information system security knowledge results in a decrease in Concern for Information Privacy.

H<sub>0</sub>: An increase in information system security knowledge does not result in a decrease in Concern for Medical Facility Errors.

H<sub>4</sub>: An increase in information system security knowledge results in a decrease in Concern for Medical Facility Errors.

H<sub>0</sub>: An increase in information system security knowledge does not result in a decrease in Concern for Unauthorized Access to Medical Information.

H<sub>5</sub>: An increase in information system security knowledge results in a decrease in Concern for Unauthorized Access to Medical Information.

H<sub>0</sub>: An increase in information system security knowledge does not result in a decrease in Concern for Secondary Use of Medical Information.

H<sub>6</sub>: An increase in information system security knowledge results in a decrease in Concern for Secondary Use of Medical Information.

H<sub>0</sub>: An increase in information system security knowledge does not result in a decrease in Concern for Personal Collection of Medical Information.

H<sub>7</sub>: An increase in information system security knowledge results in a decrease in Concern for Personal Collection of Medical Information.

H<sub>0</sub>: An increase in information system security knowledge does not result in a decrease in Information Privacy Protective Responses.

H<sub>8</sub>: An increase in information system security knowledge results in a decrease in Information Privacy Protective Responses.

H<sub>0</sub>: An increase in Concern for Information Privacy does not result in a decrease in identified risk behaviors.

H<sub>9</sub>: An increase in Concern for Information Privacy results in a decrease in identified risk behaviors.

H<sub>0</sub>: An increase in Concern for Medical Facility Errors does not result in a decrease in identified risk behaviors.

H<sub>10</sub>: An increase in Concern for Medical Facility Errors results in a decrease in identified risk behaviors.

H<sub>0</sub>: An increase in Concern for Unauthorized Access to Medical Information does not result in a decrease in identified risk behaviors.

H<sub>11</sub>: An increase in Concern for Unauthorized Access to Medical Information results in a decrease in identified risk behaviors.

H<sub>0</sub>: An increase in Concern for Secondary Use of Medical Information does not result in a decrease in identified risk behaviors.

H<sub>12</sub>: An increase in Concern for Secondary Use of Medical Information results in a decrease in identified risk behaviors.

H<sub>0</sub>: An increase in Concern for Personal Collection of Medical Information does not result in a decrease in identified risk behaviors.

H<sub>13</sub>: An increase in Concern for Personal Collection of Medical Information results in a decrease in identified risk behaviors.

H<sub>0</sub>: An increase in Concern for Personal Collection of Medical Information does not result in a decrease in identified risk behaviors.

H<sub>14</sub>: An increase in Concern for Personal Collection of Medical Information results in a decrease in identified risk behaviors.

### Threat Appraisals – Stated in the Null

For the threat appraisal hypotheses to test knowledge, risk, concern or protective response mean score differences by rankings of threat on each of the four statements of threat, the hypotheses are stated in the null:

Internal Null Hypotheses: Internal threats are not associated with knowledge, risk, concerns or protective responses.

External Null Hypotheses: External threats are not associated with knowledge, risk, concerns or protective responses.

### Ethical Consideration and Consent – Human Subject Protection

The study was submitted to the Molloy College Institutional Review Board (IRB) for approval. The National Student Nurses Association (NSNA) managed the correspondence to the eligible sample so that the researcher could not identify participants who do not self-disclose their email addresses by choice.

The information collected must be kept completely identified and anonymous. Subjects may have trepidation about disclosing their professional behavior and knowledge should they perceive a possibility that this information may be associated with their identity and recorded. The absence of requesting employer information is intended to encourage socially desirable responses. Using the anonymity function of SurveyMonkey® assured respondents that their information could not be shared with anyone. The separation of their information from their request to be eligible for the \$250 raffle was done electronically. No identifying information can be associated with any answers.

## Analysis

Descriptive analysis of the survey statistics on this national sample for items that assess mobile device use, frequency of use and other behaviors. The demographics and variables of interest are described with frequency statistics and measures of central tendency. As preliminary tests of inter-correlations between the subjects' knowledge, risk behaviors, CFIP, and IPPR, correlation and regression analyses were done. Threat appraisal was established as categories for each of the four threats and used to test differences in study variables by participants' threat ranks.

The results of the survey in SurveyMonkey® were exported in SPSS format and into SPSS Version 23 for analysis. Descriptive, correlational were done if the data met assumptions and the measures were deemed reliable. Analysis of the CFIP index and its subscales for granularity were evaluated for associations with knowledge, risk behaviors, and the subjects' IPPR and threat appraisal.

## Chapter 4: Findings

### Introduction

The purpose of this descriptive study was to explore in a national sample of nurses one year after graduation in HIT knowledge about security and risk behaviors related to their use of portable electronic devices, their knowledge of information system security, and the influence, if any, of their personal protective motivation to protect patient care information. This sample of nurses that are homogeneous with respect to experience provided a focus on how they were prepared in their nursing education in relation to information system security in order to inform educators in the future. This chapter presents the sample characteristics, descriptive summary of the general responses, and psychometric properties of the measures used in the research questions. It summarizes the overall questions and then specifies and tests hypotheses for the final research questions. Finally, summaries the general and specific findings to begin to construct a model for understanding the main research question and sub-questions:

1. How much do new nurses know about security of information systems and does their knowledge influence their risk behaviors in using mobile technology?
  - a. What kind of activities do new nurses engage in with mobile technologies, including frequency of use, types of activities, and habits or behaviors that make them vulnerable to security risk or concern about protecting patient information?
  - b. What is the level of new nurses' knowledge, risk, concern for information privacy, their protective responses to information privacy; how are these related and affected by their threat appraisal (internal or external) to themselves, their hospitals, or their patients?
  - c. Is knowledge, risk, concern or protective responses influenced by select demographic characteristics such as gender, age and education (education type or school type)?



Using Dillman's (2008) method of distribution, subjects were recruited via an email distribution to NSNA members who were one-year post-graduation and had agreed to be contacted for survey purposes. The result yielded 649 returned SurveyMonkey® surveys from nurses. Analysis of the data resulted in the removal of 135 respondent results as they did not complete the knowledge section of the survey. Therefore, a sample of n=514 was selected for analysis as the responses were either fully or nearly fully complete. Information pertaining to phone type is not analyzed with other variables and stood alone for analysis. Therefore, all respondents who provided this information were used for an N=550, not just the 514 who completed or nearly completed all elements in the survey.

### Characteristics and Demographics

For all of the characteristic and demographic details discussed in this chapter, the final cleaned data from the sample of n=514 is used. The gender analysis indicated an 87.9% female (N=452) to 12.1% male (N=62) composition, which is roughly consistent with the United States' nursing population. The United States Department of Labor indicates a 92% to 8% female to male composition of registered nurses overall nationwide without any differentiation of education or experience, however, the membership of the National Student Nurses Association (NSNA) compares favorably with this sample. The education analysis indicates that 71% of respondents have a baccalaureate degree or higher for (n=365) whereas those with an Associate degree or diploma (n=142) account for 27.6%. These results are comparable with the results from other NSNA survey data as well. Those aged 32 or younger (n=345) are roughly double the representation of their counterparts over the age of 32 (n=169). Those aged 49 or older (n=36) make up only 7% of the sample. A conceivable explanation for the age make up is that the intended target for the survey was comprised of nurses who graduated the year prior in an effort

to limit variation in experience among the sample. Presumably, some of the advanced degree nurses may have had prior experience, but overall respondents' reported education type indicates recent entry into the profession. Degrees generally considered entry points to the profession (Associates Degree Diploma, Baccalaureate Degree, Accelerated BSN program) make up the 91.4% majority (n=470) of the sample. Race was collected as an NSNA standard demographic element and displayed as part of the descriptive analysis. At 73.3%, the majority of the respondents (n=377) reported themselves as Caucasian. The ratio of public-private school type is comparable to the membership of NSNA with twice as many public school respondents as private (not for-profit schools) and four times as many public school respondents as private-for-profit schools.

Table 2 Sample Characteristics

		<b>Sample Characteristics</b>	
		Frequency	Percent
<i>Gender</i>	Male	62	12.1
	Female	452	87.9
	Total	514	100.0
<i>Degree Type</i>	Other (please specify)	5	1.0
	Associates Degree	125	24.3
	Diploma	17	3.3
	Baccalaureate Degree	243	47.3
	Accelerated BSN program	85	16.5
	Master's Degree	9	1.8
	Clinical Nurse Leader Masters	5	1.0
	Doctorate	1	.2
	RN to BSN	22	4.3
	Total	512	99.6
	Missing	2	.4
<i>Age Range</i>	≤32	345	67.1
	33-48	133	25.9
	≥49	36	7.0
	Total	514	100.0
<i>Race</i>	Other (please specify)	7	1.4
	American Indian or Alaskan Native	3	.6
	Asian	38	7.4
	Black or African American	35	6.8
	Caucasian	377	73.3
	Hispanic or Latino	29	5.6
	Mixed Race	21	4.1
	Native Hawaiian or other Pacific Islander	1	.2
	Total	511	99.4
	Missing	3	.6
<i>School Type</i>	Other	13	2.5
	Public	292	56.8
	Private not-for-profit	138	26.8
	Private proprietary for-profit	71	13.8
	Total	514	100.0

## Phone Characteristics

As the survey instrument pertains to the use of mobile devices among new nurses, the types of mobile phones used among respondents was collected to texture the study with descriptive data. This information was collected as free-text entries and tabulated both by manufacturer and operating system. Please note that the survey collected information about “personal use of technologies at work and at home.” The survey did not draw a distinction between hospital-issued and personally-owned devices whether for work or home use. At the time of this dissertation, the use of personal mobile phones in the workplace for clinical use has yet to be established commonplace for nurses. In the clinical setting, phone use among nurses is most commonly limited to voice functionality for communication (Parker, 2014). The emergence of bring-your-own-device (BYOD) modalities for smart phone features are more commonly witnessed among non-clinical staff for business purposes.

Table 3 Phone Operating System

Phone Operating System	Frequency	Percent
Android	159	28.91
iOS	389	70.73
Windows	2	0.36
Total	550	100

New nurses tend to use the iOS phone operating system more so than the general population. According to Gartner, Android had captured 86.1% of the world’s phone market compared to 13.7% for iOS in the first quarter of 2016 (Reisinger, 2017). Save the two Windows entries, the phone operating system appears among respondents to be somewhat inverse to the worldwide prevalence. The sales figures for Apple and Samsung, its major competitor in the Android marketplace, are tabulated by the respective manufacturers differently

thereby making the comparison an arduous task. Furthermore, Google’s Android operating system produces a broad range of device models from a plethora of competitors and even numerous concurrent offerings from each manufacturer. With even more manufacturers, a fractured marketplace with an assortment of devices of varying qualities and features is emerging. Apple on the other hand exclusively supports a single model operating system type (iOS) on a single line of phone products (iPhone) thereby controlling both the hardware and software with a single manufacturer.

Apple represents 70.73% of the usage among new nurses. Samsung is the largest competitor to Apple with their phones using the Android operating system. The results of the study show Samsung representing 21.64% of the phone usage and represents by far the largest denomination of manufacturers using Google’s Android operating system.

Table 4 Phone Manufacturers

Phone Manufacturer	Frequency	Percent
Alcatel	1	0.18
Android	1	0.18
Apple	389	70.73
Blackberry	1	0.18
Blu	1	0.18
Google	12	2.18
HTC	2	0.36
LG	12	2.18
Motorola	8	1.45
Nokia	1	0.18
Samsung	119	21.64
Windows Based	1	0.18
ZTE	2	0.36
Total	550	100

As the information pertaining to individual phone manufacturers was collected as a free-text field, results were at times carefully inferred by various spellings and use of ambiguous model numbers. The information is provided but any analysis using these data is out of this study's scope. One manufacturer was listed as "Windows" with the Blu phone speculatively as the other possible Windows operated phone making up the two Windows phones from previous table. Blu has historically made phones with the Windows operating system, but typically markets lower cost phones operated by Android.

### Descriptive Findings of The Study

To answer the main question of the study "How much do new nurses know about security of information systems and does their knowledge influence their risk behaviors in using mobile technology?" it is important to first describe the common mobile technology use of the participants. The first sub-question for the study is as follows:

*What kind of activities do new nurses engage in with mobile technologies, including frequency of use, types of activities, and habits or behaviors that may make them vulnerable to increasing the security risk?*

To begin to answer this question, a series of descriptive statistics were performed on questions about mobile application use and reported practices in securing devices on personal and hospital devices.

### Mobile Application Use

To answer the survey question "What is the reported level and type of new nurse mobile application use?" a series of descriptive analyses were done on their reported responses in the table Smart Phone Use By Feature. The category of "very often" received the most responses for the following features: Text Messaging (N=272), Social Media (N=250), and Web Browsing

(N=234). An 88.5% majority of respondents (N=455) reported use of social media frequency between sometimes to very often. Those features that were most often not used include the following: Chatting (N=94), Online Library (N=90), and Video/Movies (N=50). Very few respondents declared that features were unavailable; the largest segment include the following: Online Library (N=14), Chatting (N=8), and Contact List (N=2). Given that all respondents declared that they use a modern smart phone with the exception of a few ambiguous responses, the surveyed features should all be available. The exception may be that work-managed phones may have such features disabled and such differentiation was not determined in the survey. The Online Library feature, like many others surveyed, is not necessarily a native phone application, but rather an additional application or website. This feature was declared by the most number as not being available which may suggest that the question was not understood.

Table 5 Smart Phone Use By Feature

<b>Mobile (Smart Phone) Usage</b>	Minimal	Rarely	Sometimes	Often	Very Often	Do Not Use	Feature Not Available
<i>Talking</i>	54	65	195	125	63	11	1
<i>Web Browsing</i>	3	14	97	161	234	3	1
<i>Chatting</i>	73	87	92	90	67	94	8
<i>Email</i>	16	21	144	197	130	3	0
<i>Text Messaging</i>	3	8	62	166	272	2	1
<i>Multimedia Messaging</i>	28	60	166	121	114	22	1
<i>Camera</i>	30	41	166	162	108	6	1
<i>Calendar</i>	36	46	125	166	136	4	1
<i>Notes</i>	75	105	166	100	41	26	0
<i>Contact List</i>	33	78	193	129	76	3	2
<i>Maps/Navigation</i>	14	34	146	184	128	6	0
<i>Social Media</i>	19	27	78	127	250	13	0
<i>Music</i>	38	60	125	135	136	20	0
<i>Video/Movies</i>	94	128	111	75	54	50	1
<i>Online Library</i>	104	132	101	38	34	90	14

## Security Practice Results

To answer the survey question about basic security practices, a series of descriptive statistics were calculated on participants' reported responses as indicated in the Practice Responses table describing the frequencies of basic security practice of locking a device among new nurses. The survey included a matrix style question to determine how often respondents lock their phones and other mobile devices which includes both hospital-owned and person devices. The process of locking a device does not permit usage until subsequent authentication is validated. Contemporary common methods of validation include a username-password combination, numerical passcode, password, finger scan, pattern drawing, and facial recognition.

Table 6 Practice Results (By Percentage)

<b>Practices</b>	<b>Never</b>	<b>Rarely</b>	<b>Sometimes</b>	<b>Often</b>	<b>Always</b>	<b>Device Not Capable</b>	<b>Not Applicable</b>
Lock Personal Phone	10.5	2.3	3.3	4.5	79.0	.2	.2
Lock Personal Mobile Device (Laptop/Tablet)	6.2	4.3	5.3	11.1	68.9	1.6	2.7
Lock Hospital-Provided Phone	4.1	.8	2.5	2.7	16.9	16.9	56.0
Lock Hospital Provided Mobile Device (Laptop/Tablet)	1.9	.8	2.1	8.6	23.9	4.5	58.2

The results indicate that the “always” response is prevalent with personal phones and mobile devices whereas over half of respondents list the same hospital-owned devices as not applicable for locking. Hospital provided phones and mobile devices are considered as not applicable 56.0% and 58.2% respectively. A possible explanation for the rate whereby locking is not applicable may either be related to the lack of hospital-owned devices in use by nurses. Another possibility is that the prevalence of device and network management systems in hospital settings may enforce an automatic locking of devices regardless of human intervention.



The locked personal phones and devices indicate a rate of 83.5% and 70.5% respectively for those who responded with often and always as a practice. This indicates a high rate of safe practices among respondents for the security of physical access to their personal devices.

### **Knowledge of Information System Security and Risk Behaviors of New Nurses**

The main question driving the study can be broken into a series of questions related to the new nurses' specific cybersecurity knowledge, risk, and personal characteristics including:

What is the level of new nurses' knowledge of information system security (KISS), risk behaviors (RB), concern for information privacy (CFIP), their information privacy protective responses (IPPR), and how are these affected by their threat appraisal (internal or external) to themselves, their hospitals, or their patients? Concern For Information Privacy (CFIP) can also be categorized by factors including:

- a. medical facilities errors (ME)?
- b. unauthorized access to medical information (UA)?
- c. medical facilities secondary use of medical information (SU)?
- d. personal collection of medical information (CO)?

The following variables have been collected on the survey questionnaire as follows. The CFIP along with subscales, the IPPR, KISS, RB, and threat appraisal are analyzed descriptively in the following section. The measures developed for this study to measure knowledge and risk were assessed in the pilot study and psychometrically assessed for reliability again in this study. Displayed below are the variables with corresponding item numbers from the survey. Following the declaration of variables is a table displaying a breakdown of the scales and a separate table for threat appraisal (Appendix I – Survey Instrument (National Survey)).

- *Demographics – Items 1-5*
- *CFIP: Concern for Information Privacy – Items 6, 7g-j)*
- *Subscales of CFIP:*
  - *UA: Unauthorized Access to Medical Information (6a-c)*
  - *SU: Secondary Use of Medical Information (d-f)*
  - *ME: Medical Facility Errors (g-i)*
  - *CO: Personal Collection of Medical Information (7g-j)*
- *IPPR: Information Privacy Protective Responses, a response to the CFIP – Item 7 (c-h), Items 7a-b omitted to elevate the coefficient alpha=.758 based on 4 items.*
- *Personal Use of Mobile Devices Items 8-11*
- *Personal Technology Practices – Items 12-15*
- *Knowledge of Information System Security (KISS) – Items 18 -44*
- *Risk Behaviors (RB) Score – Items 17*
- *Threat appraisal (Internal and External) – Item 45*

### Level of Knowledge

What is the level of new nurses’ knowledge of information system security (KISS) related to patient privacy, security rules, and vulnerability to breaches or threats to exposing protected health information (PHI)?

The tables Knowledge Score Descriptive Statistics and Knowledge Results for instrument element-specific results. The Knowledge Score Frequency Chart displays the frequency distribution.

Table 7 Knowledge Score Descriptive Statistics

	<b>N</b>	<b>Minimum</b>	<b>Maximum</b>	<b>Mean</b>	<b>Std. Deviation</b>
Knowledge Score	514	0.33	1	0.8297	0.10667

The KISS scores overall show an average of 82.97% correct results. Within the KISS instrument are a few items with results diverging noticeably from the overall instrument mean score.

The knowledge item pertaining to the right to access a relative/spouse/partner/friend's electronic health information (Item 4) is the second lowest result in correct responses at 42.2%. Note that the questions are displayed in their entirety in the table with the ellipses completed by the multiple choice answers. The complete knowledge instrument with all response options and indicators for correct responses can be viewed in Appendix H - Content Validity: Student Nurses' Knowledge of Information System Security and Risk Behaviors.

Table 8 Knowledge Results

Item Number	Question	Percent Correct
Knowledge 1	Putting patient information on a USB drive is acceptable if...	92.8
Knowledge 2	Texting patient information is acceptable if...	88.7
Knowledge 3	Placing patient information on my personal computer is acceptable if...	75.5
Knowledge 4	I may access my relative/spouse/partner/friend's electronic health information if...	42.2
Knowledge 5	If a police officer requests a copy of the patient's chart...	99.0
Knowledge 6	If I find a USB drive around the hospital, I...	95.7
Knowledge 7	If I discover a coworker has accessed their relative's information, I...	64.2
Knowledge 8	If someone calls from the helpdesk requesting my password, I...	60.5
Knowledge 9	I can put patient data on a USB stick if...	96.1
Knowledge 10	If a website informs me that JAVA must be updated, I...	73.3
Knowledge 11	If a computer message from the FBI states my files have been scrambled and I must pay a \$300 fine, I...	88.7
Knowledge 12	If the IRS calls me about overdue taxes and requests a wire transfer, I...	99.6
Knowledge 13	An email from my bank states my account had been compromised and I must verify my identity by clicking on a link and filling out some information, I...	99.4
Knowledge 14	My coworker received a strange email from me requesting money, I...	65.8
Knowledge 15	A well-known national realtor sends an email with the subject "Hot Properties in Your Neighborhood." The link requests a Gmail or Yahoo login to proceed. Assuming there's an interest, I...	27.4
Knowledge 16	The corner deli that typically delivers lunch complains they received a fax with patient information, I...	80.4
Knowledge 17	When leaving a computer logged in with my password, I...	97.9
Knowledge 18	A pop-up appears informing me the computer is running slow, I...	69.5
Knowledge 19	Taking patient or chart photos with my own cell phone is acceptable if...	84.6
Knowledge 20	A person without a hospital badge states he is from IT and needs me to login for him to fix the slowness problem, I...	94.2
Knowledge 21	I may work with documents containing patient information on my home computer or laptop...	91.6
Knowledge 22	If I need to look at my health records, I...	90.7
Knowledge 23	If a law firm requests patient information, I...	98.8
Knowledge 24	If a standard computer without encryption has a sensitive file that is purposefully deleted...	84.4
Knowledge 25	It's acceptable to backup patient information to my personal cloud (Google Drive, Dropbox, iCloud, etc...) for safekeeping...	96.5
Knowledge 26	If my coworker suspects someone must have looked at his/her health record due to gossip about his/her condition, I would...	89.1
Knowledge 27	If I cannot find my laptop/tablet containing sensitive information, I...	93.6

The knowledge scores displayed in the graph below shows a slightly skewed frequency distribution of respondents tending to score in the higher end range according to the Knowledge Score Frequency Chart. While outlying scores exist in the lower range, this graph suggests that new nurses one-year tend to have a homogenous knowledge of information system security generally speaking. Given that nursing schools are responsible for at least some training to prepare students for hospital experiences, it is a reasonable expectation that the shape of the curve reflects how tests might be graded with the mean, median and mode around a grade of B. No inference of knowledge related to information system security is however presumed but rather the curve is akin to school test score distributions.

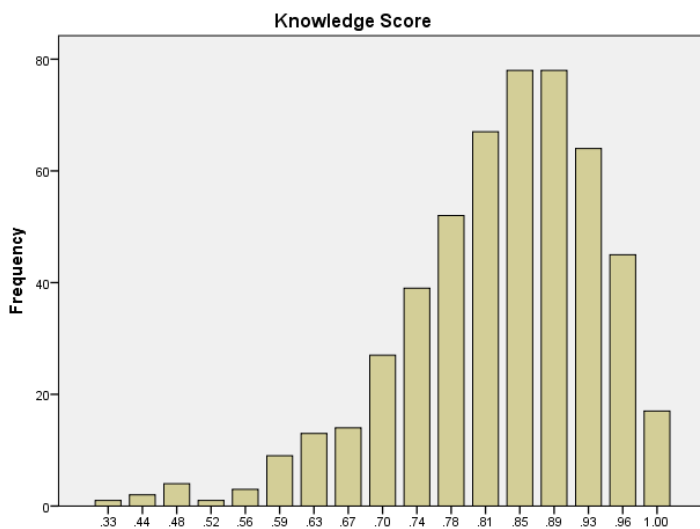


Figure 9 Knowledge Score Frequency Chart

### Level of Risk

What is the level of risk behavior of nurses and types of risk behaviors related to their use of mobile devices?

The Risk Behavior Score Descriptive Statistics table shows the instrument element-specific results. With an n=154, the mean risk behavior score is 68.86 with a standard deviation of 9.348.

Table 9 Risk Behavior Score Descriptive Statistics

	<b>N</b>	<b>Minimum</b>	<b>Maximum</b>	<b>Mean</b>	<b>Std. Deviation</b>
Risk Score	514	46	145	68.86	9.348

The Risk Behavior scores overall show a mapping of the behavior frequency among new nurses. Within the Risk Behaviors' elements are results that stand out as items for discussion.

An overwhelming 94.9% of new nurses do not send patient information via personal email. That leaves 3.6% of new nurse, who in varying levels of frequency, would send patient information via email. Note that purpose for using personal email to send PHI was not asked. To some degree 18.9% of participants obtain content outside of legitimate sources.

Security modalities such as antivirus and firewalls are not used by 41.4% of new nurses. One plausible explanation is that security modalities tend to have historically been more in commonplace usage with desktops and laptops than the prolific mobile devices such as phones and tables. Speculatively, these may not be used among respondents with their laptop use, but this has not been asked in such a granular fashion.

In the reported behaviors, it would appear that financial data breaches occurred in 30% of new nurses. Conversely, only 27.4% of new nurses recognized the phishing attack from the knowledge survey. The question did not offer any determination as to how the data may have been breached or to what degree. The data suggests that new nurses may lack knowledge of key areas of common attack by nefarious agents, do not employ protective security modalities by and large, and many may have already suffered data breaches with financial implications by the time they embarked on their career.

Table 10 Risk Behaviors Results

<b>Risk Behaviors</b>	<b>Never</b>	<b>Rarely</b>	<b>Sometimes</b>	<b>Often</b>	<b>Always</b>
I accept social media invitations for applications.	35.8	30.0	23.9	4.1	1.2
I shop on the Internet.	.6	6.2	41.4	43.0	8.6
I use Facebook, Twitter and similar social network sites.	3.7	6.0	18.3	44.0	27.8
I download/save music, movies, programs and files from the Internet.	14.0	30.9	28.4	21.0	5.1
I share my contact information on the Internet when required.	8.0	28.8	43.0	16.9	2.9
I use security programs like anti-virus, spyware removal, firewall, etc.	41.4	18.9	19.8	9.9	6.4
I delete the temporary files and Internet history before leaving a public computer.	24.1	13.6	17.7	17.7	13.8
I password protect my files.	24.3	15.6	23.0	17.5	17.5
I use complex and long passwords that cannot be easily guessed.	41.8	29.6	21.6	4.1	2.7
I change my passwords periodically.	19.5	26.1	31.5	15.8	7.0
I share my passwords with others.	68.1	25.5	5.1	.6	.2
I transfer (send or receive) files while I chat.	38.7	29.6	18.9	5.3	2.1
I use passwords when turning on all of my devices.	52.1	20.4	15.0	6.0	5.3
...“jailbreak”, or use a customized environment to get free apps.	83.9	7.4	2.1	.8	.2
...click on email links to reset my password.	32.3	17.5	35.0	10.7	3.3
...use free Wi-Fi at public locations such as cafes and airports.	3.5	22.4	45.1	22.4	6.6
...keep my device attended and in my possession.	74.9	20.4	2.9	1.0	.6
...text patient information with colleagues (aside from corporate applications).	84.4	8.8	3.1	1.0	.8
...use personal email containing patient information.	94.9	1.8	.8	.8	.2
...accept invitations for games and apps through social networks.	66.9	21.0	9.3	1.2	.4
...download movies/music/apps by pirating or otherwise without paying (aside from legit streaming services).	80.4	12.1	6.0	.4	.4
...share my password (any) with others such as family, friends, or coworkers	68.1	23.9	6.2	1.2	.6
...use autofill to complete my information in websites.	12.8	21.0	43.8	18.1	4.1
...submit my personal information such as name, address, phone number, and credit card info into websites when requested.	11.7	23.0	43.4	19.1	2.7
...chat with strangers online.	85.8	11.1	2.1	.8	.2
...post personal information on social media sites.	45.7	36.0	13.6	3.9	.6
...have had my financial/credit information personally breached (aside from publicized breaches of corporations).	69.3	21.8	7.0	1.0	.2
...have had my passwords stolen/misused. (Evident by unauthorized emails/posts or services accessed by unauthorized entities)	75.3	18.5	4.1	.2	.4
...chat with others about patient information outside of work.	79.0	13.6	5.4	.6	.2

The risk behavior score frequency in the graph below shows an approximately normal distribution around the mean. While outlying scores exist in the higher range, this graph suggests that new nurses tend to have a relatively even distribution of knowledge of risk behaviors with most falling in the medium risk range.

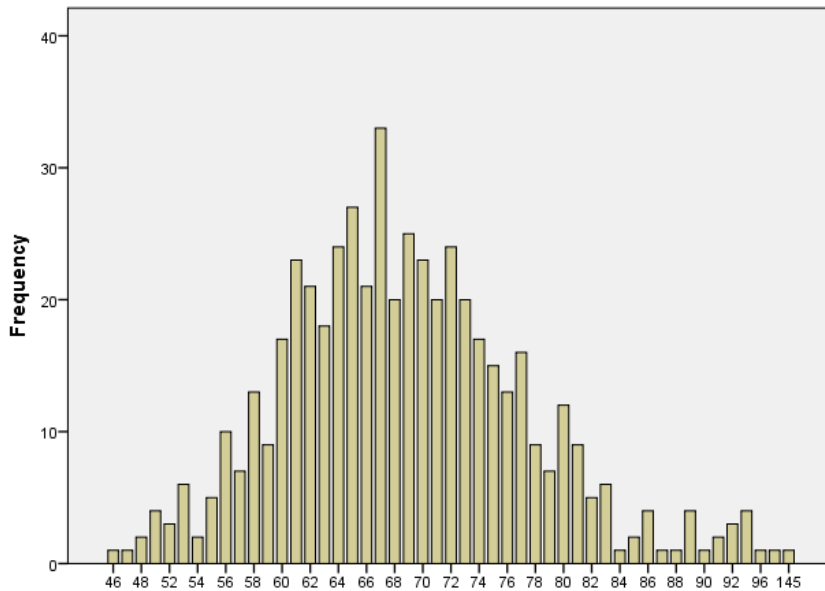


Figure 10 Risk Habit Score Frequency Distribution

### Information Privacy Protection Responses and Concern For Information Privacy

What is the level of new nurses' Information Privacy Protective Responses (IPPR) and Concern for Information Privacy (CFIP) factors?

The survey questions to capture measures for Concern for Information Privacy and Information Privacy Protective Responses were developed from an original questionnaire by Kuo, Ma, and Alexander (2014) and modified to capture new nurses' responses to the items as they would pertain to themselves rather than patients' responses. These new variables were tested for feasibility and reliability in the pilot study and reported in Chapter 3. The items were reduced following a careful assessment of the item analyses and the items were captured on the



full study. A descriptive analysis was done on the CFIP total scale and the 4 subscales as described by Kuo et al. (2014) and reported in the CFIP and IPPR Descriptive Statistics table.

Table 11 CFIP and IPPR Descriptive Statistics

	<b>N</b>	<b>Minimum</b>	<b>Maximum</b>	<b>Mean</b>	<b>Std. Deviation</b>
Total CFIP AU	513	6	18	11.56	2.463
Total CFIP SU	514	3	18	13.63	1.957
Total CFIP ER	510	6	18	11.60	2.302
Total CFIP CO	510	4	22	10.52	3.867
Total CFIP	505	28	65	47.35	6.861
Total IPPR	512	4	24	15.93	2.997

### Reliability of All Measurement Scales

The instrument reliability for all the study scales were assessed and reported in the Instrument Reliability table (Table 12), showing the Cronbach’s alpha statistic estimate for both the pilot (n=167) and current nationwide study (n=514). The reliability goal was to have a Cronbach’s alpha statistic estimate of .70 or greater for each instrument. While elements from the pilot study original questionnaire were dropped to achieve this goal, remaining elements of the current nationwide study were left intact. All elements except the knowledge instrument attained the goal with KISS having a Cronbach’s alpha statistic estimate of .669. The determination to leave the knowledge score intact was made following analysis indicating that an incremental reduction of elements within the scale would yield a diminishing minute increase in the Cronbach’s alpha statistic estimate. The IPPR scale had two items removed to achieve a

Cronbach’s alpha statistic estimate of .758. Variables were used in the study included the full scale of the Concern for Information Privacy (CFIP), 4 of the 6 items in the Information Personal Protective Response (IPPR), the four subscales for the Concern for Information Privacy (AU= Unauthorized Access; SU=Secondary Use; ME=Medical Errors; CO=Personal Collection of Medical Information), Knowledge of Information Security Systems (KISS) and the Risk Behaviors (RB).

Table 12 Instrument Reliability - Pilot and Current Study

<b>Instrument Reliability - Cronbach's Alpha</b>		
<b>Instrument</b>	<b>Pilot Study</b>	<b>Current Study</b>
CFIP	0.890	0.800
CFIP_AU	0.861	0.810
CFIP_SU	0.883	0.771
CFIP_ME	0.875	0.746
CFIP_CO	0.887	0.883
IPPR	0.704	0.758
RB (Risk)	0.728	0.715
KISS (Knowledge)	0.775	0.669

Reported Threat Appraisal – “Worry” About a Consequence – Ranked Groups

The survey asked respondents to rank in order from 1-4 statements that indicated consequences that they would “worry about” as a result in a security breach. These ranking were used to determine the level of threat by the respondents related to internal harm (threat to themselves) or external harm vis-à-vis harm related to external entities (threats to others). The question was: Which of the following statements reflects your motivation to keep your patient information on the EHR secure? Rank order from lowest (least worry) to highest (most worry) (1 to 4).

Table 13 Threat Appraisal Taxonomy

INTERNAL THREATS	___ I would worry about fines on me or my loss of position. ___ I would worry about my loss of employment.
EXTERNAL THREATS	___ I would worry that my patients' privacy would be exposed. ___ I would worry that my hospital would be fined.

The ranked groups for each of the threats were identified and used in subsequent analyses to test if the group of individuals who ranked a particular threat (internal or external) at a particular similar level (lowest threat group to highest threat group). These can be used to interpret variables associated with those groups who considered “internal threats” highest or lowest and/or “external threats” highest or lowest with each threat serving as an independent variable to test knowledge, risk, concern for information protection and information protective responses.

Table 14 Threat Rankings – Frequency of The Responses

Worry/Threat	Order of Threat (Higher = More Threat)			
	1	2	3	4
<i>Fines on me or loss of position</i>	52	182	164	86
<i>Loss of employment</i>	77	126	162	128
<i>Patient privacy exposed</i>	89	151	135	120
<i>Hospital would be fined</i>	275	30	32	162

Hypothesis Testing: Knowledge, Concern for Information Privacy, Information Privacy Protective Responses, Risk Behaviors, and Threat Appraisal

To test the second part of the sub-question: “How are knowledge, risk, concern and protective responses related and affected by their threat appraisal (internal or external) to themselves, their hospitals, or their patients?” several hypotheses were developed.

The following questions were further specified to use in testing relationships among the variables of interest and differences that might be affected by threat appraisal. These are used to organize the results reported.

Question: Is Knowledge a Predictor of Risk and Concern for Information Privacy Total and Factors?

The following are hypotheses associated with the research question:

1. Hypothesis: An increase in information system security knowledge results in a decrease in identified risk behaviors.
2. Hypothesis: An increase in information system security knowledge results in an increase in Concern for Information Privacy (CFIP).
3. Hypothesis: An increase in information system security knowledge results in an increase in Concern for Medical Facility Errors (ME).
4. Hypothesis: An increase in information system security knowledge results in an increase in Concern for unauthorized access to medical information (UA)?
5. Hypothesis: An increase in information system security knowledge results in an increase in Concern for medical facilities secondary use of medical information (SU)?
6. Hypothesis: An increase in information system security knowledge results in an increase in Concern for personal collection of medical information (CO)?
7. Hypothesis: An increase in information system security knowledge results in an increase in Information Privacy Protective Responses (IPPR).

Knowledge Related To Risk

To test the hypotheses, the data were analyzed statistically using SPSS Version 23. The following table shows the correlation analysis of the Risk Behaviors (RB) and Knowledge of Information System Security (KISS). With an n=514, a Pearson’s Correlation was performed to determine significance at the  $p \leq .05$  level.

Table 15 Risk Behaviors Related To Knowledge

<b>Correlations</b>			
		Knowledge Score	Risk Behaviors Score
Knowledge Score	Pearson Correlation	<b>1</b>	<b>-.110*</b>
	Sig. (2-tailed)		<b>.013</b>
	N	<b>514</b>	<b>514</b>
	<hr/>		
Risk Behaviors Score	Pearson Correlation	<b>-.110*</b>	<b>1</b>
	Sig. (2-tailed)	<b>.013</b>	
	N	<b>514</b>	<b>514</b>
	<hr/>		

\*. Correlation is significant at the 0.05 level (2-tailed).

The correlation between knowledge and risk behaviors among new nurses is statistically significant with a Pearson’s Correlation of  $r = -.110$  ( $p \leq .05$ ). This two-tailed test indicates that knowledge is inversely related to risk. In other words, those with a high level of knowledge related to the information security of mobile devices have a lower risk associated with their mobile device habits.

Knowledge Related To Concern For Information Privacy

The following table shows the correlation analysis of the Concern For Information Privacy (CFIP), Information Privacy Protective Responses (IPPR), and Knowledge of Information System Security (KISS). With an n=514, a Pearson’s Correlation was performed to determine significance at the  $p \leq .05$  level.

Table 16 Knowledge related to CFIP and IPPR

<b>Correlations</b>		
		Knowledge Score
Knowledge Score	Pearson Correlation	<b>1</b>
	Sig. (2-tailed)	
	N	<b>514</b>
Total CFIP	Pearson Correlation	<b>0.037</b>
	Sig. (2-tailed)	<b>0.411</b>
	N	<b>505</b>
Total IPPR	Pearson Correlation	<b>0.072</b>
	Sig. (2-tailed)	<b>0.102</b>
	N	<b>514</b>

\*\* . Correlation is significant at the 0.01 level (2-tailed).

The correlation between knowledge and participants’ CFIP and the IPPR among new nurses are not statistically significant ( $p=NS$ ) with a Pearson’s Correlation of  $r = .037$  ( $p=NS$ ) and  $r = .072$  ( $p=NS$ ) (Table 16). Although the CFIP is correlated with the IPPR ( $r = .414$ ,  $p<.05$ ) (see Table 17), which was expected as the study by Kuo, Ma and Alexander (2014) identified the factors of concern for information privacy (CFIP) converging on participants’ individual personal protective responses (IPPR). These, however, have no connection to knowledge.

These findings indicate a likelihood among new nurses with an increasing rate of CFIP to have an increase in their personal protection responses. However, knowledge is neither

correlated with the CFIP nor the IPPR. The CFIP items are related to the concern for the information privacy of the patient whereas the IPPR relates to the protective responses related to the information privacy of the nurse. Speculatively, these results could infer a correlation in nurses' disposition of information privacy between the patients and themselves regardless of the level of information security knowledge related to mobile devices.

Question: Are Risk Behaviors Related to Concern for Information Privacy Total and Factors?

The following are hypotheses associated with the research question:

1. Hypothesis: An increase in Information Privacy Protective Responses results in a decrease in identified risk behaviors.
2. Hypothesis: An increase in Concern for Information Privacy (CFIP) results in a decrease in identified risk behaviors.
3. Hypothesis: An increase in Concern for Medical Facility Errors (ME) results in a decrease in identified risk behaviors.
4. Hypothesis: An increase in Concern for Unauthorized Access to Medical Information (UA) results in a decrease in identified risk behaviors.
5. Hypothesis: An increase in Concern for Secondary Use of Medical Information (SU) results in a decrease in identified risk behaviors.
6. Hypothesis: An increase in Concern for Personal Collection of Medical Information (CO) results in a decrease in identified risk behaviors.
7. Hypothesis: An increase in Information Privacy Protective Responses (IPPR) results in a decrease in identified risk behaviors.

The Risk Behaviors related CFIP and IPPR table shows the correlation analysis of the Concern For Information Privacy (CFIP), Information Privacy Protective Responses (IPPR), and Risk Behaviors (RB). With an N=514, a Pearson's Correlation was performed to determine significance at the  $p \leq .05$  level.

Table 17 Risk Behaviors related to CFIP and IPPR

		<b>Correlations</b>		
		Total Risk Behaviors	Total CFIP	Total IPPR
Risk Behaviors	Pearson Correlation	<b>1</b>	<b>.132**</b>	<b>.116**</b>
	Sig. (2-tailed)		<b>.003</b>	<b>.008</b>
	N	<b>514</b>	<b>505</b>	<b>514</b>
Total CFIP	Pearson Correlation	<b>.132**</b>	<b>1</b>	<b>.412**</b>
	Sig. (2-tailed)	<b>.003</b>		<b>.000</b>
	N	<b>505</b>	<b>505</b>	<b>505</b>
Total IPPR	Pearson Correlation	<b>.116**</b>	<b>.412**</b>	<b>1</b>
	Sig. (2-tailed)	<b>.008</b>	<b>.000</b>	
	N	<b>514</b>	<b>505</b>	<b>514</b>

\*\* . Correlation is significant at the 0.01 level (2-tailed).

The correlation between risk behaviors, CFIP, and IPPR among new nurses is statistically significant. Risk behaviors shows a positive correlation with CFIP and IPPR with Pearson's Correlation values of  $r = .132$  and  $r = .116$  respectively at the  $p \leq .01$  level. With a Pearson's Correlation of  $r = .412$  at the  $p \leq .01$  level, CFIP and IPPR are more strongly related to one another than risk is related to either, however, this was expected as the study by Kuo, Ma and Alexander (2014) identified the factors of concern for information privacy (CFIP) converging on participants' individual personal protective responses (IPPR). This two-tailed test indicates that in this modified version of the questionnaire of the nurses' responses about concern for information privacy and information privacy protective responses are directly related to one another with a stronger correlation than that of risk behaviors. Although informative, this was not the hypothesis to be tested, and in fact, significant in the opposite direction. This suggests that it may be associated with how the risk behaviors interact with the concerns for privacy and protective responses, which were hypothesized to be inversely correlated with risk.



The hypotheses suggesting a relationship between CFIP, IPPR and risk behaviors were predicted to be inversely correlated. The findings demonstrated an increase in risk behaviors is associated with increases in the CFIP and IPPR. Therefore, new nurses tend to have increased concern for their patients' information privacy and their own protective responses as their own level of risk behaviors increase. This was not expected and runs counterintuitive to industry notions, with a prediction that one's concern would decrease one's risk behaviors. What might be evident is that participants' risk behaviors make them more suspicious of information protection privacy and more likely to select stronger protective responses – thus, yielding an inverse relationship – and suggesting that risk influences concern and protective responses, rather than concern and protective responses influences risk. With only a correlation analysis, this logic cannot be tested, and the model proposed may need to be modified.

Question: Is Threat Appraisal Associated with Knowledge, Risk, Concern for Information Privacy Total and Factors, and Personal Protective Responses?

To compare the knowledge, risk, concern and protective response mean scores by threat appraisal groups, two general null hypotheses were developed:

Internal Null Hypotheses: Internal threats are not associated with knowledge, risk, concerns or protective responses.

External Null Hypotheses: External threats are not associated with knowledge, risk, concerns or protective responses.

### Threat – Internal and External

The survey instrument contained four statements, two developed to reflect “internal” threats (i.e. threat to self, such as fine, loss of position or job) and “external” threats (i.e. threat to others such as hospital fines, patient privacy breached). Participants were asked to rank order them from “lowest threat/worry” to “highest threat/worry” that yielded four groups of threat assessments for each threat. These threat groups were used to test for differences in mean scores on the variables of interest including knowledge, risk, concern and protective responses.

The results yielded four groups indicating from least to most worrisome that a breach event could cause an impact to the nurse (internal) such as a personal threat (job, position) or that a breach event could cause an impact to others (external) vis-à-vis an impact to either the patient or hospital (external).

### Threat of Nurse Fine

The following table shows the mean score comparisons for knowledge, risk behaviors, CFIP, and IPPR by the threat ranks on the threat of fines (internal threat). With an n=514, an Analysis of Variance (ANOVA) was performed.

Table 18 Threat of fine ranks on differences in knowledge, risk behaviors, IPPR, and CFIP

		ANOVA				
		Sum of				
		Squares	df	Mean Square	F	Sig.
Knowledge Score	Between Groups	.124	3	.041	3.721	.011
	Within Groups	5.337	480	.011		
	Total	5.461	483			
Risk Behaviors	Between Groups	351.794	3	117.265	1.366	.252
	Within Groups	41195.386	480	85.824		
	Total	41547.180	483			
Total IPPR	Between Groups	35.687	3	11.896	1.288	.278
	Within Groups	4433.575	480	9.237		
	Total	4469.262	483			
Total CFIP	Between Groups	155.819	3	51.940	1.110	.344
	Within Groups	22124.294	473	46.774		
	Total	22280.113	476			

The ANOVA indicates a statistically significant difference for knowledge scores by the threat groups for fines (internal threat) between knowledge and the worry about fines among new nurses ( $F = 3.72$ ,  $df=3,480$ ,  $p<.05$ ). No other significant differences exist with the threat levels of fines and risk behaviors, IPPR, and CFIP.

Table 19 Threat of fine level related to knowledge scores

Knowledge Score			
Fines on me or loss of position	Mean	N	Std. Deviation
1	.82	52	.087
2	.85	182	.099
3	.83	164	.106
4	.81	86	.125
Total	.83	484	.106

An analysis of knowledge mean score by highest threat ranking indicates that with a mean score of .81, those indicating the highest threat of fine have the lowest knowledge score.

**Threat of Job Loss**

The following table shows the mean score comparisons for knowledge, risk behaviors, CFIP, and IPPR by the threat ranks on the threat of job loss (internal threat). With an n=514, an ANOVA was performed.

Table 20 Threat of job loss ranks on differences in knowledge, risk behaviors, IPPR, and CFIP

		<b>ANOVA</b>				
		Sum of				
		Squares	df	Mean Square	F	Sig.
Knowledge Score	Between Groups	<b>.016</b>	<b>3</b>	<b>.005</b>	<b>.499</b>	<b>.683</b>
	Within Groups	<b>5.340</b>	<b>489</b>	<b>.011</b>		
	Total	<b>5.356</b>	<b>492</b>			
Risk Score	Between Groups	<b>222.435</b>	<b>3</b>	<b>74.145</b>	<b>1.011</b>	<b>.387</b>
	Within Groups	<b>35855.362</b>	<b>489</b>	<b>73.324</b>		
	Total	<b>36077.797</b>	<b>492</b>			
Total IPPR	Between Groups	<b>1.125</b>	<b>3</b>	<b>.375</b>	<b>.041</b>	<b>.989</b>
	Within Groups	<b>4464.124</b>	<b>489</b>	<b>9.129</b>		
	Total	<b>4465.249</b>	<b>492</b>			
Total CFIP (AU/SU/ERCO)	Between Groups	<b>65.306</b>	<b>3</b>	<b>21.769</b>	<b>.470</b>	<b>.703</b>
	Within Groups	<b>22330.786</b>	<b>482</b>	<b>46.329</b>		
	Total	<b>22396.093</b>	<b>485</b>			

The ANOVA indicates that there are no differences among mean scores for knowledge, risk behaviors, CFIP and IPPR with the threat ranking of threat of job loss (internal).

Threat To Patient Privacy

The Threat to patient privacy table shows the mean score comparisons for knowledge, risk behaviors, CFIP, and IPPR by the threat ranks on the threat of patient privacy breaches (external threat). With an n=514, an ANOVA was performed.

Table 21 Threat to patient privacy related to knowledge, risk behaviors, IPPR, and CFIP

		<b>ANOVA</b>				
		Sum of Squares	df	Mean Square	F	Sig.
Knowledge Score	Between Groups	<b>.079</b>	<b>3</b>	<b>.026</b>	<b>2.443</b>	<b>.063</b>
	Within Groups	<b>5.311</b>	<b>491</b>	<b>.011</b>		
	Total	<b>5.390</b>	<b>494</b>			
Risk Score	Between Groups	<b>46.863</b>	<b>3</b>	<b>15.621</b>	<b>.210</b>	<b>.890</b>
	Within Groups	<b>36601.128</b>	<b>491</b>	<b>74.544</b>		
	Total	<b>36647.992</b>	<b>494</b>			
Total IPPR	Between Groups	<b>32.808</b>	<b>3</b>	<b>10.936</b>	<b>1.255</b>	<b>.289</b>
	Within Groups	<b>4279.374</b>	<b>491</b>	<b>8.716</b>		
	Total	<b>4312.182</b>	<b>494</b>			
Total CFIP (AU/SU/ERCO)	Between Groups	<b>98.849</b>	<b>3</b>	<b>32.950</b>	<b>.725</b>	<b>.537</b>
	Within Groups	<b>21984.624</b>	<b>484</b>	<b>45.423</b>		
	Total	<b>22083.473</b>	<b>487</b>			

The ANOVA indicates that there are no differences among mean scores for knowledge, risk behaviors, CFIP and IPPR with the threat ranking of patient privacy (external threat) in new nurses. It is important to note, however, that with the knowledge mean score comparisons suggesting potential differences by threat ranking (F = 3.443, df=3,491, p=.063), it would be prudent to follow up on this variable in future studies.

Threat of Hospital Fine

The following table shows the mean score comparisons for knowledge, risk behaviors, CFIP, and IPPR by the threat ranks on the threat of hospital fines (external threat). With an n=514, an ANOVA was performed.

Table 22 Threat of hospital fine related to knowledge, risk behaviors, IPPR, and CFIP

		<b>ANOVA</b>				
		Sum of				
		Squares	df	Mean Square	F	Sig.
Knowledge Score	Between Groups	<b>.008</b>	<b>3</b>	<b>.003</b>	<b>.230</b>	<b>.876</b>
	Within Groups	<b>5.447</b>	<b>495</b>	<b>.011</b>		
	Total	<b>5.455</b>	<b>498</b>			
Total Habit	Between Groups	<b>224.496</b>	<b>3</b>	<b>74.832</b>	<b>1.005</b>	<b>.390</b>
	Within Groups	<b>36873.071</b>	<b>495</b>	<b>74.491</b>		
	Total	<b>37097.567</b>	<b>498</b>			
Total IPPR	Between Groups	<b>13.488</b>	<b>3</b>	<b>4.496</b>	<b>.500</b>	<b>.683</b>
	Within Groups	<b>4452.769</b>	<b>495</b>	<b>8.995</b>		
	Total	<b>4466.257</b>	<b>498</b>			
Total CFIP	Between Groups	<b>89.059</b>	<b>3</b>	<b>29.686</b>	<b>.648</b>	<b>.584</b>
	Within Groups	<b>22348.866</b>	<b>488</b>	<b>45.797</b>		
	Total	<b>22437.925</b>	<b>491</b>			

The ANOVA indicates no significant differences among mean scores for knowledge, risk behaviors, CFIP and IPPR with the threat ranking of patient privacy threat in new nurses.

In summary, the hypotheses related to the main variables of interest, knowledge, risk, concern for privacy, personal protective responses and threat appraisal yielded some statistically significant findings. Of note is that knowledge and risk are correlated in the direction predicted: as knowledge of participants increased, risk behaviors decreased. While knowledge and risk were significantly related, knowledge was not related to concern for information privacy or

personal protective responses. Risk, however, was related to concern for information privacy and personal protective responses but not in the direction predicted. What is suggested by the results is that new nurses' risk behaviors influence their concern and protective responses directly – that perhaps those who take more risks are more concerned and are likely to engage in more personal protective responses. Finally, ranked groups of the internal threat appraisal for fines or loss of position did appear to affect participants' knowledge, but not risk behaviors, concern or personal protective responses. The highest threat ranking for personal fine (internal) was associated with the lowest knowledge score. The null hypotheses were not rejected for any other threat appraisal ranking differences in mean scores for the variables of interest: knowledge, risk, concern or personal protective responses.

#### Hypothesis Testing: Demographic Variables

Is knowledge, risk, concern or protective responses influenced by select demographic characteristics such as gender, age and education (program type or school type)?

#### Differences in Knowledge, Risk, and Concern for Information Privacy and Protective Responses

The following sections will present the results testing the hypotheses generated around these questions. They will include variables about the nurses (i.e. gender, age, school type) as they may or may not influence the variables in the study including:

- (1) Do men and women differ in their knowledge and risk behaviors related to cybersecurity?
- (2) Do men and women differ in their reported mobile device practices?
- (3) Does the age of nurses differ on their scores for knowledge, risk behaviors, threat appraisal, or concern for information protection?

(4) Does nursing education type or school type affect knowledge, risk behaviors, threat appraisal, or concern for information protection?

Gender Related to Knowledge, Risk Behaviors and Reported Mobile Device Practice

To test the hypotheses that the study variables of knowledge, risk, concern or protective responses and mobile device practices differ by gender, a t test was performed on study variables with no significant differences ( $p=NS$ ) for KISS, RS, CFIP or IPPR, and no significant correlations for frequency of mobile device use for any study items ( $p=NS$ ).

Age Related To Knowledge, Risk Behaviors

To test the hypotheses if age and study variables are associated, the age of participants was collapsed into three categories to correct for multiple age ranges selected by participants. These became three age ranges: Younger Age Range (ages <30); Middle age range (ages 30 to 45); Older age range (ages >45).

The following table shows the correlation analysis of age range, knowledge of information security systems (KISS), and Risk Behaviors (RB), concern (CFIP) and personal protective responses (IPPR). With an  $n=514$ , a Pearson's Correlation was performed to determine significance at both the  $p \leq .01$  and  $p \leq .05$  levels.



Table 23 Age related to knowledge, risk, concern and personal protective responses

		Age Range
Age Range	Pearson Correlation	<b>1</b>
	Sig. (2-tailed)	
	N	<b>514</b>
Knowledge Score	Pearson Correlation	<b>.124**</b>
	Sig. (2-tailed)	<b>.005</b>
	N	<b>514</b>
Total Risk	Pearson Correlation	<b>-.078</b>
	Sig. (2-tailed)	<b>.079</b>
	N	<b>514</b>
CFIP	Pearson Correlation	<b>-.023</b>
	Sig. (2-tailed)	<b>.601</b>
	N	<b>505</b>
IPPR	Pearson Correlation	<b>-.099*</b>
	Sig. (2-tailed)	<b>.025</b>
	N	<b>512</b>

\*\* . Correlation is significant at the 0.01 level (2-tailed).

\* . Correlation is significant at the 0.05 level (2-tailed).

The correlations between age range and knowledge as well as age range with personal protective response are significant, but age is not significant for risk (RB) or age for concern (CFIP). Age range shows a positive correlation for knowledge (KISS) with a Pearson's Correlation value of .124 significant at the  $p \leq .01$  level and a negative value of -.099 for personal protective responses (IPPR) significant at the  $p < .05$  level. These results indicate that older nurses have high level of knowledge of information system security and are less "protective" in their responses to using information technology. Neither risk nor concern are related.

### Age Related To Time Spent Using Mobile Device

The following table shows the correlation analysis of age range and time spent using a mobile device. With an n=514, a Pearson's Correlation was performed to determine significance at the  $p \leq .01$  level.

Table 24 Age related to time spent using mobile device

<b>Correlations</b>			
		<b>Age Range</b>	<b>Time Spent</b>
Age Range	Pearson Correlation	<b>1</b>	<b>-.121**</b>
	Sig. (2-tailed)		<b>.006</b>
	N	<b>514</b>	<b>513</b>

\*\* Correlation is significant at the 0.01 level (2-tailed).

Correlations between age range and time spent using a mobile device among new nurses has been determined to be significant. Age range shows a negative correlation with mobile device usage with Pearson's Correlation value of  $r = -.121$  ( $p \leq .01$ ). This two-tailed test indicates that the younger age range tends to spend more time using mobile devices.

### Age Related To Activity Type

The following table shows the correlation analysis of age range and types of mobile device activities. With an n=514, a Pearson's Correlation was performed to determine significance at both the  $p \leq .01$  and  $p \leq .05$  levels.

Table 25 Age activity for significant correlations

<b>Correlations</b>		Web	IM	Text	MMS	Camera	Notes	Navigation	Social Media	Music
Age Range	Pearson Correlation	<b>-.149**</b>	<b>-.106*</b>	<b>-.131**</b>	<b>-.119**</b>	<b>-.116**</b>	<b>-.095*</b>	<b>-.103*</b>	<b>-.202**</b>	<b>-.147**</b>
	Sig. (2-tailed)	<b>.001</b>	<b>.017</b>	<b>.003</b>	<b>.007</b>	<b>.009</b>	<b>.031</b>	<b>.020</b>	<b>.000</b>	<b>.001</b>
	N	<b>513</b>	<b>511</b>	<b>514</b>	<b>512</b>	<b>514</b>	<b>513</b>	<b>512</b>	<b>514</b>	<b>514</b>

\*\* . Correlation is significant at the 0.01 level (2-tailed).

\* . Correlation is significant at the 0.05 level (2-tailed).

Table 26 Age activity for non-significant correlations

		Talking	Email	Calendar	Contact List	Video/Movies	Online Library
Age Range	Pearson Correlation	.019	-.032	-.029	.071	-.029	-.013
	Sig. (2-tailed)	.673	.473	.510	.105	.513	.768
	N	514	511	514	514	513	513

All significantly correlated activities are inversely related to age. Therefore, the younger age group of new nurses have more mobile device activity related the use of web browsing, instant messaging (IM), multimedia messaging (MMS), camera, notes, navigation, social media, and music. Social media has the strongest negative Pearson’s Correlation value at **-.202**. Those activities not significantly correlated to age include talking by voice, email, calendar, contact list, video/movies, and the online library.

#### Education Related To Knowledge, Risk Behaviors, CFIP, and IPPR

Since the results of the study will be important to inform nursing education practice in was important to test for differences among types of nursing programs and to test for differences in types of schools (public, private not-for-profit, private for-profit).

To test the hypotheses that knowledge, risk, concern or protective responses differ by types of programs (i.e. Associate Degree, Diploma, Baccalaureate Degree, Masters, etc. Other) an analysis of variance was done to compare mean scores for the education groups.

The following table shows the results of education differences in knowledge, risk behaviors, CFIP, and IPPR. With an n=514, an ANOVA was performed.

Table 27 Education type effects on knowledge, risk behaviors, IPPR, and CFIP

		<b>ANOVA</b>				
		Sum of		Mean Square	F	Sig.
		Squares	df			
Knowledge Score	Between Groups	<b>.098</b>	<b>8</b>	<b>.012</b>	<b>1.084</b>	<b>.373</b>
	Within Groups	<b>5.714</b>	<b>503</b>	<b>.011</b>		
	Total	<b>5.812</b>	<b>511</b>			
Risk Behaviors	Between Groups	<b>883.638</b>	<b>8</b>	<b>110.455</b>	<b>1.266</b>	<b>.259</b>
	Within Groups	<b>43880.362</b>	<b>503</b>	<b>87.237</b>		
	Total	<b>44764.000</b>	<b>511</b>			
Total IPPR	Between Groups	<b>113.408</b>	<b>8</b>	<b>14.176</b>	<b>1.600</b>	<b>.122</b>
	Within Groups	<b>4457.199</b>	<b>503</b>	<b>8.861</b>		
	Total	<b>4570.607</b>	<b>511</b>			
Total CFIP	Between Groups	<b>551.916</b>	<b>8</b>	<b>68.990</b>	<b>1.475</b>	<b>.164</b>
	Within Groups	<b>23106.231</b>	<b>494</b>	<b>46.774</b>		
	Total	<b>23658.147</b>	<b>502</b>			

The ANOVA analysis indicates that that no significant difference exists in new nurses in their knowledge, risk behaviors, IPPR, or CFIP related to their type of education program.

Students enrolled in Associates, Baccalaureate and Master’s degree programs did not differ on these variables related to security and privacy using mobile devices.

To test if the types of schools (public, private not-for-profit, private for-profit) has an effect on the knowledge, risk, concern and protective responses of new nurses, analysis of

variance of the mean scores were calculated. The following table shows the results of the ANOVA on school type comparisons of knowledge, risk behaviors, CFIP, and IPPR.

Table 28 School type effects on knowledge, risk behaviors, IPPR, and CFIP

		<b>ANOVA</b>				
		Sum of		Mean Square	F	Sig.
		Squares	df			
Knowledge Score	Between Groups	<b>.043</b>	<b>3</b>	<b>.014</b>	<b>1.267</b>	<b>.285</b>
	Within Groups	<b>5.794</b>	<b>510</b>	<b>.011</b>		
	Total	<b>5.838</b>	<b>513</b>			
Total Risk	Between Groups	<b>139.946</b>	<b>3</b>	<b>46.649</b>	<b>.532</b>	<b>.660</b>
	Within Groups	<b>44685.969</b>	<b>510</b>	<b>87.620</b>		
	Total	<b>44825.914</b>	<b>513</b>			
Total IPPR	Between Groups	<b>9.533</b>	<b>3</b>	<b>3.178</b>	<b>.354</b>	<b>.786</b>
	Within Groups	<b>4580.803</b>	<b>510</b>	<b>8.982</b>		
	Total	<b>4590.337</b>	<b>513</b>			
Total CFIP	Between Groups	<b>184.431</b>	<b>3</b>	<b>61.477</b>	<b>1.308</b>	<b>.271</b>
	Within Groups	<b>23543.925</b>	<b>501</b>	<b>46.994</b>		
	Total	<b>23728.356</b>	<b>504</b>			

The ANOVA analysis indicates that that no significant difference exists in new nurses in their knowledge, risk behaviors, IPPR, or CFIP related to their type of schools, public, private not for-profit and private for-profit.

### Conclusion

In summary, the hypotheses related to demographics yielded some statistically significant findings. Of note is that gender made no difference on any of the study variables of knowledge, risk, concern or personal protective responses. Age had a significant influence on types of mobile device activities as well as participants' knowledge but not risk behaviors. Age was also inversely related to personal protective responses, suggesting that older nurses were less likely to

use personal protection responses. Types of nursing programs and types of schools did not affect any of the study variables. These findings suggest important considerations when addressing overall findings of the study as they relate to recommendations for practice.

In summary, the following conclusions can be made from the analyses in the study:

1. Based upon the aforementioned results, the following variables are related:

- Knowledge and risk are inversely related.
- CFIP is directly related to IPPR.
- Risk behavior is directly related to both the CFIP and IPPR.
- Age is inversely related to time spent using mobile devices.
- Age is inverse related to the following mobile activities: Web, IM, Text, MMS, Camera, Notes, Navigation, Social Media, and Music.
- Age is directly related to knowledge.
- Age is inversely related to IPPR.
- Threat of nurse fine (internal) and knowledge are related.

2. Based upon the aforementioned results, the following variables are not related:

- Knowledge is related neither to CFIP nor to IPPR.
- Threat of nurse fine (internal) is not related to risk behaviors (RB), CFIP, or IPPR.
- Threat of job loss (internal) not related to core variables.
- Threat to patient privacy (external) not related to core variables (however knowledge  $p=.06$  and suggests further exploration that may be warranted)
- Threat of hospital fine (external) not related to core variables.

3. Based upon the aforementioned results, the following demographic variables are not related:

- Gender is not related to any core variables.
- Age is not related to CFIP.
- Age is not related to risk behavior.
- Age is not related to the following mobile activities: Talking, Email, Calendar, Contact List, Video/Movies, and Online Library.
- Type of education is not related to any core variables.
- Type of school is not related to any core variables.

## Chapter 5: Discussion

### Introduction

This chapter presents an organized discussion on the study findings, implications, measurement instruments, and limitations. The overall intent of this study was to explore the information security knowledge, risk behavior in the use of portable electronic devices, the concern for and protective response related to protecting patient information, and the threat appraisal of consequences for security breaches in a sample of new nurses from across the nation who had graduated approximately one year prior, thereby sharing a common length of time in the role of nurse and similar nursing education completion dates. The sample also shared in their membership of the National Student Nurses Association (NSNA) and its associated nursing student educational programs and assistance. With respect to experience, this sample of nurses was homogenous in order to be able to inform educators, both within the educational institution and the workplace, as to factors examined herein this study. These recommendations are also discussed, along with the limitations of the study and suggestions for future research.

### Characteristics and Demographics

The survey elements related to demographics consisted of the standard used in prior NSNA surveys. As the NSNA administered the delivery of the instrument to its members who agreed to correspondence for survey purposes, consistency with their standard demographic elements was a requirement. This requirement is the basis for the manner in which the demographic elements as drafted instead of other standards, including those stock elements from SurveyMonkey® itself.

Gender data collected for analysis was determined to be congruent with the gender demographic makeup of the overall population of nurses in the United States. A 92% female to

8% male composition accounts for the gender of nurses in the United States (United States Department of Labor, 2015). These gender related statistics did not contain granular information as to experience, age, or other demographic information collected in this study. Therefore, these national statistics may be considered generally harmonious and consistent with the study sample which had an 87.9% female to 12.1% male composition with a sample population of N=541. This gender makeup, although slightly higher for male responders perhaps based on a higher likelihood to answer a computer-related survey, also does align with membership of the NSNA among its reported 60,000 members from across the nation.

The gender demographic was analyzed against all of the core variables; KISS, CFIP, IPPR, RB, and Threat Appraisal. Of note is that no significant relation has been found between gender and any of the core variables. This should inform educators, both in nursing education and in the workplace, of the homogenous nature of nurses respective to gender related to both knowledge and risk behavior associated with mobile devices.

Consistent with NSNA survey elements, race was one of the collected data elements. The majority of respondents at 73.3% reported themselves as Caucasian. With low representation among certain categories such a Native Hawaiian or other Pacific Islander having a single representative, analysis with respect to race would not likely be informative. The descriptive data are reported for information but not tested in the core analyses.

The data related to age included an expansive range with some groups too small for separating out. After collection, the NSNA-defined age categories were collapsed into the three sections of those aged 32 and younger, 33 to 48, as well as 49 and older. The rationale for selecting three groups was to explore general inferences about age related to the other core variables. The specific values were selected based upon the age range standards for NSNA-



administered surveys. Specific age values were not collected, only ranges that were collapsed into three general categories for analysis.

As anticipated with new nurses, the majority (71%) fell into 32 and younger section whereas a small section (7%) fell into the 49 and older category. As only age ranges were collected in lieu of actual ages, the ability to determine cutoff points for age ranges was limited to those range numbers already in use. Hence, the values  $\leq 32$  (younger nurses), 33-48 (mid-age nurses), and  $\geq 49$  (older nurses) were designated as the age groups consolidated for analysis and not suggesting their experience since they were all one-year post graduation.

By separating the respondents into three age groups, this survey has been able to demonstrate associations with age range and the other factors. Among the most prominent of findings was the positive association with age and knowledge of information security related to mobile devices. Counter to the narrative that younger populations have a propensity toward technology as digital natives, the security knowledge was found to increase with those in the older age range. Congruent with the digital native narrative associated with younger populations, this study did find that the inverse association between age range and the use of mobile electronic devices. Not only did the younger group tend to use their devices more often, but also the duration of different types of activities or mobile device features varied among the age groups. Mobile device features such as web, instant/text/multimedia messaging, camera, notes, navigation, social media, and music tended to be used with a longer duration among the younger age group.

The younger group of those aged 32 and younger accounted for just over double those in the other age groups combined. With only 7% of the sample at age 49 and older, the survey was most represented by the younger nurses. A plausible explanation for the age makeup of the

sample is that an effort to limit variation in experience was done by surveying NSNA members who had graduated from a nursing program roughly one year prior. Moreover, as the sample consisted of mainly nurses who did not graduate with an advanced degree but rather those associated with degrees required for the entry into the profession of nursing, the expectation is that survey respondents overall had recently commenced entry into their nursing careers. Overall, 91.4% of the sample had education types typically associated with entry into the profession of nursing.

Age also had an inverse relationship with the respondents' information privacy protection response (IPPR) but not their concern for information privacy (CFIP). Those in the higher age groups tended to show a response to the end of protecting their own data. However, there was no difference in age regarding the concern for information privacy of their own patients.

While the sample was generally homogenous with respect to having had an education type consistent with the entry into the profession, no relation was found between the type of education and any of the core variables study. Furthermore, the type of school (public, private, for-profit) did not yield any results as to its relationship with any of the core variables either. Therefore, neither education type nor school type had any impact on knowledge or risk.

As one of this study's intentions is to inform educators, this finding should be particularly noteworthy considering the current zeitgeist in which the baccalaureate degree has been sought after as the minimum entry point into the profession by multiple groups and in some cases encouraged through market forces in certain regions within the United States. The Institute of Medicine (IOM) has recommended an increase to an 80% composition of nurses at the baccalaureate level by the year 2020 (Yakusheva, 2014). Furthermore, higher baccalaureate-level proportions are associated with better outcomes according to hospital studies (Yakusheva,

2014). While improved outcomes have been appraised in the clinical setting, knowledge of information security or risk behavior does not supply any additional evidence in support of raising the entry level into the profession, as those factors are not related to education type.

The 71% majority of respondents had nursing education at the baccalaureate or higher level with 27.6% having reported a nursing education from an Associate Degree or diploma program. This nursing education type is consistent with NSNA survey data. As the survey question inquired at the type of nursing program degree, a determination cannot be presumed as to the highest level of education obtained. For example, a person with a master's degree may have pursued a nursing career by way of an Associate Degree and thus would have been constrained to report that lower level degree on the survey.

#### Phone Characteristics

To texture a survey regarding new nurses' mobile device usage, information pertaining to their particular mobile device of use was collected with respect to phone manufacturer, model, and operating system by derivation if such a determination could be extrapolated. While these data elements were not analyzed in relation to the core variable, this information could be used for future research or informative unto itself as indicative of the current landscape of mobile device usages among new nurses. Due to a plethora of phone manufacturers and continuously emerging models, the decision was made to leave this survey element as a free text field. In retrospect, data analysis on such a field was arduous due to variations in spelling and imprecise responses. For any future research capturing such data, a single-select option with the most pervasive operating systems of the time along with an "other" selection could yield cleaner data from which to analyze.

The information collected pertained to the “personal use of technologies at work and at home.” As such, the distinction could not be made as to which devices were employer-supplied or intended for personal use. As stated in Chapter 4, clinical nurse usage of phones for clinical usage is limited and often for the voice communication. While the collected data cannot be definitively attributed to personal phone usage, a general inference may be based upon commonplace mobile device usage for work purposes among nurses in a clinical setting.

While the emergence of bring-your-own-device (BYOD) modalities are becoming more pervasive in healthcare, this technology is often limited to non-clinical staff for business purposes. Current trends indicate an increased prevalence of mobile devices in the healthcare workplace without the adoption of adequate security standards (Hewitt, Dolezel, & McLeod, 2017). Therefore, the burden in part is placed upon healthcare entities and nurses in particular to protect sensitive information thus making the understanding of their information security knowledge, risk behavior, and other factors are the more relevant with this emerging paradigm.

The overwhelming majority of the world’s phone market consists of Android phones at 86.1%. Android-operated phones using Google’s Android operating system and include a plethora of manufacturers and models with variations in terms of functionality and security features. This diverse Android marketplace at times may see the need for configuration requirements on the phones themselves in order to bring these devices in alignment with employers’ mobile device management systems (MDM) compared to Apple models with inherent security safeguards. An MDS provides security assurances and configuration control. As this Android marketplace is diverse, such configurations are not universally applicable as different models have different security feature implementations.

Relatively inverse to worldwide prevalence, the 70.73% majority of new nurses tend to use Apple phones, which have the iOS operating system. The new nurse usage is a departure from the general population. This finding should be encouraging from an information security perspective as such devices come from a single manufacturer with limited model offerings, and therefore has a somewhat predictable security posture. Both the hardware and software come from a single manufacturer with limited supported devices and a single operating system line. These devices tend to require less configuration to align with the employer-based MDM. While using an employer-based MDM is not commonplace as is the introduction of personal phones into the nurses' clinical practice, it nonetheless serves as a marker for the security standards employed by the iOS devices.

Samsung had a 21.64% usage in the study and remains the largest of Android-based manufacturers in both the study and the world. Microsoft's Windows phone has a single report and may have been an outlier as worldwide usage of these models is quite sparse.

### Descriptive Findings of the Study

This section will address the overarching main question of the study, "How much do new nurses know about security of information systems and does their knowledge influence their risk behaviors in using mobile technology?" In doing so, common mobile technology usage is described with data related to mobile application and security usage analyzed using descriptive statistical analysis. This information was included in the study to provide background information on new nurses' usage in the context of the major variables examined herein this study.

## Mobile Application Use

A series of descriptive analyses were performed in an effort to answer the question “What is the reported level and type of new nurse mobile application use?” The prevailing features were Text Messaging (N=272), Social Media (N=250), and Web Browsing (N=234).

The 88.5% majority of respondents used social media either sometimes or very often. The type of social media platform was not asked. At the time of this analysis, the predominant social media platform is Facebook with 2.2 billion active users (Statista, 2018). This survey was conducted prior to the privacy disclosure involving the purported misuse of user-related data by Cambridge Analytica (Granville, 2018). There may be opportunities for future research to be conducted on nurses’ social media usage in light of this privacy issue taking on the massive media and political attention it has caused related to personal privacy.

Not surprisingly, chatting, online library, and video/movie usage was low. It should be noted that chatting might be considered uncommon vernacular supplanted by the term texting. This could perhaps account for the low level of reported usage. The online library usage may have been more apt to a student sample as the studied group consisted of nurses who had already graduated. These new nurses may use online medical references but speculatively may not have equated that usage with the term “online library” which may be more associated with school use. With fourteen participants declaring that the online library was not available, those respondents may have speculatively referred to the feature as not being available as a native application in the manner that camera, text, mail, and contact apps are commonly included as default operating system features.

## Security Practice Results

The survey had an element related to a common security practice, which is the locking of a device. The purpose of locking a device is to prevent unauthorized access to the device. Locking may occur automatically by the device at a pre-set interval without any use activity or through manual intervention often manifesting itself with the click of a button. The locking of a device would require re-authentication to the device by the authorized user. At the time of this survey, standard authentication methods may consist of a numerical passcode, username-password combination, fingerprint scan, pattern drawing or facial recognition.

Instead of a binary response selection, the question was asked in a matrix format about the frequency to which this locking practice occurred with phones and tablets both personally owned and employer-supplied. The distinction of frequency is informative and may be indicative of a propensity to protect information. Opportunities may exist for future studies regarding such a propensity relating other security practices to the key variables in this study.

A majority listed hospital phones and mobile devices as not applicable regarding locking at 56.0% and 58.2% respectively. As previously discussed, the supposition is that nurses do not commonly use their mobile phones for clinical practice. The MDM solutions typically include those mandatory locking features in addition to likely requiring more secure authentication methods than the device's native minimum requirements. This could include a requirement for a complex numerical passcode of six digits as opposed to a simpler one of four digits or even no authentication required at all. With the emergence of the MDM solution, this security practice may be automatically performed. Perhaps a plausible explanation for the reported lack of availability might be the absence of required nurse intervention to perform this security function.

Regarding personal phones and mobile devices, the “always” response prevailed. This indicates that new nurses recognize the existence of the security feature and actively use it. New nurses lock their personal phones and devices at 83.5% and 70.5% respectively for often and always indicated as a practice. Nurses are aware of and take action to safeguard their own devices from unauthorized physical access. While this process may be automated in the workplace for those employers who have implemented an MDM solution and configured it for this feature, educators and employers should know that nurses typically safeguard data habitually at least in respect to unauthorized physical access based upon the finding that 83.5% of new nurses reported locking their phones often or always.

### Level of Knowledge

The survey instrument included the knowledge of information security (KISS) measure, developed by the principal investigator, and administered as a pilot to a convenience sample of nursing students (N=167) prior to the full study implementation.

A predicted finding, and comforting result albeit a weak correlation, is that knowledge is inversely related to risk. Those with greater knowledge of information system security have a reduced predilection toward risk behavior in their use of mobile devices, as those with higher knowledge scores tend to have a safer posture. The new nurses with information security knowledge may understand risks and therefore participate in fewer risk activities. This finding could be informative and possibly lead to future research in behavior analysis. This should also inform educators and employers that knowledge may be a mitigating factor in reducing risk behavior. This finding supports healthcare employer practices of HHS-mandated security awareness training, which tends to focus on knowledge. Perhaps behavior-based practices may be more suitable for risk behavior reduction as a supplement to knowledge. There is an



opportunity for future studies in order to understand the relationship between risk behavior and knowledge in light of this finding.

For the most part, the knowledge portion of the survey had the majority responding correctly and the histogram showed a normal distribution and grade score consistent with that of a college education program. However, there were a few outliers of interest.

Most notable is that only 27.4% of the sample responded correctly to item 15 in the KISS instrument. The question refers to a nefarious attempt to by a third party to acquire a person's credentials through a cleverly designed email. This type of email correspondence, commonly known as a "phishing" attack, is a social engineering technique with the intended purpose to trick the recipient. Phishing is a type of social engineering attack, which may target healthcare, a specific institution, a specific person, or may simply be delivered to a nurse incidentally as part of a larger campaign to steal credentials. The broader subject of social engineering is discussed in chapter two.

With this item being the lowest score, perhaps the result could inform educators and employers of an identified gap to pursue. Credentials may be stolen for not only direct access to patient and financial information but may also be used to control computer systems. At the time of this analysis, many phishing emails contain or compel the user to obtain malicious code that could cause severe disruption in computer systems such as Ransomware (Palmer, 2017). Ransomware is essentially malicious software or a virus, which scrambles one or more computer systems rendering them unusable until an untraceable financial ransom is provided to the perpetrator. The impact of such an attack has been proven to affect the clinical functioning of a healthcare entity for extended periods as clinical systems moreover are digitally connected.

Therefore, understanding this knowledge question may have not only privacy implications but clinical ones as well.

Several questions were related to the proper disclosure of PHI for which legal guidance has been outlined. In 2013, HHS provided direction for permissible cases of PHI disclosure (45 CFR parts 160 and 164). The KISS item 4 refers to permission to view a relative's chart. The ability to access the chart does not infer permission. There are circumstances whereby access to a relative's PHI would be permitted by law but being a nurse does not warrant an exception unto itself. In the absence of certain conditions and generally speaking, the law does not permit access to a relative's data. However, 57.8% of new nurses believed that access to relative's data was permissible. This item too offers a potential knowledge gap worth further exploration for education and employers.

Knowledge is related to neither the CFIP nor the IPPR. This describes how new nurses may have concern over the protection of patient information and exhibit responses whether or not they have an understanding of information system security.

### Level of Risk

Analysis of risk behavior has produced a paradoxical unanticipated finding. Risk behavior has already been discussed as having an inverse relationship with knowledge. Unlike knowledge, risk behavior is also directly related to both the CFIP and IPPR. This infers that new nurses who engage in higher rates of risk behavior activities related to their use of mobile devices have both a low knowledge of information security and an affinity to not only have concern for privacy but also exhibit protective responses. A plausible elucidation is that new nurses with an elevation in risk behavior may have a sense of self-awareness that their actions

may put sensitive information at risk and are therefore more cognizant of the implications to the safeguarding of protected health information.

The acceptance of using personal email for patient information by a minor segment of new nurses is an education gap that could be filled. While the HHS final ruling modifying the HIPAA Security Rule does not explicitly prohibit the use of personal email for PHI, the onus is on the healthcare entity to safeguard protected health information and personal email is considered a risk vehicle for the correspondence of PHI. Yahoo, a large provider of personal email, reported that all three billion of their accounts were hacked in 2013 (Business Time Singapore, 2017). The willingness of some to use PHI in email textured with a relatively low number of respondents appropriately responding to a phishing attack and in context with Yahoo hack disclosure should indicate that targeted education and the implementation of security controls regarding email use may be suitable.

Unexpectedly, 19.9% of new nurses declared that they download pirated material although most stated the occurrences to be rare. Employers should be aware and have security measures in place to prevent the downloading of unauthorized material regardless of the finding. Legal considerations notwithstanding, the acquisition of products without using reputable means could lead to cybersecurity incidents such as the introduction of malware and viruses. Note that the use of antivirus is not to be considered a universal protector or panacea against viruses as seen with numerous cybersecurity incidents in the news, the most noteworthy at the time of this data collection, being WannaCry, a virus that caused billions of dollars in damage worldwide; including the healthcare sector (Reuters, 2017). Although WannaCry was not propagated by illegally obtained software or even by email (as widely falsely reported), the example serves as the degree to which virus can cause damage. WannaCry is used in this instance, as it is the

widest cybersecurity attack to date and affected systems worldwide including clinical systems. This risk behavior has the potential to affect the functionality of clinical systems.

In the reported behaviors, it would appear that financial data breaches occurred in 30% of new nurses. Conversely and in alignment with the new nurses' financial data breach finding, only 27.4% of new nurses recognized the phishing attack from the knowledge survey. The question did not offer any determination as to how the data may have been breached or to what degree. The data suggests that new nurses may lack knowledge of key areas of common attack by nefarious agents and many may have already suffered data breaches with financial implications by the time they embarked on their career. Both the data breach and knowledge question statistics support a lack of knowledge and sophistication with both security practices and knowledge. This confluence of factors indicates a need for better education both in school and in the workplace to recognize phishing attacks. Simulated phishing attacks are offered by vendors as part of an effort to educate employees and encourage engagement to report instances to the employer.

#### Information Privacy Protection Responses and Concern for Information Privacy

New nurses' Concern For Information Privacy and the Information Privacy Protective Responses are directly related to one another. Analysis included the subscales of the CFIP as well as the variable as a whole. This finding was anticipated as the CFIP elements were posed in the context of nurses' concern for patient information. The IPPR, although questioned in the context of responding to transgressions involving the nurses' information, is consistent in its relation to the IPPR as prior studies (Kuo, Ma, & Alexander, 2014). Age is not related to the CFIP but it is related to the IPPR even as CFIP and IPPR are however related to one another.

The level of concern about patient information is unrelated to age. There is no significant relation between age and CFIP. Although there is a negligible correlation between age and the IPPR, the direction is inverse.

### Reliability of All Measurement Scales

As discussed in Chapter 4, the instrument reliability has been assessed and reported in descriptive and tabulated formats using Cronbach's alpha statistic estimates for the pilot (n=167) and the nationwide study (n=514). While the goal of having Cronbach's alpha statistic estimate values of .70 or greater for each instrument, the KISS instrument was accepted at the principal investigator's discretion with a Cronbach's alpha statistic estimate of .669. Based upon the discovery that the reduction in knowledge score elements would yield only minor increments in improving the value and that the reduction of elements would reduce informative results, the score was accepted without reduction in items. The knowledge score was developed by the principle investigator with an expert jury panel and delivered to a convenience sample of nursing student. The Concern for Information Privacy (CFIP), Information Personal Protective Response, the four subscales for the Concern for Information Privacy (AU= Unauthorized Access; SU=Secondary Use; ME=Medical Errors; CO=Personal Collection of Medical Information), Knowledge of Information Security Systems (KISS) and the Risk Behaviors (RB) were the scales modified from existing scales in the literature (Kuo, Ma, & Alexander, 2014) and used with permission in this study with demonstrated reliability.

### Reported Threat Appraisal – “Worry” About a Consequence – Ranked Groups

Threat appraisal was surveyed to determine the degree to which new nurses would be worried about consequences resulting from a security incident. This was a rank-order question on a scale of 1-4 with 4 being the most severe sense of worry. This was an effort to determine the level of internal versus external threat. Internal threat was related to the nurses themselves whereas external was related to consequences for others. More specifically, the internal threat asked about job loss and fines to the nurse. The external threat asked about the consequences to the patient and fines to the hospital.

The internal threat of the fine to the nurse was directly related to knowledge. Results related to the external threat to patient privacy suggests that further exploration may be warranted. The internal threat of job loss was not found to relate to any of the core variables, nor were any other aggregate associations. Further study might be warranted on focusing on some of the factors associated with these threat appraisal categories.

### Question: Is Knowledge a Predictor of Risk and Concern for Information Privacy Total and Factors?

#### Knowledge Related To Risk

Speculatively, these results could infer that having a workforce membership with higher knowledge of information security could result in a lower level of risk behaviors associated with those devices. This finding could inform educators and stakeholders of information security of the need for knowledge in order to reduce risk behaviors among nurses who make up the largest segment of workforce membership in the healthcare industry.

### Knowledge Related To Concern For Information Privacy

Knowledge is related to neither the CFIP nor IPPR, which are closely correlated to one another.

### Question: Are Risk Behaviors Related to Concern for Information Privacy Total and Factors?

CFIP and IPPR are related to one another with risk behaviors showing a positive correlation to both. However, CFIP and IPPR are more strongly correlated than either is to risk behavior. As discussed, the CFIP and IPPR correlation was anticipated and are consistent with findings from the Kuo, Ma, and Alexander (2014) study from which elements of this study were derived.

Although the relation between risk behavior to both the IPPR and CFIP is informative, this was not the hypothesis to be tested, and in fact, significant in the opposite direction from the hypothesis. The hypotheses suggesting a relationship between CFIP, IPPR and risk behaviors were predicted to have an inverse correlation. That is to state that lower risk behavior was anticipated to show an increase in both concern and response.

Perhaps those new nurses who engage in an increased risk behavior may be aware of the harm potential. The nurses may be more apprehensive about the protection of sensitive data given their understanding and susceptibility to behaviors that increase risk. As this finding was unanticipated and counterintuitive, there may be an opportunity for further study of these factors' relationship.

Question: Is Threat Appraisal Associated with Knowledge, Risk, Concern for Information Privacy Total and Factors, and Personal Protective Responses?

Threat is not related to risk behavior, CFIP, or IPPR. The internal threat of nurse fine is however related to knowledge whereas the external threat to patient privacy approaches significance and may be worthwhile of further investigation.

OCR is the branch of HHS charged with enforcement of regulation infractions related to PHI. OCR action has resulted in large fines to healthcare entities and those actions have been covered by the media in addition to being placed onto the proverbial “wall of shame.” However, nurses are not typically named in any of these high-profile actions. The anecdotal messages through either school or the employment experience may have shaped these nurses’ sense of threat.

Threat – Internal and External

The survey contains four elements that are evenly divided into external and internal related threats. Those results are discussed in the subsequent sections as analysis was performed to test for differences in mean scores on the core variables. In future studies, these should be more granularly described to produce a more meaningful distribution of responses.

An ANOVA was performed on the mean score for the threat of nurse fine (internal threat) showing statistically significant differences for knowledge but none of the other core variables. The highest threat ranking with a mean score of .81 indicates the highest threat of fine have the lowest knowledge score. Perhaps those who have a greater understanding of information system security are less worried of fines as opposed to those without knowledge having a fear of the unknown. It should be noted that this fear is unsubstantiated as newsworthy



action taken by OCR typically results in fines and corrective action directed at institutions and physician practices, not individual nurses.

The mean score comparisons for knowledge, risk behaviors, CFIP, and IPPR by the threat ranks on the threat of job loss (internal threat) showed no differences among mean scores. The same results stand for threat to patient privacy (external threat) and threat of hospital fine (external threat). The threat to patient privacy (external) may have implication for further research as this was the only other factor approaching significance.

#### Hypothesis Testing: Demographic Variables

Is knowledge, risk, concern or protective responses influenced by select demographic characteristics such as gender, age and education (program type or school type)?

#### Differences in Knowledge, Risk, and Concern for Information Privacy and Protective Responses

##### Age Related To Knowledge, Risk Behaviors

From the study findings, the conclusion is that risk behaviors are related to knowledge and knowledge is related to age, but age is not related to risk behaviors or concern. Age is directly related to knowledge. Those in the older age group had higher knowledge scores. This suggests although nursing experience was primarily eliminated, those in the older group may have had other experiences that could have contributed to their knowledge base. Knowledge of information security is different from skills related to the use of clinical information systems. Although the younger group may be considered digital natives, it is their older counterparts that have the insight to produce significantly higher knowledge scores.

While not a primary variable, the time spent using mobile devices is inversely related to age. There are also notable differences in the use of mobile device features by age. Age is inversely related to the IPPR but not related to the CFIP or risk behavior.

### Education Related To Knowledge, Risk Behaviors, CFIP, and IPPR

In general, nursing education prepares prospective nurses for entry into the profession. It serves as a major component of the prerequisites mandated by the individual state board to receive licensure with each state regulatory body setting such licensure requirements. Educational institutions are subject to accreditation requirements set forth by sanctioned accreditation bodies.

The NSNA serves over 60,000 members from across the United States and its territories serving in both an advocacy and promotional role in its mission to support the development of emerging professional nurses. With its vast membership, this organization could serve as a vehicle for delivering cybersecurity guidance to the masses. None of the core variables studied were related to the type of education program or type of school which indicates that tailoring cybersecurity guidance to those demographic targets is not necessary. However, gaps in cybersecurity knowledge of new nurses were uncovered by this study.

Furthermore, cybersecurity education tends to be deficient for nurses in their education programs and even for students of computer science where such information may be considered more germane to this area of study (Rozenfeld, 2016). This absence of cybersecurity knowledge in education is not unique to nursing program and member associations.

The National Council of State Boards of Nursing (NSCSBN) offers guidance mostly related to social media use which has implications tangentially related to cybersecurity but is for the most part lacking in cybersecurity knowledge needed to support the safeguard of PHI in the

workplace. Both the NSNA and the NSCSBN could see the gap as an opportunity to educate its members through a program of cybersecurity guidance.

The standard demographic elements from the NSNA included questions related to the type of school such as public or private. The survey also asked the type of education in the nursing program such as associate, baccalaureate, or masters. The type of school and type of education did not yield any relation to the core variables. The nursing education variables did not have any impact on their knowledge, risk behaviors, CFIP, or IPPR. The Institute for Medicine has called for an increase to an 80% ratio of nurses with a baccalaureate by the year 2020 and hospital-based studies have supported this notion with findings showing improved outcomes (Yakusheva, 2014). However, no such supportive findings are evident in this study related to the security of mobile devices among new nurses.

### Limitations

Information related to employment status, type of employment, healthcare-related experience, and Registered Nurse experience for those with advanced degrees was not collected. By using a sample of nurses one-year post graduation, the sample was considered mostly homogenous in relation to experience.

Of the 649 respondents, 135 of those did not opt to complete the knowledge section. Speculatively, this section may have seemed daunting as the largest segment of the survey and participants may have experienced a sense of survey fatigue.

The sample consisted only of those nurses who were NSNA members and had agreed to receive correspondence such as this survey. This 514-person sample represented only those members who self-selected to perform the study to its completion. This pool may be considered

representative of new nurses from across the nation, but not necessarily the entire population of nurses in the United States or the world for that matter.

NSNA was gracious in administering the survey to their members. Without their collaboration, obtaining such a sample for which to study may not have been possible or at least an arduous task at best. However, the survey product, methodology of delivery, and follow up were directed by NSNA. The demographic questions were also the NSNA standard used on their surveys. While not a constraint unto itself, flexibility to augment the process was nonetheless limiting.

The knowledge score was internally developed by the principal investigator with validation by a jury panel and content validity analysis. This instrument was not based upon a gold standard instrument as one does not currently exist for the population studied and with the content used to construct the instrument.

### Conclusion

Data security incidents and issues are regularly featured in the media. The public has been exposed to a growing sense of awareness about cybersecurity and the implications for their privacy.

Former government contractor Eric Snowden provided revelations as to the United States government operation with data collection and analytic activities. Russian government operations have been implicated in hacking and social media activities resulting in the interference with the United States 2016 Presidential election (Shane, Sanger, & Kramer, 2017).

Related to the reports of Russian hacking is the disclosure that Facebook users' information was misappropriated by a data analytics company for the expressed purpose of

influencing the same election (Granville, 2018). The disclosure about the misuse of Facebook data is an example of the Concern For Information Privacy subscales. Collection: The data was collected. Secondary Use: The data was then used by a third party unbeknownst to the users that had their data collected.

Other political activities include North Korea's purported creation and spread of the WannaCry virus, the most vast cybersecurity incident in history resulting in detrimental effects to the world's economy and to the clinical operations of healthcare facilities. The United States Department of Homeland Security has issued a bulletin about activities by the Russian Government resulting in the infiltration into energy sector computers (DOH, 2018). The techniques described in the bulletin may also be applied to the healthcare sector.

The general public may relate more to nefarious activities that are personally-directed. These include identity theft, credit card fraud, hijacked online accounts, and even phishing phone scams. An example of phone phishing are those prevalent calls with fake Internal Revenue Service representatives demanding back taxes. Related to healthcare, an emerging scam is the fake hospital representative calling to collect bills or financial data. Yahoo had virtually all of its accounts hacked. Equifax, Target, and Home Depot have had high profile breaches affecting consumers' financial data. Anthem's 2015 cybersecurity incident was also prominently covered in the media after nearly 80 million company records were hacked, including a substantial portion from individuals who were not even customers of Anthem.

In brief, the public has a sense of awareness about information security and its effects on their own personal data. This personal data includes PHI. Anthem was probably the most prevalent healthcare related cybersecurity event reported in the news media. The media has also

repeatedly reported on hospital ransomware infections. An identity theft protection company ran a promotional advertisement regarding PHI data theft.

In addition to public awareness, healthcare entities are faced with the pressure of compliance with regulation meant to safeguard PHI and penalties for both noncompliance and incidents. While certainly protective mechanisms span a multitude of factors, the workforce is a major part of an overall cybersecurity strategy. In healthcare, the largest professional segment consists of nurses; hence the importance of this study.

For education, this study has produced implications. First and foremost is that education contains only sparse information related to information security. This is not only true for nursing, but other disciplines including computer science (Rozenfeld, 2016). Some of the data elements with the knowledge section indicated key weaknesses which have the potential to put patient data at risk.

A recommendation from this study is that security awareness training should be conducted at all levels of nursing education meant for entry into the profession. As variations in quality and content may result from organically-grown institution-specific programs, perhaps a national or international organization may develop education standards or a framework to provide uniform coverage of education material across the nation. This investigator is a member of the Health Information Management Systems Society (HIMSS) National Education Task Force and would look to organizations such as this with a history of successfully implementing standards.

Employers already have a mandate from HHS to provide security awareness training to its workforce members. However, regulations are not prescriptive as to the content or manner of instruction. This study should provide information to employers not only on key areas of

knowledge to address but also the understanding of nurse risk behavior and mobile device usage. A vehicle to provide comprehensive education akin to the aforementioned nursing education recommendation might be via the state and local hospital associations that supply its members with recommendations and services.

Mobile device manufacturers and MDM vendors are already addressing the security needs of its healthcare use base. However, the lines between clinical systems, medical devices, wearable devices, and mobile devices is becoming blurred and likely to continue as new innovations emerge and are facilitated by mobile device platforms that are conducive to the rapid development of highly usable systems. The term IOT (internet of things) describes the phenomenon of smart internet-connected devices such as locks, alarms, and other innovations. With these factors in mind, mobile device vendors should develop hardened systems and platforms which address the cybersecurity needs of the healthcare industry at present and with a flexible foundation to endure the foreseeable future. Currently, healthcare does not have uniformly prescriptive standards for safeguarding these devices by legislation, only market forces (customers) and government agency guidance.

Employers should focus on implementing technology and processes that remove the human element from security wherever possible while having the least negative impact on clinical function and system usability. As discussed in the social engineering section, humans are the weakest link in the cybersecurity chain. Removing human factors from cybersecurity should be a key endeavor and permit clinicians to focus on patients. The solutions should be turn-key and transparent to the nurses. Make security compliance easy to obtain and expect a higher rate of security compliance in return.

In conclusion this nationwide study has examined new nurses' knowledge of information systems, risk behaviors, concern for information privacy, information privacy protective responses, threat appeal, associations among the variables, and associations with collected demographic detail. Nurses are the largest segment of the healthcare workforce and the human element in the protection of patient information. Therefore this study is imperative to understand nurses as a key endeavor protecting our health system in the informatics age. The study also provides recommendations to educators, employers, and mobile device manufacturers. Findings also offer opportunities for further research which will undoubtedly be necessary as the information system landscape evolves.



## References

- § 164.308(a)(5) 45 CFR subtitle A, Retrieved from <https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec164-308.pdf>
- Administrative simplification compliance act self assessment. (2014). Retrieved from <https://www.cms.gov/Medicare/Billing/ElectronicBillingEDITrans/ASCASelfAssessment.html>
- American recovery and reinvestment act, (2009). Retrieved from [http://www.healthit.gov/sites/default/files/hitech\\_act\\_excerpt\\_from\\_arra\\_with\\_index.pdf](http://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf)
- Aydın, Ö M., & Chouseinoglou, O. (2013). Fuzzy assessment of health information system users' security awareness. *Journal of Medical Systems*, 37(6), 9984. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/24141530>
- Breaches affecting 500 or more individuals. Retrieved from [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)
- Dillman, D., Smyth, J., & Melani, L. (2008). *Internet, mail, and mixed-mode surveys: The tailored design method* (3rd ed.) Wiley.
- Feeg, V., & Mancino, D. (2015). New graduates in nursing: A secondary analysis of reported stressors in the clinical setting. *Nursing Research*, 2(64), E61.
- Gardner, C. L., & Jones, S. J. (2012). Utilization of academic electronic medical records in undergraduate nursing education. *Online Journal of Nursing Informatics*, 16(2)
- Hadnagy, C. (2010). *Social engineering: The art of human hacking* John Wiley & Sons.

Hewitt, B., Dolezel, D., & McLeod, A., (2017). Mobile device security: Perspectives of future healthcare workers. *Perspectives in Health Information Management*, , 1-14.

HHS delegates security rule authority to OCR. (2009). *Managed Care Outlook*, 22(17), 1.

HHS releases HIPAA omnibus rule: Finally ... it's final. (2013, Mar 1,). *Briefings on HIPAA*

The HIPAA privacy rule. (2015). Retrieved from <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>

Granville, K. (2018). Facebook and cambridge analytica: What you need to know as fallout widens. *New York Times (Online)* Retrieved from <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

Kuo, K., Ma, C., & Alexander, J. W. (2014). How do patients respond to violation of their information privacy? *Health Information Management Journal*, 43(2), 23-33. 10.1177/183335831404300204 Retrieved from <http://journals.sagepub.com/doi/full/10.1177/183335831404300204>

Lori J Strauss. (2013). Overview of the HIPAA final omnibus rule. *Journal of Health Care Compliance*, 15(3), 53.

Medicare mandates electronic claims. (2003). Retrieved from <http://www.healthdatamanagement.com/news/8919-1.html>

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception*. Indianapolis, In: Wiley.

Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the health information technology for economic and clinical health act and the genetic

information nondiscrimination act; other modifications to the HIPAA rules. (2013). *Federal Register*, 78(17), 5565. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/23476971>

Most famous social network sites worldwide as of January 2018, ranked by number of active users (in millions). Retrieved from <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>

NSNA: About us. (2018). Retrieved from <https://www.nsna.org/about-nsna.html>

Ong, K. R. (2015). *Medical informatics: An executive primer* (3 ed. ed.) HIMSS Publishing. Retrieved from <http://www.crcnetbase.com/isbn/9781498757409>

Palmer, D. (2017). This expensive new ransomware targets organisations with specially crafted phishing lures. Retrieved from <http://www.zdnet.com/article/expensive-new-defray-ransomware-targets-us-and-uk-organisations-with-specially-crafted-phishing/>

Parker, C. (2014). Evolution or revolution - smartphone use in nursing practice *American Nurses Today*, 9(11) Retrieved from <https://www.americannursetoday.com/evolution-revolution-smartphone-use-nursing-practice/>

Recommendations for Social media usage and maintaining privacy, confidentiality and professionalism. (2018). Retrieved from [https://www.ncsbn.org/NSNA\\_Social\\_Media\\_Recommendations.pdf](https://www.ncsbn.org/NSNA_Social_Media_Recommendations.pdf)

Reisinger, D. (2017, May 23,). Apple and samsung stumble as smartphone market soars. *Fortune*, Retrieved from <http://fortune.com/2017/05/23/apple-iphone-gartner-market-share/>

- H.R.6 - 21st century cures act, (2015). Retrieved from <https://www.congress.gov/bill/114th-congress/house-bill/6/text>
- Rezaeibagha, F., Khin, T. W., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: Technical perspectives. *Health Information Management Journal*, 44(3), 23-38. 10.12826/18333575.2015.0001.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93.
- Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology*, , 153-176.
- Rozenfeld, M. (2016). Most top computer science programs skip cybersecurity. *The Institute*, Retrieved from <http://theinstitute.ieee.org/career-and-education/education/most-top-computer-science-programs-skip-cybersecurity>
- Shane, S., Sanger, D., & Kramer, A. (2017, Jan 27,). Russians charged with treason worked in office linked to election hacking. *New York Times (Online)*
- Smith, H.J., Milberg, J.S., and Burke, J.S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 196.
- TED: The economics daily image. Retrieved from <https://www.bls.gov/opub/ted/2015/registered-nurses-have-highest-employment-in-healthcare-occupations-anesthesiologists-earn-the-most.htm>

- Third annual survey on medical identity theft. (2012). Retrieved from [http://www.ponemon.org/local/upload/file/Third\\_Annual\\_Survey\\_on\\_Medical\\_Identity\\_Theft\\_FINAL.pdf](http://www.ponemon.org/local/upload/file/Third_Annual_Survey_on_Medical_Identity_Theft_FINAL.pdf)
- Tuttle, M. S. (1997). Medical informatics challenges of the 1990s: Acknowledging secular change. *Journal of the American Medical Informatics Association : JAMIA*, 4(4), 322-324. 10.1136/jamia.1997.0040322 Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/9223038>
- U.S. blame North Korea for cyber-attack WannaCry. (2017, Dec 19,). *International Wire*
- United States Department of Homeland Security. (2018). *Alert (TA18-074A) Russian government cyber activity targeting energy and other critical infrastructure sectors* Retrieved from <https://www.us-cert.gov/ncas/alerts/TA18-074A>
- United States Department of Labor. (2015). Retrieved from [https://www.dol.gov/wb/stats/occ\\_gender\\_share\\_em\\_1020\\_txt.htm](https://www.dol.gov/wb/stats/occ_gender_share_em_1020_txt.htm)
- Whipple, E., Allgood, K., & Larue, E. (2012). Third-year medical students' knowledge of privacy and security issues concerning mobile devices. *Medical Teacher*, 34(8), e532. 10.3109/0142159X.2012.670319
- White paper: A nurse's guide to the use of social media. (2011). *The Journal of Practical Nursing*, 61(3), 3. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/22479966>
- Yahoo says all 3 billion accounts hacked in 2013 data theft. (2017, Oct 5,). *Business Times Singapore*

Yakusheva, O. (2014). Economic evaluation of the 80% baccalaureate nurse workforce recommendation A patient-level analysis. *Medical Care*, 52(10), 864-869.

## Appendix A – Study Permission Fuzzy Logic



Keith Weiner <keithrn@gmail.com>

---

### Permission Requested - Research Study

---

Oumout Chouseinoglou <uhus@hacettepe.edu.tr>

Wed, Dec 23, 2015 at 4:10 AM

To: Keith Weiner <kweiner@lions.molloy.edu>, umuth@baskent.edu.tr, umut.huseyinoglu@gmail.com, ozlemaydin@hacettepe.edu.tr

Dear Keith,

me and Prof. Aydın we are very honored that you have been conducting a research that will be using some elements of our survey. If we understood you correctly, are you asking for the survey questions that we used in our research? If yes, we can email the survey and its questions to you, together with the information about Scale/Question combinations.

We will be looking for your email so that we can send you whatever you are requiring.

Thank you once again for your interest,

Yours sincerely

Oumout C.

On 12/22/2015 5:47 PM, Keith Weiner wrote:

Özlem Müge Aydın & Oumout Chouseinoglou,

I am a PhD Candidate conducting healthcare informatics research at Molloy College in New York.

Your article "Fuzzy Assessment of Health Information System Users' Security Awareness" is of particular interest to me.

I would be interested in using elements of your survey in a study I am conducting with nursing students in the United States. I seek your permission and would of course provide full credit. I would also modify some elements to suit the target demographic.

I thank you in advance for your consideration.

Kind Regards,

Keith Weiner

Figure 11 Permission: Fuzzy Assessment of Health Information System Users Security Awareness Survey and Study

## Appendix B – Fuzzy Logic Materials



Keith Weiner <keithrn@gmail.com>

---

### Permission Requested - Research Study

---

**Oumout Chouseinoglou** <uhus@hacettepe.edu.tr>

Thu, Dec 24, 2015 at 4:11 AM

To: Keith Weiner <kweiner@lions.molloy.edu>

Cc: umuth@baskent.edu.tr, Umut Huseyinoglu <umut.huseyinoglu@gmail.com>, ozlemaydin@hacettepe.edu.tr

Dear Keith,  
find attached the complete survey and the related article. As the survey was prepared for native Turkish speakers in Turkish, the translation of the survey may have some translation errors. Furthermore, the Survey questions / Scale associations are given at Table 2 of the article. Demographic questions are specific to the study group (students, admin, academics).

If you require anything further please do not hesitate to contact us,


Yours sincerely

Oumout C.

[Quoted text hidden]

---

#### 2 attachments

 **FuzzyAssessmentofHealthInformationSystemUsersSecurityAwarenessSurvey.pdf**  
209K


 **FuzzyAssessmentofHealthInformationSystemUsersSecurityAwareness.pdf**  
260K

Figure 12 Permission: Fuzzy Assessment of Health Information System Users Security

Awareness Survey and Study With Materials



Appendix C – Study Permission Violation of Information Security



Keith Weiner <keithrn@gmail.com>

---

**Permission Requested - Research Study**

---

郭光明(Kuang-Ming Kuo)@ISU <kmkuo@isu.edu.tw>  
To: KeithRN <keithrn@gmail.com>

Tue, Dec 22, 2015 at 7:21 PM

Dear Keith,

You have my permission to use or modify any ideas from this article.

Best Wishes,

Kuang-ming

2015-12-23 0:02 GMT+08:00 KeithRN <keithrn@gmail.com>:

Kuang-Ming Kuo, Chen-Chung Ma and Judith Alexander,

I am a PhD Candidate conducting healthcare informatics research at Molloy College in New York.

Your article "How do patients respond to violation of their information privacy?" is of particular interest to me.

I would be interested in using elements of your survey in a study I am conducting with nursing students in the United States. I seek your permission and would of course provide full credit. I would also modify some elements to suit the target demographic.

I thank you in advance for your consideration.

Kind Regards,  
Keith Weiner

Figure 13 Permission: How Patients Respond To Violation of Their Information Privacy

## Appendix D – Molloy College Institution Review Board Approval



1000 Hempstead Avenue  
Rockville Centre, NY 11571  
[www.molloy.edu](http://www.molloy.edu)

Tel. 516.323.3801  
Tel. 516.323.3711

**Date:** March 15, 2016  
**To:** Keith Weiner (Student), Veronica Feeg, Ph.D.  
**From:** Kathleen Maurer Smith, Ph.D.  
Co-Chair, Molloy College Institutional Review Board  
Patricia Eckardt, Ph.D., RN  
Co-Chair, Molloy College Institutional Review Board

**SUBJECT:** MOLLOY IRB REVIEW AND DETERMINATION OF EXEMPT STATUS  
**Study Title:** HEALTH INFORMATICS SECURITY AND PRIVACY: A SOCIAL SCIENCE EXPLORATION OF NURSES' KNOWLEDGE AND RISK BEHAVIORS WITH SECURITY AND PRIVACY ISSUES FOCUSING ON USE OF MOBILE DEVICES

**Approved:** March 15, 2016  
**Approval No:** 11230509-0315

Dear Keith and Dr. Feeg:

The Institutional Review Board (IRB) of Molloy College has reviewed the above-mentioned research proposal and determined that this proposal is approved by the committee. It is EXEMPT from the requirements of Department of Health and Human Services (DHHS) regulations for the protection of human subjects as defined in 45CFR46.101(b). Please note that as Principal Investigator (PI), it is your responsibility to be CITI Certified and submit the evidence in order to conduct your research.

You may proceed with your research. Please submit a report to the committee at the conclusion of your project.

Changes to the Research: It is the responsibility of the Principal Investigator to inform the Molloy College IRB of any changes to this research. A change in the research may disqualify the project from exempt status.

Sincerely,

Kathleen Maurer Smith, Ph.D.

Patricia Eckardt, Ph.D., RN

Figure 14 Molloy Institution Review Board Approval Letter

## Appendix E - Pilot Survey

### Demographic Background Information

1. Are you male or female?
  - Male
  - Female
  
2. When did you graduate from your basic nursing (RN) program?
  - 2016
  - 2015
  - 2014
  - Before 2014
  
3. What program did you complete for your nursing degree?
  - Baccalaureate Degree in Nursing
  - Associates Degree in Nursing
  - Accelerated Baccalaureate Degree in Nursing
  - Master's Degree in Nursing
  - Other
  
3. What is your age?
  - <17
  - 18-20
  - 21-29
  - 30-39
  - 40-49
  - 50-59
  - 60+
  
6. Does your program include educational sessions regarding the security of electronic health records?
  - Yes
  - No
  - Other (please specify) \_\_\_\_\_
  
7. Does your program include educational material regarding the security of electronic health records?
  - Yes
  - No
  - Other (please specify) \_\_\_\_\_

## Information Systems Security Survey

### Professional Habits (Risk Taking Behaviors)

(Includes All Items – Content Review by Experts)

\*(R) = Reverse Coded Item (↓Risk)

8. For my mobile device (phone/tablet), I .....

	Never	Rarely	Sometimes	Frequently	Always	N/A
...use my fingerprint complex passcode, or gesture to log on. (R)						
...regular update my operating system. (R)						
...“jailbreak”, or use a customized environment to get free apps.						
...click on email links to reset my password.						
...use free Wi-Fi at public locations such as cafes and airports.						
...keep my device attended and in my possession. (R)						
...encrypt my device (Apple users may select always). (R)						
...text patient information with colleagues (aside from corporate applications).						
...use personal email containing patient information.						
...accept invitations for games and apps through social networks.						
...download movies/music/apps by pirating or otherwise without paying (aside from legit streaming services).						
...have a complex Wi-Fi password on the home router. (R)						
...share my password (any) with others such as family, friends, or coworkers						

...use autofill to complete my information in websites.

...submit my personal information such as name, address, phone number, and credit card info into websites when requested.

...chat with strangers online.

...post personal information on social media sites.

...have had my financial/credit information personally breached (aside from publicized breaches of corporations).

...have had my passwords stolen/misused. This would be evident by unauthorized emails/posts sent or known to sites/services accessed by unauthorized entities.

9. I would.....

	Never	Sometimes	Frequently	Always
...report chart printouts found in a garbage can or publicly-accessible fax/printer. <b>(R)</b>				
...chat with others about patient information outside of work.				

**Information System Security Knowledge**  
**(Includes All Items Used for Content Review by Experts)**

**Choose the best answer.**

**You may not be fully in agreement with the answer.**

**You may have to choose one answer from what you feel may be multiple correct answers.**

*\* = Correct Response*

10. If my co-worker's login does not work, I may share mine.

- True
- False \*

11. Putting patient information on a USB drive is acceptable if....

- My superior instructs me to do so.
- The USB drive encrypted and used in a manner consistent with institutional policy. \*
- I delete it shortly thereafter.
- I keep the USB drive securely on my person at all times.

12. Texting patient information is acceptable if....

- My supervisor instructs me to do so.
- I am using a hospital-issued cell phone.
- I am using a hospital-issued secure messaging system. \*
- I urgently need to communicate with a physician.

13. Placing patient information on my personal computer is acceptable if....

- My supervisor instructs me to do so.
- I have antivirus and a firewall.
- I am a private contractor with contracted responsibility and liability.
- I have a HIPAA-compliant logon.
- None of the above. \*

14. I may access my relative/spouse/partner/friend's electronic health information if....

- This person gave me permission to do so.
- I need information to care for this relative at home.
- I am helping this person to access information through the patient portal. \*
- My supervisor instructs me to do so.

15. If a police officer requests a copy of the patient's chart...

- I provide it on a USB drive
- I print out the chart.
- I ask my supervisor for guidance.

- I do not provide any information without a court order and would refer the office to the medical records department. \*

16. If I find a USB drive around the hospital, I...

- Hand it in to security or lost and found. \*
- Use it at home.
- Use it at the hospital.
- Dispose of it in the garbage.

17. If I discover a coworker/classmate has accessed their relative's information, I...

- Report this person to the supervisor or other personnel per institution policy. \*
- Remind the person that this behavior is not acceptable and in violation of HPA regulations.
- Do nothing as no action is necessary on my part.
- Contact administration or hospital-supplied privacy number. \*

18. If someone calls from the helpdesk requesting my password, I...

- Provide it as the helpdesk is a trusted entity.
- Would never provide my password. \*
- Call back to helpdesk to verify identity.
- Check with my supervisor first.

19. If IT (computer department) sends me an email to upgrade my email and asks me to verify my password. I...

- Enter my username and password after clicking on the email in order to upgrade
- Report the email to the proper person. \*
- Ask my supervisor for advice.
- Delete the email. \*

20. If my password is not working and my coworker/classmate offers to log in for me, I...

- Let my coworker to log in so I can continue working.
- Respectfully refuse and contact the helpdesk for assistance.
- Already have my coworker/classmate's password and log in.
- Remind my coworker not to share passwords and report if appropriate.
- Both D & B \*

21. I can put patient data on a USB stick if...

- I use it for work purposes.
- I always keep it in my possession.
- Make sure to delete the data when finished.

- It is encrypted/scrambled and used according to hospital policy. \*
22. If a website informs me that JAVA must be updated, I....
- Contact the helpdesk. \*
  - Install the file from the website.
  - Ask my supervisor.
  - Ignore the message.
23. If a computer message from the FBI states my files have been scrambled and I must pay 1 \$300 fine, I...
- Pay the file and have my files accessible.
  - Ignore the message and use another computer.
  - Contact the helpdesk. \*
  - Ask my supervisor.
24. If the IRS calls me about overdue taxes and requests a wire transfer, I....
- Follow the instructions to avoid legal repercussions.
  - Contact the helpdesk or security. \*
  - Hang up.
  - Report the call to the authorities.
25. If my phone regularly requires updates every few months. I....
- Update promptly. \*
  - Ignore the message.
  - Call the helpdesk.
  - Contact the phone carrier.
26. An email from my bank states my account had been compromised and I must verify my identity by clicking on a link and filling out some information, I....
- Enter my personal information to verify my identity and preserve my account.
  - Ignore and delete the email.
  - Contact the helpdesk. \*
  - Call the bank.
27. My coworker received a strange email from me requesting money, I....
- Tell the coworker it's a mistake and to ignore the email.
  - Ask the coworker to respond to the other email address listed in the email to state that this is a mistake.
  - Contact the helpdesk. \*
  - Contact that other email address in the email with a nasty message.



28. A well-known national realtor sends an email with the subject “Hot Properties in Your Neighborhood”. The link requests a Gmail or Yahoo login to proceed. Assuming there’s an interest, I....
- Log in using my Gmail or Yahoo account.
  - Contact the helpdesk. \*
  - Delete the email.
  - Ask my supervisor.
29. The corner deli that typically delivers lunch complains they received a fax with patient information, I....
- Instruct the deli to throw out the papers.
  - Instruct the deli to wait for me to pick up papers.
  - Contact helpdesk, compliance or other department per policy. \*
  - Ask the deli to return the papers with the next lunch delivery.
30. When leaving a computer logged in with my password, I....
- Lock the computer. \*
  - Sign out.
  - Leave it out courtesy for my coworker.
  - Leave it asking my coworkers not to touch it.
31. A pop-up appears informing me the computer is running slow, I....
- Follow the instructions as the computer has been running quite slow.
  - Close the pop-up and continue working.
  - Contact the helpdesk. \*
  - Ask the supervisor.
32. Taking patient or chart photos with my own cell phone is acceptable if....
- Delete after using.
  - A program is used to cover any identifiable information.
  - Done so in strict accordance with hospital policy permits.
  - Requested to do so by a doctor.
  - Never. \*
33. A person without a hospital badge states he is from IT and needs me to login for him to fix the slowness problem, I....
- Log in for him as the electronic records as the system has been slow.
  - Ask him for his hospital badge and upon display log in for him.
  - Ask him for the hospital badge and state policy will not permit you to log in for him. \*

- Call security if he does not show the badge upon request. \*

34. I may work with documents containing patient information on my home computer or laptop....

- If I delete the files afterwards.
- If I password protect my computer.
- If my supervisor gives me permission.
- No, this is not permitted. \*

35. If I need to look at my health records, I....

- Look in the electronic health records as this is my data and policy applies to other patient's data.
- Look in the electronic health records if explicitly permitted by policy.
- Use the patient portal or medical records department. \*
- Ask any doctor to look up my information.

36. If a law firm requests patient information, I....

- Provide the information on a USB stick the supply.
- Print out the information for them.
- Allow them to view the information, but not have a copy.
- Contact medical records, security, supervisor, or other personnel as per policy. \*

37. If a standard computer without encryption has a sensitive file that is purposefully deleted...

- I can be sure that it is gone as I emptied the computer trash container.
- Do not know if it is really gone. \*
- Definitely gone no matter what because I have password on my computer.
- Only gone once I reboot.

38. It is acceptable to backup patient information to my personal cloud (Google Drive, Dropbox, iCloud, etc...) for safekeeping.

- If I make sure I use a strong password.
- If I delete the files when I'm done with them
- If I do not let anyone know.
- Never as this is not permitted. \*

39. If my coworker suspects someone must have looked at his/her health record due to gossip about his/her condition, I would...

- Assure my coworker that no one would have looked at the health records.
- Ask around who looked at the health records.
- Warn people no to look at coworkers' health information.
- Make an inquiry/report to corporate compliance or appropriate entity per policy. \*

40. If I cannot find my laptop/tablet containing sensitive information, I...

- Wait until the device turns up and take later if it does not.
- Know it's secure because I need a password to log in.
- Know it's secure because I erased all of the sensitive information.
- Contact security, helpdesk or other entity as required by policy. \*

**Nurses' Belief About Medical Facilities and Personal Health Information  
Concern for Information Protection (CFIP) Scales**

Regarding the use of technology related to personal health information, please state your opinion on the following statements. Medical facilities should.....

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
...devote more time and effort to preventing the unauthorized access of patients' personal information. (UA)					
... prevent unauthorized people from accessing patients' personal information without considering the cost. (UA)					
...take more measures to ensure that unauthorized people cannot use their computer to access patient's information. (UA)					
... never use patients' personal information for purposes other than medical care unless it has been authorized by the patient. (SU)					
... not use the personal information provided by the patient for any purpose other than those required for medical care. (SU)					
... never sell their patients' personal information to other institutions unless it has been authorized by the patient. (CO)					
... not share patients' personal information with other institutions unless it has been authorized by patients. (SU)					
... repeatedly check the accuracy of patients' personal information without considering the cost. (ME)					
... use more procedures to check the accuracy of patients' personal information. (ME)					
... have more comprehensive procedure to correct the errors in patients' personal information. (ME)					

**Nurses Beliefs as Patients**

**Concern for Information Privacy (CFIP) - Scales Integrated Throughout Items**

42. Please indicate the extent at which you agree for the following statements.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I would refuse to provide information to medical facilities because I think it is too private.					
I would misrepresent some of my personal information if it is requested by medical facilities.					
I would take some action to have my private information removed from the EHR database when it was not properly used.					
I would speak with my acquaintances about my poor experience with medical facilities' mishandling of my personal information.					
I would contact medical facilities to complain about the way they mishandled my personal information.					
I would contact an elected official or consumer protection organization to complain about the way they mishandled my personal information by medical facilities.					
I would refuse to provide information to medical facilities because I think it is too private.					
I would misrepresent some of my personal information if it is requested by medical facilities.					
I would take some action to have my private information removed from the EHR database when it was not properly manipulated.					
I would speak with my acquaintances about my poor experience with medical facilities' mishandling of my personal information.					
I would contact medical facilities to complain about the way they mishandled my personal information.					
I would contact an elected official or consumer protection organization to complain about the way they mishandled my personal information by medical facilities.					

It bothers me when medical facilities ask me for personal information.

I sometimes think for a while when medical facilities ask me to provide personal information.

It bothers me to find personal information in so many facilities.

It bothers me that medical facilities collect so much personal information.

## Appendix F – Abbreviation Definitions

ARRA: American Recovery and Reinvestment Act

CFIP: Concern For Information Privacy

- AU: Unauthorized access to medical information
- CO: Personal collection of medical information
- ME: Medical facilities errors
- SU: Medical facilities' secondary use of medical information

EHR: Electronic Health Record

ePHI: Electronic Protected Health Information

HIT: Health Information Technology

HITECH: Health Information Technology for Economic and Clinical Health

IPPR: Information Privacy Protective Responses

KISS: Knowledge of Information Systems Security

MDH: Mobile Device Habits

PHI: Protected Health Information

PTP: Personal Technology Practices

RB: Risk Behaviors

RN: Registered Nurse

## Appendix G – National Student Nurse Association Social Media Guidelines

NSNA Guidelines	Example
Student nurses should be cognizant of the potential impact of each post made, with the understanding that patients, classmates, instructors, employers, and other personal or professional contacts may view an individual’s online activity as a reflection of the individual’s career as well as the nursing profession in general.	
Student nurses should stay informed about the privacy settings of the social media sites they utilize, as privacy settings often change.	For example, Facebook previously offered a privacy setting that restricted anyone (even friends) from viewing photos that you are tagged in. This was discontinued.
Student nurses who utilize social networking sites should actively maintain an awareness of how their professionalism may be affected by friends’ and peers’ usage of the same sites.	For example, Jane posts photos from a weekend party and tags Dave in several of them. Dave immediately untags himself to maintain his professionalism. However, Jane has set her privacy settings for the photo album so that “friends of friends” may view them. Even though Dave is no longer tagged, all of Jane’s friends—and everyone connected to each friend of Jane—can view photos of Dave that Jane uploaded.
Student nurses who are elected/appointed officers should restrict their personal activity to family and friends, and maintain a second option for their “public face” for colleagues, classmates and peers while in office. This is also recommended for student nurses who want to maintain a separation of their personal lives from their professional lives.	A school president creates a public Facebook page that followers can “like” to maintain professional networking and communications with the school chapter Board.  After thoroughly reviewing the privacy setting options, a student chooses a customized setting so that anyone in their “Restricted” group may only view their profile photo and contact information. When a new professional contact requests friendship, the student adds the new contact to their “Restricted” group and accepts the request. If the student would like to post a healthcare related article, she/he may change the settings for that particular post so that all friends can view it
Student nurses should not share, post, or otherwise disseminate any information, that can identify a patient, or in any way violate a patient’s rights or privacy. Limiting access through privacy setting is not sufficient to ensure privacy of patients.	
Student nurses should never refer to anyone in a disparaging manner, even if the person cannot be identified with the information stated.	
Student nurses should not make threatening, harassing, sexually explicit, or derogatory statements regarding any person’s race, ethnicity, gender, age, citizenship, national origin, sexual orientation, disability, religious beliefs, political views, or educational choices.	
Student nurses should not make disparaging remarks about any college, university, or school of nursing, including the students, faculty members and staff.	
Student nurses should not post content or otherwise speak on behalf of any college, university, school of nursing, or other student nurses association unless authorized to do so.	
NSNA constituent school chapters, state associations and individual members should refrain from social media usage that individually represents—or attempts to represent—the voice of NSNA.	

Figure 15 NSNA Social Media Guidelines



Appendix H - Content Validity: Student Nurses' Knowledge of Information System Security and Risk Behaviors

(Original – Content Validity)

- Please circle the appropriate number and provide comments where applicable.
- Use the numerical value if corrected according to your commentary, not as it was originally written

**Survey Items**

The purpose of this nation-wide pilot survey is to assess student nurses' knowledge of information system security and assess their risk behaviors.

**Representativeness**

1 = the item is not representative of a student nurse's knowledge or behavior of information system security.

2 = the item needs major revisions to be representative of a student nurse's knowledge or behavior of information system security.

3 = the item needs minor revisions to be representative of a student nurse's knowledge or behavior of information system security.

4 = the item is representative of a student nurse's knowledge or behavior of information system security.

	1	2	3	4
What is your current level of nursing education?				
First Year				
Second Year				
Third Year				
Fourth Year				
Enrolled in Diploma Program				
Enrolled in Certificate Program (non-NP)				
Enrolled in Master's Program (non-NP)				
Enrolled in an NP Program				
Enrolled in PhD Program				
Enrolled in DNP Program				
Other (Please state)				
Have you already been a Registered Nurse?				
<input type="checkbox"/> Yes <input type="checkbox"/> No				

Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

Does your program include lesson material regarding Information System security or electronic health record security?

1

2

3

4

Comments:

Yes  No

Item well written and succinct.  Yes  No  
If no, please provide edits.

(CONTINUED)

For my mobile device (phone/tablet), I...

1                      2                      3                      4  
Comments:

<Never/Sometimes/Frequently/Always>

- use my fingerprint, complex passcode, or gesture to log in.
- regularly update my operating system.
- “jailbreak”, or use a customized environment to get free apps.
- click on email links to reset my passwords.
- use free wifi at public locations such as cafes and airports.
- keep my device attended and in my possession.
- encrypt my device (Apple uses may select always).
- text patient information with colleagues (aside from corporate applications).
- use personal email containing patient information.
- accept invitations for games and apps through social networks.
- download movies/music/apps by pirating or otherwise without paying (aside from legit streaming services).
- use filesharing programs such as Azure, uTorrent, Vuse, etc...
- have a complex wifi password on the home router.
- share my passwords (any) with others such as family, friends, or coworkers.
- use autofill to complete my information in websites.
- submit my personal information such as name, address, phone number, and credit card info into websites when requested.
- chat with strangers online.
- post personal information on social media sites.
- have had my financial/credit information personally breached (aside from publicized breaches of corporations).
- have had my passwords stolen/misused. This would be evident by unauthorized emails/posts sent or known of sites/services accessed by unauthorized entities.

Item well written and succinct.  Yes  No  
If no, please provide edits.

1) If my co-worker's login does not work, I may share mine.

True  False

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

2) Putting patient information on a USB drive is acceptable if...

- a. my superior instructs me to do so.
- b. the USB drive is encrypted and used in a manner consistent with institutional policy.
- c. I delete it shortly thereafter.
- d. I keep the USB drive securely on my person at all times.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

3) Texting patient information is acceptable if...

- a. my superior instructs me to do so.
- b. I am using a hospital-issued cell phone.
- c. I am using a hospital-issued secure messaging system.
- d. I urgently need to communicate with a physician.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

4) Placing patient information on my personal computer is acceptable if...

- a. my superior instructs me to do so.
- b. I have antivirus and a firewall.
- c. I am a private contractor with contracted responsibility and liability.
- d. None of the above

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

5) I may access my relative's electronic health information if...

- a. my relative gave me verbal permission to do so.
- b. I need information to care for this relative at home.
- c. I was helping my relative access information through the patient portal.
- d. my superior instructs me to do so.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

1            2            3            4

6) If a police officer requests a copy of the patient's chart....

- a. I provide it on a USB drive.
- b. I print out the chart.
- c. I ask my supervisor for guidance.
- d. I do not provide any information without a court order and guidance from a supervisor.

Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

1                    2                    3                    4

Comments:

7) If I find a USB drive around the hospital, I...

- a. Hand it in to security or lost and found.
- b. Use it at home.
- c. Use it at the hospital.
- d. Dispose of it in the garbage.

Item well written and succinct.  Yes  No  
If no, please provide edits.

1                    2                    3                    4

Comments:

8) If I discover a coworker has accessed their relative's information, I...

- a. Report this person to the supervisor or other personnel per institution policy.
- b. Remind the person that this behavior is not acceptable and in violation of HIPAA regulations.
- c. Do nothing as no action is necessary on my part.
- d. Contact administration or hospital-supplied privacy number.

Item well written and succinct.  Yes  No  
If no, please provide edits.

1                    2                    3                    4

Comments:

9) If someone calls from the helpdesk requesting my password, I...

- a. Provide it as the helpdesk is a trusted entity.
- b. Would never provide my password.
- c. Call back to helpdesk to verify identity.
- d. Check with my supervisor first.

Item well written and succinct.  Yes  No  
If no, please provide edits.

1                    2                    3                    4

Comments:

10) If IT (computer department) sends me an email to upgrade my email and asks me to verify my password, I...

- a. Enter my username and password after clicking on the email link in order to upgrade.
- b. Report the email to the proper person.
- c. Ask my supervisor for advice.
- d. Delete the email.

Item well written and succinct.  Yes  No  
If no, please provide edits.

1                    2                    3                    4

Comments:

11) If my password is not working and my coworker offers to log in for me, I...

- a. Let my coworker to log in so I can continue working.
- b. Respectfully refuse and contact the helpdesk for assistance.
- c. Already have my coworker's password and log in.
- d. Remind my coworker not to share passwords and report if appropriate.

Item well written and succinct.  Yes  No  
If no, please provide edits.

12) I can put patient data on a USB stick if...  
a. I use it for work purposes.  
b. I always keep it in my possession.  
c. Make sure to delete the data when finished.  
d. It is encrypted/scrambled and used according to hospital policy.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

13) If a website informs me that JAVA must be updated, I...

- a. Contact the helpdesk.
- b. Install the file from the website.
- c. Ask my supervisor.
- d. Ignore the message.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

14) If a computer message from the FBI states my files have been scrambled and I must pay a \$300 fine, I...

- a. Pay the file and have my files accessible.
- b. Ignore the message and use another computer.
- c. Contact the helpdesk.
- d. Ask my supervisor.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

15) If the IRS calls me about overdue taxes and requests a wire transfer, I...

- a. Follow their instructions to avoid legal repercussions.
- b. Contact the helpdesk or security.
- c. Hang up.
- d. Report the call to the authorities.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

16) If the phone regularly requires updates every few months, I...

- a. Update promptly.
- b. Ignore the message.
- c. Call the helpdesk.
- d. Contact the phone carrier.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

17) An email from my bank states my account has been compromised and I must verify my identity by clicking on a link and filling out some information. I...

- a. Enter my personal information to verify my identity and preserve my account.
- b. Ignore and delete the email.
- c. Contact the helpdesk.
- d. Call the bank.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

18) My coworker received a strange email from me requesting money. I...

a. Tell the coworker it's a mistake and to just ignore the email.

b. Ask the coworker to respond to the other email address listed in the email to state that this is a mistake.

c. Contact the helpdesk.

d. Contact that other email address in the email with a nasty message.

19) A well-known national realtor sends an email with the subject "Hot Properties In Your Neighbourhood". The link requests a Gmail or Yahoo login to proceed. Assuming there's an interest, I...

a. Log in using my Gmail or Yahoo account.

b. Contact the helpdesk.

c. Delete the email.

d. Ask my supervisor.

20) The corner deli that typically delivers lunch complains they received a fax with patient information. I...

a. Instruct the deli to throw out the papers.

b. Instruct the deli to wait for me to pick up the papers.

c. Contact helpdesk, compliance or other department per policy.

d. Ask the deli to return the papers with the next lunch delivery.

21) When leaving a computer logged in with my password, I...

a. Lock the computer.

b. Sign out.

c. Leave it out of courtesy for my coworker.

d. Leave it asking my coworkers not to touch it.

22) A pop-up appears informing me the computer is running slow, I...

a. Follow the instructions as the computer has been running quite slow.

b. Close the pop-up and continue working.

c. Contact the helpdesk.

d. Ask the supervisor.

1                      2                      3                      4

Comments:

Item well written and succinct.  Yes  No

If no, please provide edits.

1                      2                      3                      4

Comments:

Item well written and succinct.  Yes  No

If no, please provide edits.

1                      2                      3                      4

Comments:

Item well written and succinct.  Yes  No

If no, please provide edits.

1                      2                      3                      4

Comments:

Item well written and succinct.  Yes  No

If no, please provide edits.

1                      2                      3                      4

Comments:

Item well written and succinct.  Yes  No

If no, please provide edits.

- 23) Taking patient or chart photos with a cell phone is acceptable if...
- 1                      2                      3                      4
- Comments:
- a. Deleted after using.
- b. A program is used to cover any identifiable information.
- c. Done so in strict accordance with hospital policy if policy permits.
- d. Requested to do so by a doctor.
- Item well written and succinct.  Yes  No  
If no, please provide edits.
- 24) A person without a hospital badge states he is from IT and needs me to login for him to fix the slowness problem. I...
- 1                      2                      3                      4
- Comments:
- a. Log in for him as the electronic record as the system has been slow.
- b. Ask him for his hospital badge and upon display log in for him.
- c. Ask him for the hospital badge and state policy will not permit you to log in for him.
- d. Call security if he does not show the badge upon request.
- Item well written and succinct.  Yes  No  
If no, please provide edits.
- 25) I may work with documents containing patient information on my home computer or laptop.
- 1                      2                      3                      4
- Comments:
- a. If I delete the files afterward.
- b. If I password protect my computer.
- c. I my supervisor gives me permission.
- d. No, this is not permitted.
- Item well written and succinct.  Yes  No  
If no, please provide edits.
- 26) If I need to look at my health record, I...
- 1                      2                      3                      4
- Comments:
- a. Look in the electronic health record as this is my data and policy applies to other patients' data.
- b. Look in the electronic health record if explicitly permitted by policy.
- c. Use the patient portal or medical records department.
- d. Ask any doctor to look up my information.
- Item well written and succinct.  Yes  No  
If no, please provide edits.
- 27) If a law firm requests patient information, I...
- 1                      2                      3                      4
- Comments:
- a. Provide the information on a USB stick they supply.
- b. Print out the information for them.
- c. Allow them to view the information, but not have a copy.
- d. Contact medical records, security, supervisor, or other personnel as per policy.
- Item well written and succinct.  Yes  No  
If no, please provide edits.



28) If a standard computer without encryption has a sensitive file that is purposefully deleted...

- a. I can be sure that it is gone as I emptied the computer trash container.
- b. Do not know if it is really gone.
- c. Definitely gone no matter what because I have a password on my computer.
- d. Only gone once I reboot.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

29) It's acceptable to backup patient information to my personal cloud (Google Drive, Dropbox, iCloud, etc..) for safekeeping...

- a. If I make sure I use a strong password.
- b. If I delete the files when I'm done with them.
- c. If I do not let anyone know.
- d. Never as this is not permitted.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

30) If my coworker suspects someone must have looked at his/her health record due to gossip about his/her condition, I would...

- a. Assure my coworker that no one would have looked at the health records.
- b. Ask around who looked at the health record.
- c. Warn people not to look at coworkers' health information.
- d. Make an inquiry/report to corporate compliance or appropriate entity per policy.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

31) If I cannot find my laptop/tablet containing sensitive information, I...

- a. Wait until the device turns up and take action later if it does not.
- b. Know it's secure because I need a password to log in.
- c. Know it's secure because I erased all of the sensitive information.
- d. Contact security, helpdesk or other entity as required by policy.

1            2            3            4  
Comments:

Item well written and succinct.  Yes  No  
If no, please provide edits.

## Appendix I – Survey Instrument (National Survey)

### Technology in Your Nursing Practice

**Please take a few minutes to answer the following questions related to using technologies in your nursing practice.**

**The purpose of this survey is to assess your personal use of technologies at work and at home, including mobile devices and social media. It also will seek information about your personal responses to patient health information protections.**

**This survey is voluntary and your information is anonymous. You may quit at any time. The survey conducted by Keith Weiner, a doctoral candidate, under supervision of Dr. Veronica Feeg. For questions, please email Keith at [kweiner1@molloy.edu](mailto:kweiner1@molloy.edu) or Dr. Feeg at [vfeeg@molloy.edu](mailto:vfeeg@molloy.edu).**

**A cash incentive of \$100 will be raffled to a one participant selected at random. To be eligible, you may optionally submit your email address (kept separate from the survey results) at the end of the survey.**

**Thank you for your participation.**

**1. Gender**

- Male
- Female

**2. Type of nursing program did you graduated from?**

- Associates Degree
- Diploma
- Baccalaureate Degree
- Accelerated BSN program
- Masters Degree
- Clinical Nurse Leader Masters
- Doctorate
- RN to BSN
- Other (please specify)

**3. What is your age?**

- Under 22
- 23-28
- 29-32
- 33-38
- 39-42
- 43-48
- Over 49

4. Please check

- American Indian or Alaskan Native
- Asian
- Black or African American
- Caucasian
- Hispanic or Latino
- Mixed Race
- Native Hawaiian or other Pacific Islander
- Other (please specify)

5. Was the nursing program that you attended a public; private not-for-profit; private for-profit, proprietary school/university?

- Public (i.e. state colleges and state universities; community colleges)
- Private not-for-profit (i.e. New York University; Columbia University)
- Private proprietary for-profit (i.e. Chamberlain College; University of Phoenix; DeVry College)
- Other (please specify)

**Dimensions of Personal Health Information in Technology**

The following statements apply to one's belief about use of technology related to personal health information. Please answer each statement with the extent that you agree or disagree, from **STRONGLY DISAGREE (1) to STRONGLY AGREE (5)**.

6. The following statements reflect opinions about personal information in medical facilities. Please indicate for each statement below the extent that you "strongly disagree" - "disagree" - are "neutral" - "agree" or "strongly agree"

Medical facilities should...

6a

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not applicable/No opinion
devote more time and effort to preventing the unauthorized access of patients' personal information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not applicable/No opinion
6b	prevent unauthorized people from accessing patients' personal information without consideration of cost.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6c	take more measures to ensure that unauthorized people cannot use their computer to access patients' personal information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6d	never use patients' personal information for purposes other than medical care, unless authorized by the patient.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6e	not use the personal information provided by patients for any purpose other than those required for medical care.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6f	never share patients' personal information with other institutions unless authorized by the patient.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6g	repeatedly check the accuracy of patients' personal information without considering cost.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6h	use more procedures to ensure the accuracy of patients' personal information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6i	have a more comprehensive procedure to correct for errors in patients' personal information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7. The following statements are about YOU, in the event you are ever a patient in a medical or health facility. Please indicate for each statement below the extent that you "strongly disagree" "disagree" are "neutral", "agree" or "strongly agree."

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Not applicable/No opinion	
7a	I would refuse to provide information to medical facilities because I think it is too private.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Item not used in analysis
7b	I would misrepresent some of my personal information if it is requested by medical facilities.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Item not used in analysis
7c	I would take action to have my private information removed from a medical facilities database if it was not properly handled.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
7d	I would speak to my acquaintances about my poor experience with medical facilities' mishandling of my personal information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
7e	I would contact medical facilities to complain about the way they mishandle my personal information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
7f	I would contact an elected official or consumer protection organization to complain about the mishandling of my personal information by medical facilities.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
7g	It bothers me when medical facilities ask me for personal information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
7h	I sometimes think for a while when medical facilities ask me to provide personal information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
7i	It bothers me to give personal information to so many medical facilities.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	

7j

It bothers me that medical facilities collect too much personal information.

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

Not applicable/No opinion

Please add any comment or clarify

## Personal Use of Mobile Devices

**The following questions seek information about the types and extent you use personal mobile devices.**

8. What type of cell phone do you use? Make and Model? (eg iPhone 6S, Samsung Galaxy S6, HTC Bolt, etc...)

9. What is your estimate of the TOTAL number of minutes/hours you spend on a mobile device DURING A NORMAL WEEKDAY?

- Minimal (1-10 minutes)
- Rarely (11-30 minutes)
- Sometimes (31-60 minutes)
- Often (1 - 3 hours)
- Very Often (More than 3 hours)
- Not applicable

10. How often do you use these features on a mobile device (mobile phone or other device) during a normal weekday?

	Minimal	Rarely	Sometimes	Often	Very Often	Do Not Use	Feature Not Available
Talking (voice to voice)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web Browsing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Chatting (IM)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Text Messaging (SMS)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multimedia Messaging (MMS) - Picture and video	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Camera	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Calendar	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Notes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Contact List	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Maps/Navigation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social Media (Facebook, Instagram, etc..)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Music (Play/Stream)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Video/Movies (Play/Stream)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online Library	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please add any comment or clarify

11. Do you lock your mobile device using password or fingerprint protection while not in use?

	Always (100%)	Frequently (75%)	Sometimes (50%)	Rarely (25%)	Never (0%)	Device Not Capable	Not Applicable/Don't Know
Personal Phone	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Personal Mobile Device (Laptop/Tablet)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hospital-Provided Phone	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hospital Provided Mobile Device (Laptop/Tablet)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



## Personal Technology Practices

**The following questions assess your information technology and typical mobile technology practices.**

12. How often do you delete your web page cache/browsing history on your mobile device?

- Never
- Immediately
- When I think my significant other/boss might be looking at it
- Automatically, set every \_\_\_ day/week/month/etc.

13. How often do you delete emails from your mobile device?

- Never
- Immediately
- When space is needed
- Automatically or set on schedule

14. How often do you delete texts from your mobile device?

- Never
- Immediately
- When space is needed
- Automatically or set on schedule

15. Do you receive any patient/clinical data on your mobile device?

- Never
- Sometimes
- Often

## Technology Behaviors

**The following activities list a variety of internet and mobile device behaviors. Please indicate to what extent you engage in each behavior.**

16. Please indicate how frequently you engage in each of the following activities. Your responses can include "Never" "Rarely" "Usually" "Often" "Always"

	Never	Rarely	Usually	Often	Always
I accept social media invitations for applications.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I shop on the Internet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I use Facebook, Twitter and similar social network sites.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I download/save music, movies, programs and files from the Internet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I share my contact information on the Internet when required.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I use security programs like anti-virus, spyware removal, firewall, etc.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I delete the temporary files and Internet history before leaving a public computer.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I password protect my files.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I use complex and long passwords that cannot be easily guessed.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I change my passwords periodically.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I share my passwords with others.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I transfer (send or receive) files while I chat.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I use passwords when turning on all of my devices.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please add any comment or clarify

**Professional Habits**

17. For my mobile device (phone/tablet), I .....

	Never	Rarely	Usually	Often	Always
...“jailbreak”, or use a customized environment to get free apps.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...click on email links to reset my password.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...use free Wi-Fi at public locations such as cafes and airports.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...keep my device attended and in my possession.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...text patient information with colleagues (aside from corporate applications).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...use personal email containing patient information.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...accept invitations for games and apps through social networks.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...download movies/music/apps by pirating or otherwise without paying (aside from legit streaming services).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...share my password (any) with others such as family, friends, or coworkers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...use autofill to complete my information in websites.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...submit my personal information such as name, address, phone number, and credit card info into websites when requested.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...chat with strangers online.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
...post personal information on social media sites.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	Never	Rarely	Usually	Often	Always
...have had my financial/credit information personally breached (aside from publicized breaches of corporations).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

...have had my passwords stolen/misused. This would be evident by unauthorized emails/posts sent or known to sites. services accessed by unauthorized entities.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
---	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

...chat with others about patient information outside of work.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
--	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------

Please add any comment or clarify

## Information System Security Knowledge

18. Putting patient information on a USB drive is acceptable if....

- My superior instructs me to do so.
- The USB drive encrypted and used in a manner consistent with institutional policy.
- I delete it shortly thereafter.
- I keep the USB drive securely on my person at all times.

19. Texting patient information is acceptable if....

- My supervisor instructs me to do so.
- I am using a hospital-issued cell phone.
- I am using a hospital-issued secure messaging system.
- I urgently need to communicate with a physician.

20. Placing patient information on my personal computer is acceptable if...

- My supervisor instructs me to do so.
- I have antivirus and a firewall.
- I am a private contractor with contracted responsibility and liability.
- I have a HIPAA-compliant logon.
- None of the above.

21. I may access my relative/spouse/partner/friend's electronic health information if...

- This person gave me permission to do so.
- I need information to care for this relative at home.
- I am helping this person to access information through the patient portal
- My supervisor instructs me to do so.

22. If a police officer requests a copy of the patient's chart...

- I provide it on a USB drive
- I print out the chart.
- I ask my supervisor for guidance.
- I do not provide any information without a court order and would refer the office to the medical records department.

23. If I find a USB drive around the hospital, I...

- Hand it in to security or lost and found.
- Use it at home.
- Use it at the hospital.
- Dispose of it in the garbage.

24. If I discover a coworker has accessed their relative's information, I...

- Report this person to the supervisor or other personnel per institution policy.
- Remind the person that this behaviour is not acceptable and in violation of HIPAA regulations.
- Do nothing as no action is necessary on my part.
- Contact administration or hospital-supplied privacy number.

25. If someone calls from the helpdesk requesting my password, I....

- Provide it as the helpdesk is a trusted entity.
- Would never provide my password.
- Call back to helpdesk to verify identity.
- Check with my supervisor first.

26. I can put patient data on a USB stick if....

- I use it for work purposes.
- I always keep it in my possession.
- Make sure to delete the data when finished.
- It is encrypted/scrambled and used according to hospital policy.

27. If a website informs me that JAVA must be updated, I....

- Contact the helpdesk.
- Install the file from the website.
- Ask my supervisor.
- Ignore the message.

28. If a computer message from the FBI states my files have been scrambled and I must pay 1 \$300 fine, I...

- Pay the file and have my files accessible.
- Ignore the message and use another computer.
- Contact the helpdesk.
- Ask my supervisor.

29. If the IRS calls me about overdue taxes and requests a wire transfer, I....

- Follow the instructions to avoid legal repercussions.
- Contact the helpdesk or security.
- Hang up.
- Report the call to the authorities.

30. An email from my bank states my account had been compromised and I must verify my identity by clicking on a link and filling out some information, I....

- Enter my personal information to verify my identity and preserve my account.
- Ignore and delete the email.
- Contact the helpdesk.
- Call the bank.

31. My coworker received a strange email from me requesting money, I....

- Tell the coworker it's a mistake and to ignore the email.
- Ask the coworker to respond to the other email address listed in the email to state that this is a mistake.
- Contact the helpdesk
- Contact that other email address in the email with a nasty message.

32. A well-known national realtor sends an email with the subject "Hot Properties in Your Neighbourhood". The link requests a Gmail or Yahoo login to proceed. Assuming there's an interest, I....

- Log in using my Gmail or Yahoo account.
- Contact the helpdesk.
- Delete the email.
- Ask my supervisor.

33. The corner deli that typically delivers lunch complains they received a fax with patient information, I....

- Instruct the deli to throw out the papers.
- Instruct the deli to wait for me to pick up papers.
- Contact helpdesk, compliance or other department per policy.
- Ask the deli to return the papers with the next lunch delivery

34. When leaving a computer logged in with my password, I....

- Lock the computer.
- Sign out.
- Leave it out courtesy for my coworker.
- Leave it asking my coworkers not to touch it.

35. A pop-up appears informing me the computer is running slow, I....

- Follow the instructions as the computer has been running quite slow.
- Close the pop-up and continue working.
- Contact the helpdesk.
- Ask the supervisor.

36. Taking patient or chart photos with my own cell phone is acceptable if....

- Delete after using.
- A program is used to cover any identifiable information.
- Done so in strict accordance with hospital policy permits.
- Requested to do so by a doctor.
- Never.

37. A person without a hospital badge states he is from IT and needs me to login for him to fix the slowness problem, I....

- Log in for him as the electronic records as the system has been slow.
- Ask him for his hospital badge and upon display log in for him.
- Ask him for the hospital badge and state policy will not permit you to log in for him.
- Call security if he does not show the badge upon request.

38. I may work with documents containing patient information on my home computer or laptop....

- If I delete the files afterwards.
- If I password protect my computer.
- If my supervisor gives me permission.
- No, this is not permitted.

39. If I need to look at my health records, I....

- Look in the electronic health records as this is my data and policy applies to other patient's data.
- Look in the electronic health records if explicitly permitted by policy.
- Use the patient portal or medical records department.
- Ask any doctor to look up my information.



40. If a law firm requests patient information, I...

- Provide the information on a USB stick the supply.
- Print out the information for them.
- Allow them to view the information, but not have a copy.
- Contact medical records, security, supervisor, or other personnel as per policy.

41. If a standard computer without encryption has a sensitive file that is purposefully deleted...

- I can be sure that it is gone as I emptied the computer trash container.
- Do not know if it is really gone.
- Definitely gone no matter what because I have password on my computer.
- Only gone once I reboot.

42. It's acceptable to backup patient information to my personal cloud (Google Drive, Dropbox, iCloud, etc...) for safekeeping...

- If I make sure I use a strong password.
- If I delete the files when I'm done with them
- If I do not let anyone know.
- Never as this is not permitted.

43. If my coworker suspects someone must have looked at his/her health record due to gossip about his/her condition, I would...

- Assure my coworker that no one would have looked at the health records.
- Ask around who looked at the health records.
- Warn people no to look at coworkers' health information.
- Make an inquiry/report to corporate compliance or appropriate entity per policy.

44. If I cannot find my laptop/tablet containing sensitive information, I...

- Wait until the device turns up and take later if it does not.
- Know it's secure because I need a password to log in.
- Know it's secure because I erased all of the sensitive information.
- Contact security, helpdesk or other entity as required by policy.

#### Nurses' Belief About Medical Facilities & Personal Health Info - Concern for Info Privacy

45. Which most concerns you about keeping patient information secure in an EHR?

Rank in order from 1 (least worried) to 4 (most worried).

<input type="text"/>	Fines on me or loss of position
<input type="text"/>	Loss of employment
<input type="text"/>	Patient privacy exposed
<input type="text"/>	Hospital would be fined

Eligible for a \$100 gift certificate raffle

**Your information has been entered anonymously.**

**Click done to submit and you will have the option to participate in the raffle for a \$100 Amazon gift certificate on a separate, private page.**

**Thank you for participating.**

**Your information has been collected anonymously and kept separate from the raffle.**

**If you would like to be eligible for the \$100 Amazon gift certificate raffle, enter your email address for the drawing.**

**Your email address is not linked to your survey responses.**

**Thank you for participating.**

\* Please enter your email address below.

## Appendix J – Knowledge Test and Results Key

*\*Denotes designated correct response*

*Bold knowledge heading represents the corresponding reference number in the data analysis.*

### **Knowledge 1**

18. Putting patient information on a USB drive is acceptable if....

- a) My superior instructs me to do so.
- b) The USB drive encrypted and used in a manner consistent with institutional policy.\*
- c) I delete it shortly thereafter.
- d) I keep the USB drive securely on my person at all times.

### **Knowledge 2**

19. Texting patient information is acceptable if....

- a) My supervisor instructs me to do so.
- b) I am using a hospital-issued cell phone.
- c) I am using a hospital-issued secure messaging system.\*
- d) I urgently need to communicate with a physician.

### **Knowledge 3**

20. Placing patient information on my personal computer is acceptable if....

- a) My supervisor instructs me to do so.
- b) I have antivirus and a firewall.
- c) I am a private contractor with contracted responsibility and liability.
- d) I have a HIPAA-compliant logon.
- e) None of the above.\*

### **Knowledge 4**

21. I may access my relative/spouse/partner/friend's electronic health information if....

- a) This person gave me permission to do so.
- b) I need information to care for this relative at home.
- c) I am helping this person to access information through the patient portal\*
- d) My supervisor instructs me to do so.

### **Knowledge 5**

22. If a police officer requests a copy of the patient's chart...

- a) I provide it on a USB drive
- b) I print out the chart.
- c) I ask my supervisor for guidance.\*
- d) I do not provide any information without a court order and would refer the officer to the medical records department.\*

### **Knowledge 6**

23. If I find a USB drive around the hospital, I...

- a) Hand it in to security or lost and found.\*
- b) Use it at home.
- c) Use it at the hospital.
- d) Dispose of it in the garbage.

### **Knowledge 7**

24. If I discover a coworker has accessed their relative's information, I...

- a) Report this person to the supervisor or other personnel per institution policy.\*
- b) Remind the person that this behavior is not acceptable and in violation of HIPAA regulations.
- c) Do nothing as no action is necessary on my part.
- d) Contact administration or hospital-supplied privacy number.\*

### **Knowledge 8**

25. If someone calls from the helpdesk requesting my password, I...

- a) Provide it as the helpdesk is a trusted entity.
- b) Would never provide my password.\*
- c) Call back to helpdesk to verify identity.
- d) Check with my supervisor first.

### **Knowledge 9**

26. I can put patient data on a USB stick if...

- a) I use it for work purposes.
- b) I always keep it in my possession.
- c) Make sure to delete the data when finished.
- d) It is encrypted/scrambled and used according to hospital policy.\*

### **Knowledge 10**

27. If a website informs me that JAVA must be updated, I...

- a) Contact the helpdesk.\*
- b) Install the file from the website.
- c) Ask my supervisor.
- d) Ignore the message.

### **Knowledge 11**

28. If a computer message from the FBI states my files have been scrambled and I must pay a \$300 fine, I...

- a) Pay the fine and have my files accessible.
- b) Ignore the message and use another computer.
- c) Contact the helpdesk.\*
- d) Ask my supervisor.\*

### **Knowledge 12**

29. If the IRS calls me about overdue taxes and requests a wire transfer, I...

- a) Follow the instructions to avoid legal repercussions.
- b) Contact the helpdesk or security.\*
- c) Hang up.\*
- d) Report the call to the authorities.\*

### **Knowledge 13**

30. An email from my bank states my account had been compromised and I must verify my identity by clicking on a link and filling out some information, I...

- a) Enter my personal information to verify my identity and preserve my account.
- b) Ignore and delete the email.\*
- c) Contact the helpdesk.\*
- d) Call the bank.\*

### **Knowledge 14**

31. My coworker received a strange email from me requesting money, I...

- a) Tell the coworker it's a mistake and to ignore the email.
- b) Ask the coworker to respond to the other email address listed in the email to state that this is a mistake.
- c) Contact the helpdesk\*
- d) Contact that other email address in the email with a nasty message.

### **Knowledge 15**

32. A well-known national realtor sends an email with the subject "Hot Properties in Your Neighborhood."

The link requests a Gmail or Yahoo login to proceed. Assuming there's an interest, I...

- a) Log in using my Gmail or Yahoo account.
- b) Contact the helpdesk.\*
- c) Delete the email.
- d) Ask my supervisor.

### **Knowledge 16**

33. The corner deli that typically delivers lunch complains they received a fax with patient information, I...

- a) Instruct the deli to throw out the papers.
- b) Instruct the deli to wait for me to pick up papers.
- c) Contact helpdesk, compliance or other department per policy.\*
- d) Ask the deli to return the papers with the next lunch delivery

### **Knowledge 17**

34. When leaving a computer logged in with my password, I...

- a) Lock the computer.\*
- b) Sign out.\*
- c) Leave it out courtesy for my coworker.
- d) Leave it asking my coworkers not to touch it.

### **Knowledge 18**

35. A pop-up appears informing me the computer is running slow, I...

- a) Follow the instructions as the computer has been running quite slow.
- b) Close the pop-up and continue working.
- c) Contact the helpdesk.\*
- d) Ask the supervisor.

### **Knowledge 19**

36. Taking patient or chart photos with my own cell phone is acceptable if...

- a) Delete after using.
- b) A program is used to cover any identifiable information.
- c) Done so in strict accordance with hospital policy permits.
- d) Requested to do so by a doctor.
- e) Never.\*

### **Knowledge 20**

37. A person without a hospital badge states he is from IT and needs me to login for him to fix the slowness problem, I...

- a) Log in for him as the electronic records as the system has been slow.
- b) Ask him for his hospital badge and upon display log in for him.
- c) Ask him for the hospital badge and state policy will not permit you to log in for him.\*
- d) Call security if he does not show the badge upon request.\*

### **Knowledge 21**

38. I may work with documents containing patient information on my home computer or laptop....

- a) If I delete the files afterwards.
- b) If I password protect my computer.
- c) If my supervisor gives me permission.
- d) No, this is not permitted.\*

### **Knowledge 22**

39. If I need to look at my health records, I....

- a) Look in the electronic health records as this is my data and policy applies to other patient's data.
- b) Look in the electronic health records if explicitly permitted by policy.\*
- c) Use the patient portal or medical records department.\*
- d) Ask any doctor to look up my information.

### **Knowledge 23**

40. If a law firm requests patient information, I....

- a) Provide the information on a USB stick the supply.
- b) Print out the information for them.
- c) Allow them to view the information, but not have a copy.
- d) Contact medical records, security, supervisor, or other personnel as per policy.\*

### **Knowledge 24**

41. If a standard computer without encryption has a sensitive file that is purposefully deleted...

- a) I can be sure that it is gone as I emptied the computer trash container.
- b) Do not know if it is really gone.\*
- c) Definitely gone no matter what because I have password on my computer.
- d) Only gone once I reboot.

### **Knowledge 25**

42. It's acceptable to backup patient information to my personal cloud (Google Drive, Dropbox, iCloud, etc...) for safekeeping...

- a) If I make sure I use a strong password.
- b) If I delete the files when I'm done with them
- c) If I do not let anyone know.
- d) Never as this is not permitted.\*



**Knowledge 26**

43. If my coworker suspects someone must have looked at his/her health record due to gossip about his/her condition, I would...

- a) Assure my coworker that no one would have looked at the health records.
- b) Ask around who looked at the health records.
- c) Warn people not to look at coworkers' health information.
- d) Make an inquiry/report to corporate compliance or appropriate entity per policy.\*

**Knowledge 27**

44. If I cannot find my laptop/tablet containing sensitive information, I...

- a) Wait until the device turns up and possibly report later.
- b) Know it's secure because I need a password to log in.
- c) Know it's secure because I erased all of the sensitive information.
- d) Contact security, helpdesk or other entity as required by policy.\*

## Appendix K – Survey Raffle

Your information has been collected anonymously and kept separate from the drawing.

If you would like to be eligible for the \$250 Amazon gift certificate, enter your email address for the drawing. Your email address is not linked to your survey responses.

Thank you for participating.

\* Please enter your email address below.

Next