Evidence-Based Cybersecurity Awareness Toolkit

Mirsad Maglajlic, BSN, GSRNA

University of Saint Francis

NURS 785

June 15, 2020

I have read and understood the plagiarism policy as outlined in the course syllabus, the Nursing Student Handbook appropriate to my program of study and the USF Student Handbook relating to the USF Academic Integrity and Plagiarism Policy. By affixing this statement to the title page of my work, I certify that I have not violated any respect of the USF Academic Integrity/Plagiarism Policy in the process of completing this assignment. If it is found that I have violated any of the above-mentioned policy in this assignment, I understand the possible consequences of the act(s), which could include the dismissal from USF

Table of Contents

DNP Scholarly Project Final Approval Form

Abstract

In the last decade, the United States experienced the greatest number of targeted cyberattacks in the world and the healthcare industry became the most ransomware targeted industry in the country. Mobile devices infected with malware pose a security threat and may allow cybercriminals to exploit corporate servers, medical databases, and gain unauthorized access to protected health information (PHI). The consumers of healthcare services are frequently offered an easy and convenient way to access their electronic health records (EHR) online, however, they are not being educated as to how to perform this task safely. The identified practice-knowledge gap stems from the lack of awareness of the essential cybersecurity principles in keeping personal and mobile devices safe when accessing PHI. The focus of this DNP project was on quality improvement (QI) using a synthesis of the evidence-based guidelines issued by the cybersecurity branch of the federal government and private enterprises in the same field of study. The DNP project objectives were two-fold: the first objective was to train registered nurses (RN) and patients about the basic cybersecurity principles in keeping personal and mobile devices safe when accessing PHI and EHR online; the second objective was to incorporate an evidence-based cybersecurity awareness toolkit (EBCST) in the discharge routine on the medical-surgical unit. Due to COVID-19 restrictions on healthcare facilities in 2020 and subsequent inability to implement the DNP project in the clinical setting, a written project implementation plan was presented instead. The EBCST was delineated along with a proposed two-part implementation plan. Knowledge gained and change in RNs' perceptions related to cybersecurity principles were to be measured. Planned data analysis interpretation using IBM SPSS Statistics ver. 25 and a paired t-test were outlined and discussed.

Executive Summary

DNP Project Problem Statement

In 2017, the cost of an average cyberattack data breach to a U.S. company was $7.91 million. On a global scale, the United States experienced the greatest number of targeted attacks in the world, while the healthcare industry became the most ransomware targeted industry in the country (McAfee, 2018; Symantec, 2018) with a per capita cost of $408 per single medical record breach (Ponemon Institute LLC, 2018). In the State of Indiana nine hospitals, clinics, and healthcare centers were attacked by ransomware, causing disruption of healthcare services, financial losses, and breach of PHI (SecuLore Solutions, 2019). Historically, human error has been identified as the weakest link in the chain of all cybersecurity measures (Fisher, 2018; Greengard, 2017; Hadlington, 2017; Kim, 2017; King et al., 2018; McAfee, 2018). The consumers of healthcare services are frequently offered an easy and convenient way to access their EHR online; however, they are not being educated as to how to perform this task safely. The identified practice-knowledge gap stems from the lack of awareness of the essential cybersecurity principles necessary to keep personal and mobile devices safe when accessing PHI. Personal and mobile devices infected with malware pose a security threat and may allow cybercriminals to exploit corporate servers and gain unauthorized access to PHI (IBM, 2018; McAfee, 2018). A cultural shift is desperately needed in the medical IT world, where both providers and consumers are trained to take individual responsibility to secure their own personal and mobile devices in order to protect the EHR (Greengard, 2017; Kim, 2017; Kruse et al., 2017).

Scope of Project

The focus of this DNP project was on QI, creation of an EBCST that would be used to train RN staff and patients at AMH about the basic cybersecurity principles to keep personal and mobile devices safe when accessing PHI and EHR online, and incorporating the EBCST in the discharge routine on the medical-surgical unit.

Stakeholders

The main stakeholders of this project were the AMH senior leadership, participating staff RNs, and the healthcare service consumers (patients) who have in the past or will in the future receive medical services throughout the Adams Health Network.

Budget

The estimated budget for the DNP project was $1000 and it was fully funded by AMH. The budget consisted of direct expenses for the training of the medical-surgical unit RNs, the printing of educational materials, and the time spent on patient education during a two-week implementation period. Indirect expenses consisted of meetings with administration and a reservation of a conference room for the inservice that included a computer, PowerPoint software, and a large screen TV.

Implementation Facility IRB Approval

The senior leadership of AMH has determined that facility-specific IRB approval was unnecessary (Appendix B). The required training in human subject protection has been completed (Appendix A).

Methodology

The DNP project preparation steps consisted of initial and ongoing meetings with leadership personnel, approval, and printing of the EBCST, and establishing a list of participating medical-surgical RNs. For phase one of the DNP project, the staff inclusion criteria consisted of part-time and full-time RNs employed at AMH. Exclusion criteria consisted of nursing students, temporary agency nurses, and recently hired nurses still in training. For phase two of the DNP project, the patient inclusion criteria consisted of English-speaking adults, ages eighteen and older. The patient exclusion criteria consisted of patients with a new and life-altering diagnosis. The designated project location was the medical-surgical unit at AMH. The RN inservice was planned for thirty minutes and patient education was planned to be carried out over a two-week period. During the implementation phase two, participating RNs would use the EBCST to raise awareness and educate patients upon discharge as to how to secure personal and mobile devices from cyber-related attacks and malware prior to accessing EHR.

Risk Analysis, Informed Consent, Procedures, Participants Protection

The assessed risk for this DNP project is relatively low. The stakeholder's disinterest and lack of support risks were relatively low. The participating RNs' dropout risk during both phases one and two of the DNP project was low. The implementation failure risk was assessed to be at a low to moderate level and was attributed to a possibility of RNs' poor compliance and disinterest in the subject matter, patient disinterest in receiving EBCST education, and limiting factors such as the patient's literacy level. Per the consent form provisioned to be signed by participating RNs, the participation in this DNP project was voluntary without project-related financial compensation.

Implementation Methods, Instruments, Data Collection, and Confidentiality

Medical-surgical RN's knowledge and perceptions gained regarding the essentials on cybersecurity measures were planned to be measured via the pre- and post-tests (Appendix C, D). The pre-test would be administered and collected at the beginning and the post-test at the end of the inservice. Secondary data would be obtained via the collection of EBCST teaching records during phase two of the DNP project. RNs' long-term knowledge retention was planned to be assessed thirty days after the in-service via a second post-test planned to be administered electronically via the SurveyMonkey cloud-based service.

Chapter 1 Introduction

The twenty-first century is marked by rapid and profound advancements in all fields of science, including information technology. The invention and availability of electronic health records have revolutionized the way healthcare professionals provide care. The ability to quickly lookup a patient's health history, most recent hospital or primary care visit, current, and past laboratory findings, etc. has allowed for faster and easier delivery of medical services (Hussung, 2015). Protecting information technology (IT) infrastructure has become a necessary focus in the context of data security and the fight against cybercrimes.

In 2017, the cost of an average cyberattack data breach to a U.S. company was nearly eight million US dollars. It took an average of one hundred ninety-six days for the breach to be discovered (Ponemon Institute LLC, 2018). On a global scale, in 2017, the United States experienced the greatest number of targeted attacks in the world while the healthcare industry became the most ransomware targeted industry in the country (McAfee, 2018; Symantec, 2018). A significant increase of over 1,000 percent in cyber-related attacks on healthcare has been noted in early 2018 with a per capita cost of $408 per single medical record breach (Ponemon Institute LLC, 2018). In addition to ransomware, the number of uniquely identified malware threats has escalated from 0.13 to 8.4 million in the last decade, with an average of 996 malware specimens discovered every hour (G Data Software, 2018).

The State of Indiana has also witnessed a significant increase in the number of cyberattacks. In the last five years, nine hospitals, clinics, and healthcare centers in Adams, Allen, DeKalb, Hancock, Jefferson, and St. Joseph County were attacked by various types of ransomware (SecuLore Solutions, 2019). These cyberattacks had significant outcomes and were reflected in disruption of healthcare services, database and patient records breaches, financial losses in the thousands of dollars, or all of the above (SecuLore Solutions, 2019).

Problem

Problem Statement

The PICOT question for this Doctor of Nursing Practice (DNP) scholarly project reads as follows: (P) For hospital-employed medical-surgical registered nurses, (I) will implementation of an evidence-based cybersecurity awareness toolkit (O) increase knowledge of cybersecurity awareness principles (C) as compared to participant's prior knowledge.

Background of the Problem

Most healthcare institutions, including clinics, hospitals, pharmacies, labs, and nursing homes, offer their customers easy access to personal health information via a patient's online portal. A patient portal is defined as an online service that affords patients with "24-hour access to personal health information from anywhere with an internet connection" (ONC, 2017, para. 1). In 2017, fifty-two percent of healthcare consumers nationwide were offered online access to their medical records. Nearly one half accessed and viewed their records at least once, and one-third used an electronic device such as a smartphone or a tablet, in the process of doing so (Patel & Johnson, 2018). Despite the ongoing cybersecurity attacks on the healthcare industry, and exponentially growing malware threats on mobile devices (Symantec, 2018), presently, no standardized guidelines or policies exist that require or hold health providers accountable to educate the end-system users (patients) about basic cybersecurity principles when accessing the personal health information online.

Historically, from all possible threats that could compromise a data health network, human error has been identified as the weakest link in the chain of all cybersecurity measures

(Fisher, 2018; Greengard, 2017; Hadlington, 2017; Kim, 2017; King et al., 2018; McAfee, 2018). Most human errors are not based on ill-intent; instead, they occur due to either lack of awareness, forgetfulness, lack of technical training, and lack of understanding of computer equipment or devices (IBM, 2018). Also, corporate IT infrastructure is managed and maintained by IT experts, while personal devices are often operated by individuals without formal IT training. A lack of awareness and compliance with basic cybersecurity measures leaves the private and corporate world more vulnerable and exposed to hackers and cyberthieves (Kruse, Frederick, Jacobson, & Monticone, 2017; Olalere, Abdullah, Mahmod, & Abdullah, 2015).

Personal and mobile devices such as cellphones, iPads, tablets, and laptops, infected with malware pose a security threat and may allow cybercriminals to further exploit the corporate servers, medical databases, and gain unauthorized access to protected health information (PHI), i.e. patients’ personal, financial, and medical records (IBM, 2018; McAfee, 2018). Malware threat variants including spyware, ransomware, and viruses, targeting mobile devices specifically, have increased by 54 percent in 2017 (Symantec, 2018). A cultural shift is desperately needed in the medical IT world, where both providers and consumers are trained to take individual responsibility to secure their own personal and mobile devices in order to protect electronic health records (EHR) (Greengard, 2017; Kim, 2017; Kruse et al., 2017).

Practice and Knowledge Gap

The consumers of health care services are frequently offered an easy and convenient way to access their PHI online; however, they are not being educated as to how to perform this task safely. Therefore, a practice-knowledge gap stems from the lack of awareness of the essential cybersecurity principles in keeping personal and mobile devices safe when accessing PHI.

Assessment Needs

Summary of Necessity of the Project

Cybersecurity continues to be a concern for both the public and the private sector. Millions of taxpayer dollars are being spent on cybersecurity infrastructure and more costs are yet to come. Due to the very nature of the healthcare industry, the collection of a vast amount of personal client data, storage, and repositories of sensitive data in one central place, the healthcare sector will remain a major target of cyber-attacks. In order to expand the scope of cyber-protection within the healthcare industry, the protection of PHI at the healthcare consumers' level is also needed. An EBCST can be used as a potential solution for raising awareness amongst the healthcare staff as to how to secure personal and mobile devices from cyber-related attacks and malware.

DNP Project Overview

Scope of Project

The DNP project is focused on synthesizing an EBCST that will be used to train medical-surgical unit registered nurses (RN) at Adams Memorial Hospital (AMH), charged with the responsibility of discharging patients home. A minimum desired number of participating RNs for the pilot phase is eight to ten. Upon completion of the evidence-based cybersecurity training, participating RNs will be qualified to raise awareness and educate patients on how to keep their personal and mobile devices safe. The U.S. government and private cybersecurity enterprises have published essential guidelines on this topic. Recommended steps that must be taken to secure a personal computer or a mobile device include: keep the firewall turned on, install or update antivirus software, install or update the antispyware technology, keep the operating system up to date, be careful when downloading, and turn off the computer when not in use (FBI, 2016). These essential guidelines on cybersecurity measures have been incorporated in the EBCST.

Stakeholders

The main stakeholders of this project include the AMH senior leadership, including the chief nursing officer (CNO), the director of support services, and a mid-level manager of the medical-surgical and intensive care units. Clinical personnel consisting of RNs on the medical-surgical unit who are full-time or part-time employees will also be included. Finally, at the end of the chain, are the end-system users, meaning the healthcare service consumers or patients who have in the past or will in the future receive medical services throughout the Adams Health Network.

Budget and Resources

Cost

The projected DNP budget consisted of direct expenses including the expense for training the medical-surgical unit RNs, printing the EBCST and EBCST patient education records, time required to take a pre- and a post-test upon completion of the training, second post-test four weeks after the training, and the time medical-surgical RNs will invest in teaching patients about the EBCST at the time of discharge during a three-week project piloting phase. Indirect expenses included meetings with leadership personnel and director of support services. The extrapolated DNP project budget was one-thousand US dollars (Appendix A). Adams Memorial Hospital senior leadership agreed to cover all project expenses.

Description of Resources

The implementation facility was the AMH medical-surgical unit. No special or additional resources were needed for this project besides a reservation of a conference room for training purposes. Conference rooms were equipped with a computer, a projector, and a microphone with a lectern.

Process and Outcomes

General Timeline

The objective of this scholarly project was to incorporate an EBCST in the discharge routine on the medical-surgical unit. General preparations for the implementation phase took place in Fall 2019. Preparation measures consisted of initial and ongoing meetings with leadership personnel, finalization, approval, and printing of the EBCST, and establishing a list of participating medical-surgical RNs. The actual implementation phase was scheduled for Spring 2020 and was planned to be carried out over a two-week period.

Setting and Target Population

The DNP project participant's inclusion criteria consisted of part-time and full-time RNs employed at Adams Health Network. Exclusion criteria consisted of nursing students obtaining clinical training at AMH, temporary agency nurses, and recently hired nurses who were still in training or orientation. Patient inclusion criteria consisted of English-speaking adults, ages eighteen and older. The total planned participation time requirement for the participating RNs included thirty-minutes for the training session, ten to fifteen minutes for a pre- and post-test, and approximately three to four minutes of cybersecurity education time per patient per discharge during the implementation phase of the project. In addition to two tests and patient education, participating RNs were provisioned to fill out an EBCST education record daily (Appendix B). The EBCST education record consisted of two data entries; first was a number of daily EBCST teachings performed; second was the number of patients' refusals to receive the EBCST education. If a patent refused the EBCST education, the discharging RN would document the patient's refusal on the EBCST teaching record. Participating RNs would be instructed to place completed teaching records in a designated, reserved, and properly labeled and secured (locked) bin at the main nurse's station on the medical-surgical unit. Teaching records would be collected weekly by the DNP project manager, digitalized and saved in an encrypted folder in the cloud. Original records would be shredded immediately after digitalization. No identifiable information would be collected on participating RNs or patients.

Expected Outcomes Described

The outcome objectives of this project were educational in nature and were directed at raising awareness, providing education, and increasing understanding of evidence-based cybersecurity awareness principles. Specific outcomes were to assess knowledge gained about the cybersecurity awareness principles after the completion of the in-service as compared to RN's prior baseline knowledge. The RN's attitudes and perceptions of the evidence-based cybersecurity principles in the context of keeping the personal and mobile devices safe when accessing the PHI online were planned to be evaluated via the pre- and post-test as well (Appendix C, D). Long-term knowledge retention was to be assessed via a second post-test administered a month after the in-service.

Data analysis was planned to be performed using the IBM SPSS Statistics ver. 25 software application. Disclosure of final data analysis and outcomes was planned to be disseminated in a final meeting with AMH leadership personnel and shared via email with RNs interested in the outcome of the study.

Risk Analysis

The assessed risk for this DNP project was relatively low. Potential risks included the stakeholder's disinterest to support the project, RNs dropout risk, project implementation failure risk, and unexpected project impact risk. The stakeholder's disinterest and lack of support risk was relatively low. The senior administration of AMH has accepted the proposed implementation of the DNP project in their facility and has signed the USF DNP Scholarly Project Team Agreement (Appendix E). Another potential risk was the RNs' dropout potential during both, phases one or two of the DNP project. The dropout risk was also low and could have occurred potentially in the event a participating RN was fired, resigned, or became ill during a part or the entire duration of the training or implementation period. A risk of implementation failure was also considered as a possibility. Potential reasons included ineffective inservice presentation, inability to reach project objectives due to participating RNs' poor compliance and disinterest in the subject matter, and on the extreme scale of things limited student access to implementation facility for unforeseen reasons. The implementation failure risk was assessed to be at a low to moderate level. Additionally, patient risks were also considered. Patients diagnosed with a new and life-altering medical diagnosis were assessed to be poor candidates for EBCST teaching. These patients were planned to be exempt during the piloting phase of this DNP project. Finally, factors like the patient's culture, literacy level, and preferred language were identified as potential impediments in providing effective education. The assessed risks were planned to be addressed through detailed planning, scheduled and follow up meetings with leadership and participating RNs during the preparation, training, and implementation phase of the project. The participation in this project was voluntary. Aside from their normal work hours, participating RNs were not planned to be reimbursed financially or in any other capacity for the services rendered or their time spent on this project. A written consent was planned to be discussed and signed by each participating RN on the day of the inservice (Appendix F).

Finally, the COVID-19 pandemic outbreak was an unanticipated risk. The pandemic lead to Indiana's stay-at-home order while students' access to clinical facilities was severely limited. AMH senior leadership paused nonessential community engagements including the implementation of any DNP projects in their facility. As a result, a written DNP project implementation plan was presented instead.

Chapter 2 Synthesis of Supporting Evidence and Project Framework

Relevant Theory and Concepts

Havelock's theory of change is a modification of Lewin's change theory. Compared to Lewin's theory that outlines three phases of change, Havelocks' theory proposes six stages of change with an additional stage zero, also known as the care stage. The six sequential stages of change include relationship, diagnosis, securing recourses, identifying solutions, extending, and accepting the change, and lastly the maintenance and renewal stage (White et al., 2016).

A pre-stage, also known as the step zero or care stage is a unique stage in Havelock's theory. Step zero reflects an awareness of the existing problem or concern. During this stage, one acknowledges for the first time that a problem exists. It is also the first occurrence of concern with no actionable remedies. Step zero represented the most important milestone for this DNP project. In 2017, at least one in seven mobile device owners were a victim of cyberattacks (Allot Communications, 2017), and in the same year, the healthcare industry became the most ransomware targeted industry in the United States (McAfee, 2018; Symantec, 2018). If this problem was not acknowledged and agreed upon by AMH senior administration, it may have been very challenging if not impossible to successfully translate this DNP project into clinical practice.

The first step in Havelock's theory of change is the relationship phase. Havelock postulated that in order to elicit a change, a meaningful relationship must be established between all parties and should be rooted in open and bidirectional communication (Myers, 2017). The second step reflects the examination or diagnosis phase. During this phase, it is explored and ascertained whether the perceived need for a change is welcomed or even desired. If the process of change survives the diagnosis phase, it transitions to the third step which consists of information gathering and obtaining resources pertinent to the concept of change. A viable solution is identified, selected, and implemented during the fourth stage of the process. The fourth stage of this DNP project consisted of raising awareness and increasing knowledge among the medical-surgical RNs about the essential cybersecurity principles. The cycle of change, however, is not considered successful until it passes the fifth step of Havelock's theory of planned change (White et al., 2016). During this step, the new information is disseminated throughout the entire organization until it overcomes the initial resistance and becomes widely accepted. Finally, the last step involves a suitable level of supervision as well as a continuous renewal and the maintenance of the newly achieved level of change. It is during this final step of the process, that the change becomes fully integrated within an organization (Myers, 2017).

Integration of Project Framework with Supporting Evidence and Literature

An exhaustive review of the literature related to cybersecurity was conducted by searching multiple databases including Campbell Collaboration Library of Systematic Reviews, Cochrane Database of Systematic Reviews, EBSCO databases, TRIP Database, CINAHL Plus, Emcare (Ovid), Google Scholar, PubMed (Medline), ProQuest databases, as well as the National Guideline Clearinghouse and Directory of Open Access Journals. Relevant cybersecurity and cybercrimes data reports were obtained from the federal bureau investigation (FBI) public repositories. Over thirty relevant search terms were identified. The most commonly occurring terms were cybercrime, cyberliteracy, cybersecurity, cyberthreats, data security, digital health, information technology, theft, identity theft, prevention and control, and portable devices. Literature review was narrowed down through additional inclusion criteria consisting primarily of six search terms including control, awareness, defense, prevention, security, and skills. Over two hundred literature pieces, including both articles and reports were reviewed. Eighty-five articles have received a detailed review. A final literature pool consisted of fifty-six articles and reports being included for the purpose of the DNP project.

Summary of Supportive Evidence

Types of Security Threats

Vast majority of security threats can be classified into nine different categories such as the brute-force and dictionary attacks, cross-site scripting (XSS), denial-of-service attacks, malware attacks, man-in-the-middle (MITM) attacks, phishing attacks, spear-phishing attacks, SQL injection attacks (SQLi), and whaling phishing attacks (CISCO, 2019; Herjavec Group, 2019; McAfee, 2018; Symantec, 2019). The most commonly encountered threats have been identified as phishing attacks; phishing is defined as an illicit attempt to gain access to sensitive data i.e. username, password, social security number, bank account information, etc. by digitally camouflaging or obscuring online identity when engaging in electronic or other types of digital communication (IBM, 2018). Finally, the health industry has also been threatened with a newer type of cyber-attacks, commonly known as ransomware (Pope, 2016). Ransomware is primarily used by cybercriminals to encrypt sensitive data on a target device i.e. a corporate server, EHR system, personal computer, portable device such as a cellphone, and then seek a payment of ransom (Savage, Coogan, & Lau, 2015). Aside from financial extortion, ransomware also poses a significant obstacle in providing quality patient care by limiting access to EHR, electronic billing and online payments, corporate emails, and even facility voice-over-ip phone systems (Paul, 2017; Pope, 2016). In the last five years, ransomware attacks were the sole cause of financial havoc and disruption of healthcare services in over nine hospitals, clinics, and outpatient centers in Adams, Allen, DeKalb, Hancock, Jefferson, and St. Joseph County (SecuLore Solutions, 2019). This DNP project directed at translating the evidence-based practice as it relates to cybersecurity with an objective to educate the medical-surgical RNs and patients to take individual responsibility and secure personal and mobile devices as a measure in protecting the EHR (Greengard, 2017; Kim, 2017; Kruse et al., 2017).

Why Cybercriminals Target the Healthcare System

Several reasons have been identified as to why the healthcare industries became a major target for cyber-criminals. The two most common reasons are the collection, storage, and availability of vast amounts of personal data in one place, i.e. on a corporate data server, and the second reason is the financial gain through exploitation of medical and personal information, including medical and personal identity thefts (Herjavec Group, 2019). A significant increase of over one thousand percent in cyber-related attacks on healthcare has been noted in early 2018 with a per capita cost of four-hundred-and-eight US dollars per single medical record (Ponemon Institute LLC, 2018). McAfee (2018) and Symantec (2019), global computer security software companies in the United States, emphasized that cybercrimes are likely to continue in this path as cybercriminals are technologically sophisticated and committed, even more so than most advanced IT companies. And finally, “since many technology users fail to take the most basic protective measures” in securing their personal and mobile devices, the internet-related crimes will continue to grow and simply remain “too easy and too rewarding” for cybercriminals to even slow down (McAfee, 2018, p. 3). A DNP project like the EBCST is only the first step in the right direction. Ongoing effort is certainly required from DNP graduates to translate and disseminate evidence-based knowledge as it relates to cybersecurity principles and the protection of PHI and EHR.

How Are Healthcare Industries Protecting EHR

The modern EHR systems offer far-reaching capabilities, including remote access for medical providers, either via a personal computer, or a mobile device, including a cell phone. Since the innovation of the iPhone in 2007, the usage of mobile devices has exponentially grown, and so did the concept of staying connected twenty-four-seven with the world-wide-web. From this event onward, the appetite of amateur and professional hackers has risen exponentially, as evidenced by the rise in the number of uniquely identified malware threats from 0.13 million in 2007 to 8.4 million in 2017 (G Data Software, 2018; McAfee, 2018).

Corporations and institutions implement on average three levels of security measures to protect consumers' EHR. The first one involves sustainable supervision of the EHR system through regular system audits and development of contingency plans; the second security measure reflects the physical access restrictions via the hardware and software alternatives; and the third level of security is the protection of electronic health data within the organization, i.e. firewalls, user access, etc. (Kruse, Smith, Vanderlinden, & Nealand, 2017). Additionally, most organizations rely on their own, in-house IT specialist to update and maintain either a part or all of the IT-related equipment, including individual computer stations, mobile devices, corporate servers, and network storage devices (Harman, Flite, & Bond, 2012). Additionally, reports from the Center for Internet Security (2017) have also identified some common areas of vulnerability, including outdated IT infrastructure, lack of firmware updates, and lack of software updates.

The protection of PHI also includes the protection of personal and mobile devices utilized to access the EHR (Herjavec Group, 2019). In 2017, after a mobile device cyberattack, twenty-six percent of users have reported contacting the security app vendor or service provider while over thirty-five percent contacted no one (Allot Communications, 2017). This DNP project aimed to raise awareness and educate the medical-surgical RNs about the cybersecurity principles via the EBCST. A long-term objective was to integrate the EBCST as permanent part of the discharge routine in the healthcare setting.

Chapter 3 Project Design

Methodology

The DNP project was primarily directed toward quality improvement (QI) using a synthesis of the evidence-based guidelines issued by the cybersecurity branch of the federal government and private enterprises in the same field of study. The objective was to incorporate an evidence-based cybersecurity toolkit (EBCST) in the discharge routine on the medical-surgical unit.

Project Design Plan

This Doctor of Nursing Practice scholarly project aimed to review and translate the evidence-based standards of practice relevant to the preservation of data security as it relates to the EHR and utilization of personal and mobile devices. The evidence-based practice guidelines and recommendations were synthesized and summarized in an EBCST. The project was planned to be piloted on the medical-surgical unit with eight to ten participating RNs. The project was planned in two phases. Phase one included an educational inservice for the participating RNs and phase two was provisioned for EBCST patient education at the time of discharge. During the two-week project implementation phase, RNs who received the inservice on EBSCT and were tested via the pre- and post-test, would raise awareness and introduce the EBSCT to patients at the time of discharge from the medical-surgical floor.

Ethical Considerations

In order to meet the academic and scholarly requirements of the program curriculum and the DNP project, the required training in human subject protection has been completed (Appendix G). A review of the DNP project by the senior leadership of Adams Memorial Hospital has determined that facility-specific institutional review board (IRB) approval is unnecessary (Appendix H). IRB approval from the University of Saint Francis was granted in October 2019 (Appendix L). The risk analysis component of this DNP project has been discussed in chapter one.

Project Schedule

The objective of this scholarly project was to incorporate an EBCST in the discharge routine on the medical-surgical unit. Preparations for the implementation phase one and two commenced in Fall 2019. Preparation measures consisted of initial and ongoing meetings with leadership personnel, approval, and printing of the EBCST, establishing a list of participating medical-surgical RNs and reserving a conference room for the training of the participating RNs. The implementation phase was scheduled for Spring 2020. Phase two project implementation was to be carried out over a two week period (Appendix M). Due to COVID-19 pandemic restrictions, the DNP project was never implemented. A written implementation plan was presented instead.

Implementation Methods

The DNP project was planned to be implemented in two phases. Phase one was scheduled in the second week of January 2020. During phase one, the medical-surgical RNs would be introduced to basic concepts of cybersecurity measures and commonly encountered cybersecurity terms. Cybersecurity-related events in local and neighboring counties as well as the reasons and the necessity for the implementation and integration of an EBCST were planned. All information, statistics, and data discussed during the in-service would be displayed on a large projector screen using PowerPoint. By the end of the inservice, the participating RNs would be able to identify the essential cybersecurity principles in keeping personal and mobile devices save when accessing EHR. Additionally, all participating RNs would receive the EBCST pamphlet (Appendix N) and EBSCT teaching record (Appendix B). Both the EBCST pamphlet and EBSCT teaching record would be added to the discharge packet of each patient on the medical-surgical unit during the implementation of phase two of the DNP project. The objective of the phase one in-service was for the participating RNs to become familiar with EBCST and evidence-based guidelines in securing personal and mobile devices from cyber-related attacks and malware threats.

Phase two of the DNP project provisioned for the medical-surgical RNs to raise awareness and educate patients at the time of discharge as how to secure personal and mobile devices from cyber-related attacks and malware threats. Phase two implementation was scheduled to begin in the third week of January 2020 over a two-week period. The medical-surgical RNs would provide a copy of the EBCST pamphlet to patients at the time of discharge from the hospital and educate them about it. Following each patient discharge, the medical-surgical RN would fill out the EBCST teaching record and place it in a secured, designated box, located at the main nurse's desk. The unit clerk would place in advance a copy of an EBCST teaching record inside every discharge packet on the medical-surgical unit.

Measures, Tools, Instruments

Medical-surgical RN’s knowledge and perceptions gained regarding the essentials on cybersecurity measures were planned to be measured via the pre- and post-tests (Appendix C, D). Due to uniqueness and the specificity of the topic of this DNP project, no relevant and or published measurement scale was found that could assess the desired outcomes. A self-created instrument was designed instead. The instrument mimics primarily the Likert scale format and encompasses a total of 15 questions. The top portion of the survey asked for basic demographic information. The second part of the survey asked questions in the Likert format to evaluate how much knowledge and understanding has been gained about the evidence-based cybersecurity guidelines in the context of keeping the personal and mobile devices safe and secure when accessing EHR.

Evaluation Plan

Methods for Collection of Data.

The participating medical-surgical RNs baseline knowledge and perceptions would be assessed via a pre-test. A pre-test would be administered at the beginning of the in-service. The knowledge gained about the cybersecurity and change in perceptions would be assessed via a post-test. The post-test would be administered at the end of the in-service. Both tests would be administered in-person and in a hard-copy format. Tests would be collected by the project manager immediately upon completion. Long-term knowledge retention was planned to be assessed thirty days after the in-service via the second post-test that was planned to be administered electronically via the SurveyMonkey cloud-based service. The participating RNs would receive a link and a reminder for the second post-test via email. Participating RNs would be allocated up to two weeks to take the second post-test. After two weeks have elapsed, the provided link would expire.

In addition to pre- and post-tests, the participating RNs would be collecting and recording data on two variables daily (Appendix B). One variable is a number of EBCST teachings performed. If a patent refuses the EBCST education, the participating RN will indicate a patient's refusal on the EBCST teaching record (Appendix B). The participating RNs would be instructed to place teaching records in a designated, labeled, and secured bin at the main nurse's desk on the medical-surgical unit. Teaching records would be collected weekly by the DNP project manager, digitalized and saved in an encrypted folder in the cloud. Original records would be shredded immediately after digitalization. Additional inclusion criteria considered for the patient education record sheet were the documentation of the current date, circling yes or no to indicate whether the EBCST teaching was provided, and if applicable, annotating the reason for patient refusal to receive EBCST education.

Personal identifiers would not be collected on RN participants or patients receiving EBCST education and no manipulation would be employed at any given instance during the preparation or implementation phase of the project.

Data analysis plan.

Data analysis would be performed using the IBM SPSS Statistics v.25 software application. Initially, a comparison of the results would be made between the pre- and post-tests administered during the in-service. A paired t-test would be employed for this purpose and a statistical difference would be ascertained with a p-value of less than 0.05. The objective of this analysis was to learn if knowledge has been gained as a result of the educational in-service provided and if the change is statistically significant. An additional comparison would be made between the first and second post-tests utilizing the paired t-test once again.

Dissemination plan.

Disclosure of the final data analysis and project outcomes would be disseminated in a final meeting with AMH leadership personnel as well as during a formal presentation at USF. A verbal and written Executive Summary would be shared with the DNP project facility and stakeholders. A PowerPoint presentation could be utilized as a visual aid in the academic setting, while a hardcopy of the final data analysis was planned to be provided and utilized during the final meeting with AMH senior leadership. Data interpretation would also be shared via email in a PDF format to the participating medical-surgical RNs at AMH interested in the outcome of the study.

Chapter 4 Results and Outcomes Analysis

Data Collection Techniques

Due to COVID-19, DNP project implementation was not possible. Per the implementation plan, the primary research data would be obtained via the pre- and post-test during phase one of the DNP project. The pre-test would be administered and collected at the beginning and the post-test at the end of the inservice. Both tests are designed to be administered in a hardcopy format. Secondary data would be obtained via the collection of EBCST teaching records during phase two of the DNP project. Per the implementation plan, the RN who is discharging the patient home would fill out an EBCST teaching record and placed it in a properly labeled and secured bin at the main nurse's station on the medical-surgical unit. Only the project manager would have a key to open the secure bin and collect EBCST teaching records. The bin would be emptied once a week, on Fridays.

Measures/Indicators

The pre- and post-tests would be administered to the same group of participating RNs. Per the implementation plan, both tests would have an identical set of seven questions in a six-point Likert scale format. Three questions would assess RNs' perceptions. The remaining four questions would appraise RNs' knowledge and understanding of the cybersecurity measures. The pre-test would also include additional questions about RNs' demographics, employment status, number of personal devices owned, number of personal devices currently protected by antivirus software, and RNs' individual preferences between privacy, security vs. convenience of device utilization.

Data Analysis Inferences

The primary goal of data analyses would be interpreted in two ways: first assessing the knowledge gained and change in RNs' perceptions as it relates to cybersecurity measures; the second interpretation would be focused on measuring RNs' compliance in teaching the essentials of EBCST to patients at the time of discharge. The first goal would be accomplished through data analysis obtained from the pre- and post-tests. The assessment of RNs' compliance in teaching the essentials of EBCST would be evaluated through data analysis obtained from EBSCT teaching records.

Assessment of Knowledge Gained and Perception Changes

IBM SPSS Statistics ver. 25 software would be employed as the main tool for statistical analysis of the data obtained. Parametric inferential statistics and a paired t-test would be selected to compare the means of pre- and post-test scores. A total of fourteen SPSS variables would be created, one for each of the seven pre-test and seven post-test questions. Each variable would be appropriated one of the suffix letters: letter "K" indicating a knowledge question and letter "P" indicating a perception question. For instance, the variable "Pre_Q1_P" would represent a pre-test question number one, assessing RN's perception as it relates to cybersecurity measures. Each variable would be assigned a total of six value labels, one for each point on the

Likert scale, i.e., 0=not at all, 1=strongly disagree, 2=disagree, etc. Pre-test and post-test data values would be entered accordingly. Four variables would then be computed using the SPSS "Compute Variable" function: pre-test knowledge "Pre_K", pre-test perceptions "Pre_P", post-test knowledge "Post_K", and post-test perceptions "Post_P". Finally, a comparison of means would be calculated using the SPSS Paired-Samples t-test for the variables "Pre_K" vs. "Post_K", and "Pre_P" vs. "Post_P". In the Paired Samples Statistics output column, differences in mean values between variables would be noted. Within the third part of the output labeled "Paired Samples Test", the two-tailed significance level p values would be noted. A test would be considered statistically significant with p values <0.05.

Assessment of EBCST Teaching Compliance

IBM SPSS Statistics ver. 25 software would be employed as the main tool for statistical analysis of the data obtained. Nonparametric inferential statistics and a one-sample, Goodness of fit Chi-Square test would be selected to analyze the compliance of RNs in teaching the essentials of EBCST to patients at the time of discharge. For this test, a single SPSS variable would be created, and two value labels would be assigned, one for each point on the Likert scale, i.e., 0=No and 1=Yes. Data values obtained from EBSCT teaching records would be entered accordingly. Finally, the Goodness of fit Chi-Square test would be calculated comparing the frequency of "Yes" vs. "No" responses from RNs. The significance level p would be noted and the null-hypothesis would be rejected with a p <0.05. A rejected null-hypothesis would also be indicative of discharging RNs being compliant in teaching the essentials of EBCST to patients upon discharge from the hospital.

Gaps

A gap analysis was not possible due to a lack of project data and the inability to implement the DNP project as a result of Covid-19 restrictions on healthcare facilities and limited student access to the project implementation site.

Unanticipated Consequences

The unanticipated consequence in the context of data analysis is directly related to the lack of opportunity to implement the DNP project. Consequently, data was not collected, and analyses were not able to be performed. The planed data analysis steps outlined in this chapter would have been the steps taken to critically study and interpret the project data outcomes.

Expenditures

The SPSS computations would have been conducted by the project manager. Additional assistance would have been solicited from the DNP project advisor and DNP project faculty members. No additional costs would have been encountered as it relates to data analysis.

Chapter 5 Leadership And Management

Organizational Culture

Organizational culture can be defined as a set of ethical, behavioral, and emotional standards that influence positively or negatively employees of a healthcare organization (Grossman & Valiga, 2017). Organizational culture is a powerful tool that can be utilized to move the entire institution forward, the employees and the leadership alike. In other words, the organizational culture is a medium for expression by which an organization shares and nurtures its core values (White, Dudley-Brown, & Terhaar, 2016).

Adoptive cultures lead organizations to success and often determine the organization’s productivity, growth, and overall performance (Grossman & Valiga, 2017). The organizational culture at Adams Memorial Hospital was patient-centered, taught its employees to serve with compassion and excellence, taught to maintain a safe environment for patients and employees, and to treat each other with respect, and compassion (Adams Health Network, 2019). The senior leadership at Adams Memorial Hospital maintained a work culture that was open to change and process improvement, maintained clinical competency of their employees, and was driven clinically through evidence-based practice. A chain of command was clearly delineated while individual positions had specific titles and scope of practice clearly defined. Adams Memorial Hospital senior leadership personnel, including the chief nursing officer as well as the manager of the medical-surgical unit, had expressed interest in supporting this DNP project to its full completion.

Change Strategy

Change strategies can play an important role during the planning and successful implementation of a DNP project. Human resistance may be viewed as one of the most commonly occurring, and difficult to anticipate, encounters in various phases of a project. Human resistance may occur due to four reasons, including "a desire not to lose something of value, a misunderstanding of the change and its implications, a belief that the change does not make sense for the organization, and a low tolerance for change" (Kotter & Schlesinger, 2008). Project managers need to be aware of the human resistance phenomenon and have a clear change strategy in place to address issues of this nature. At Adams Memorial Hospital, the potential of human resistance was relatively low but certainly possible. The cybersecurity toolkit was entirely based on evidence-based research and was congruent with the mission values and believes of this organization.

Havelock's theory of change was selected as the theoretical model of change for this DNP project. Compared to Lewin's theory that outlines three phases of change, Havelocks' theory proposes six stages with an additional stage zero, also known as the care stage. The six sequential stages of change include relationship, diagnosis, securing resources, identifying solutions, extending and accepting the change, and lastly the maintenance and renewal stage (White et al., 2016). All six stages of change are essential for the successful implementation of a scholarly DNP project. The care stage, however, was regarded as the most important step in the process of change. Care stage mirrored the awareness of an existing problem or concern. During this stage, one acknowledges for the first time that a problem exists. Senior leadership of Adams Memorial Hospital has acknowledged that cybersecurity breaches represent a real threat to the healthcare industry. Implementation of the evidence-based cybersecurity toolkit was congruent with Adams Memorial Hospital's mission, values, and beliefs.

Leadership Style

DNP Essential II addresses organizational and systems leadership. An APRN is empowered through this essential to collaborate with many health and political entities in the context of improving the US healthcare system, i.e. local or state-wide healthcare policies, procedures, etc. In order to address the present and future challenges in healthcare, a DNP graduate needs to clearly differentiate between two concepts; namely the concept of management vs. leadership. Grossman & Valiga (2017) summarized the main differences between a manager and a leader, stating that a leader is a visionary, exerts creativity and innovation, and the leadership power is derived primarily from "knowledge, credibility, and ability to motivate followers", while a manager is mostly concerned with maintaining the order of business, focuses on short-term goals, facilitates “efficiency”, and the manger’s power mostly “arises from one’s position of authority” (p. 21). This does not mean that an APRN does not share both leadership and managerial qualities. A DNP graduate can teach, educate, advise, manage, and lead in this regard. However, the best utilization of an APRN’s time investment is to assume leadership roles and positions in society.

According to DNP Essential VI, a nursing DNP graduate is an expert in building effective teams and alliances in the context of a complex culture and a “complex environment“; furthermore, a DNP nurse is trained to engage on a multilevel scale in interprofessional dimensions of healthcare ("AACN," 2006). The challenges of this nature can only be addressed with a set of strong and sustainable, but also functional, leadership skills. Perhaps, the most important concept is a clear distinction and simultaneous interdependency between leadership and followership. In any well-established organization, corporation, and government agency, leadership cannot exist without followership, and vice versa. For instance, in the past, the leader has been allocated the central position and followers were always expected to conform to their leaders. The new concept, however, maintains that followers and leaders share the same platform of functioning, while the purpose, goal, vision, etc. is placed at the center of attention for all members of the organization (Grossman & Valiga, 2017). Adams Memorial Hospital administration adhered to the modern leadership style with the patient being at the center of attention. As a DNP scholar, I have used these leadership skills to fulfill the requirements set forth in DNP Essentials I – VIII. Furthermore, I have chosen the modern leadership concepts for the implementation of this DNP project.

Interprofessional Collaboration

DNP Essential VI addresses interprofessional collaboration as the means to not only improve the patient and population health outcomes but also to remove existing and potential barriers in this process. Grossman & Valiga (2017) stress that leaders are not born into this world and leadership skills are not genetically acquired. Instead, any person, male or female, can become a leader and still retain a level of flexibility i.e. switching between the leadership and followership roles as the situational demands change. More importantly, the concept of becoming a leader means to go through "stages of development", to exude a high level of commitment, vision, open-mindedness, mindfulness, self-reflection, and patients (p. 200).

One of the common barriers to participation in interprofessional collaboration is the notion that one must be formally assigned to a leadership position in order to lead. Grossman & Valiga (2017) debunk this myth by dissecting and comparing followership and leadership qualities. These two concepts are closely interrelated and codependent. A good follower can easily lead by example and positively influence others. A good follower can also be one of the most valuable assets in an organization, i.e. having specialty clinical skills as compared to other members of the team. In that context, a good follower's experience and feedback can make him or her an ideal candidate for an interprofessional collaboration team. Additionally, observational experiences alone are not enough to help a person acquire effective leadership and interprofessional collaboration skills. Rather, one develops these skills by engaging, practicing, "serving as a leader", and by actively seeking out opportunities to do so (Grossman & Valiga, 2017, p. 200).

Phase one of this DNP project was designed to provide education and clarify the participation guidelines to registered nurses on the medical-surgical unit. Phase two, however, allows the registered nurses to take charge and assume the leadership positions. Medical-surgical registered nurses will be teaching, but also empowering the patients at the time of discharge with knowledge on how to keep personal and mobile devices safe and secure when accessing personal electronic health records. This DNP project was to include a written communication for the initial pre- and post-questionnaires, and technology-related communication via email for the second post-test questionnaire utilizing SurveyMonkey a month later.

Conflict Management

Changes may give rise to many conflicts within a healthcare organization. Conflicts may be considered positive or negative. If understood and perceived correctly, conflicts have the potential to instigate new growth and development and help move the organization forward (Grossman & Valiga, 2017). Conflict avoidance may seem like an appropriate choice at first; however, on a long-term basis, conflict avoidance leads to a mental and or emotional strain among the team members and can also exude a negative influence on the care environment (Jacinta, 2006).

The probability of a serious conflict occurring during the preparation or implementation phases of the DNP project was low, as all team members have already voiced a strong interest in seeing this project to full completion. In case a conflict did occur, strategies like reflection, identification of the problem at hand, and mutual decision making could be employed. Conflict strategies like these could lead to a positive resolution, mutual agreement, personal and professional growth, and development of all members involved (Grossman & Valiga, 2017).

Implementation Plan

Due to the COVID-19 pandemic outbreak, limited student access to clinical sites, and the necessity to take reasonable precautions in limiting the spread of the viral illness, a written implementation plan has been created instead. The implementation site considered for this DNP project remains Adams Memorial Hospital in Decatur, Indiana. A written project implementation plan may be enacted at a later date when COVID-19 restrictions on the healthcare industry have been relaxed.

Preparation

All educational materials would be printed inhouse one week before the inservice. Printing tasks would be delegated by the med-surg manager to a unit clerk or a staff nurse in charge of education. The project manager would oversee the printing progress and provide assistance when needed. The person in charge of printing would compile thirty folders for phase one of the DNP project implementation. Each folder would contain the following:

- Pre-test; 2 pages
- PowerPoint presentation; 23 pages
- EBCST; 1 page, in color
- Patient teaching record; 1 page, on colored paper, i.e. red
- Post-test; 1 page

For phase two of the DNP project implementation, a copy of EBCST would be placed in eighty patient folders. At AMH, the premade discharge folders were kept at the main nurses' desk. Additionally, twenty-five patient teaching records would be placed at each of the four nurses' stations. A secure, drop-off box for EBCST teaching records would also be placed at each nurses' station. These tasks would be carried out in collaboration between the project manager and the person in charge of printing.

Participating Staff

The participating staff would consist of full-time and part-time registered nurses assigned to the medical-surgical. Agency nurses, nursing students, and nursing staff in training would be excluded from this study. The list of the nursing staff meeting the set criteria would be compiled and provided by the med-surg manager.

Phase One

The educational inservice would occur one time, either during a scheduled, mandatory monthly staff meeting or follow immediately after the meeting. The inservice would be presented by the project manager. The duration of the inservice would be thirty minutes. During the inservice, a pre-test, educational component, and a post-test would be delivered. Educational materials would be printed in advance and bundled in a folder that would include a pre- and post-test, a copy of an evidence-based cybersecurity toolkit, and PowerPoint presentation slides. Folders and pens would be readily available for participating RNs as they enter the conference room.

Pre-Test.

All participating RNs would be asked to fill out the pre-test at the beginning of the inservice. Educational presentation would commence immediately after the completed pre-tests have been collected by the project manager.

Education.

The educational component would be delivered in a PowerPoint format and displayed on a large screen TV. A question and answer session will be conducted at the end of the educational presentation. PowerPoint presentation would consist of twenty slides and would address the following:

- facts about the cyberattacks within the healthcare industry
- trends of EHR consumer access
- practice and knowledge gap related to EHR consumer access
- scope of the DNP project as it relates to cybersecurity
- a detailed but succinct explanation of the DNP phase two implementation, as well as the tasks required of participating RNs during phase two of this project

- Special attention will be devoted to the contents of the evidence-based cybersecurity toolkit.

Post-Test.

All participating RNs would be asked to fill out the post-test after the educational component has been delivered and leave the completed post-tests on the table, placed face-down. Post-tests would be collected by the project manager immediately after the participants depart from the inservice.

Phase Two

The second phase of the DNP project implementation was designed for the participating RNs to educate patients about the EBCST at the time of discharge. Phase two would be conducted over a two-week period and would begin on Monday, immediately following the phase one inservice. A participating RN who is discharging the patient home would take the EBCST pamphlet from the patient's discharge folder, present it to the patient, and discuss its content with over a reasonable period of time, i.e. three to five minutes. After the patient has been discharged home, the RN would fill out a teaching record card and place it in a designated and secured drop-off box. The teaching record cards and the drop-off box will be readily available at each nurses' station. The project manager would be in charge of collecting the accumulated teaching records once a week on Fridays. The project manager would also keep the line of communication open with the med-surg manager and participating RN staff via email or be available via the phone at least once a week.

Chapter 6 Discussion

Impact of Project

The EBCST would have been introduced as a measure for participating RNs to raise awareness and educate patients on how to keep their personal and mobile devices safe when accessing EHR. The senior leadership of Adams Memorial Hospital reviewed the proposed DNP project and agreed to conduct a pilot study on the medical-surgical and intensive care units. The EBCST printout was planned to be integrated in the discharge process during the pilot study. The CNO as well as the medical-surgical and intensive care unit manager advocated for a potentially long-term commitment as it relates to informing and teaching patients about cybersecurity essentials. While the Covid-19 pandemic ultimately impeded the implementation of the DNP project, the overall experience and collaboration had a very positive impact on this healthcare organization.

Decisions and Recommendations

The gained knowledge and the change in RNs' perceptions were originally intended to be measured on three separate encounters: a pre-test, a post-test, and a second post-test four weeks later. The second post-test was intended to assess RNs' long-term knowledge retention. A possible modification recommendation moving forward is to relinquish the second post-test, and instead, expand the number of knowledge-based and perception-based questions on the pre- and post-test. Choosing an alternative implementation site with a greater number of RNs per unit may provide a greater number of participating RNs and subsequently a greater number of acquired pre- and post-test responses.

Limitations of the Project

Some limitations have been identified over the course of the project. The limited number of participating RNs on the medical-surgical and intensive care unit in a community hospital may yield a limited number of responses on the pre- and post-test for an optimal data analysis. Additional limiting factors are related to implementation site project approvals and decision-making processes. Responses for project approval and or project modifications in a community hospital setting may take longer due to the lack of specialized committees or infrequently scheduled senior leadership meetings.

Application to Other Settings

The piloting phase of this DNP project was originally planned to be implemented on a medical-surgical unit, however, in collaboration with AMH senior leadership, the project was modified to include the intensive care unit also. After a successful implementation of the piloting phase, the collected data would have been studied and analyzed. The project could have been expanded to other hospital units, i.e. acute care settings where patients are being given access to their personal EHR, including the emergency room, outpatient surgery center, and affiliated primary care offices.

Strategies for Maintaining and Sustaining

A major driving force and simultaneously an impediment to a long-term project integration is linked to the willingness of the senior leadership to support a DNP project. In the light of the Covid-19 pandemic, the approval for the implementation of the proposed scholarly DNP project at a later time was welcomed and afforded by the senior leadership of Adams Memorial Hospital. Pursuing the implementation of the project at a later time may facilitate a permanent integration of the EBCST in the discharge procedures at Adams Memorial Hospital. A follow-up meeting and discussion about the implementation challenges, encountered roadblocks, feedback from participating RNs, and senior leadership may also aid toward the sustainability of this project.

Lessons Learned

A DNP scholarly project is a multistep process. An exhaustive literature review and a succinct summary of evidence-based guidelines on the subject matter has proven beneficial in getting a message across and gaining the support from hospital administration and RN staff alike. A clearly delineated project timetable has been essential in advancing the scholarly project. Additionally, the project timetable may have to be modified over the course of the project for many reasons, including delays in project approvals, meeting cancellation, etc. The project manager can address the anticipated and help mitigate the unanticipated project impediments through collaboration and leadership skills as well as by practicing the Eight Essentials of Doctoral Education for Advanced Nursing Practice.

Chapter 7 Conclusion

Potential Project Impact on Health Outcomes Beyond Implementation Site

At the time the DNP project was written, no similar DNP project was found in any of the DNP repositories and online databases. Historically, from all possible threats that could compromise a data health network, human error has been identified as the weakest link in the chain of all cybersecurity measures (Fisher, 2018; Greengard, 2017; Hadlington, 2017; Kim, 2017; King et al., 2018; McAfee, 2018). Most human errors are not based on ill-intent; instead, they occur due to either lack of awareness, forgetfulness, lack of technical training, and lack of understanding of computer equipment or devices (IBM, 2018). In the light of ongoing cybersecurity threats on the healthcare industry and the consumers of healthcare services, the scholarly project was aimed at raising awareness and educating both providers and consumers about evidence-based guidelines in securing personal devices as a safety step in preserving and protecting the EHR. The proposed DNP project is applicable to any healthcare organization that offers healthcare consumers online access to electronic health records.

Health Policy Implications of Project

A health policy sets the objectives to be pursued as well as the means to achieve and implement those objectives (White, 2016). Cybersecurity measures related to the safeguarding of electronic health records and protected health information are essential for both the healthcare service providers and consumers (Ponemon Institute LLC, 2018). Health policy represents a vital component in translating and integrating evidence-based research into clinical practice. The integration of an EBCST in the discharge process, i.e. in a hospital setting, primary care office, emergency room, etc. aids in educating patients and providers as well as disseminating the essential knowledge about the evidence-based recommendations in keeping the personal and mobile devices safe when accessing EHR online.

Proposed Future Direction for Practice

The lack of published DNP projects related to evidence-based cybersecurity measures in the context of raising awareness and educating the healthcare providers and consumers is concerning. A lack of awareness and compliance with basic cybersecurity measures leaves the private and corporate world more vulnerable and exposed to hackers and cyberthieves (Kruse, Frederick, Jacobson, & Monticone, 2017; Olalere, Abdullah, Mahmod, & Abdullah, 2015). Doctoral prepared advance practice nurses are in a suitable position to take a lead on this issue, form committees, engage at a local, state, and federal level, and establish healthcare policies that help reduce the gap between the evidence-based research and clinical practice. Additional research is needed to learn more about the effective methods of implementation and dissemination of the EBCST within the healthcare industry.

References

Adams Health Network (2019). Our mission and vision. Retrieved from https://adamshospital.org/

Allot Communications. (2017). *Allot MobileTrends Report*. Retrieved from https://www.allot.com/resources/MobileTrends_Consumer-View-on-Mobile-Security.pdf

Center for Internet Security. (2017). *Ransomware: In the healthcare sector*. Retrieved from https://www.cisecurity.org/blog/ransomware-in-the-healthcare-sector/

CISCO. (2019). What are common cyberthreats. Retrieved from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

CISCO. (2019). What Is cybersecurity. Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cybint Solutions. (2019). Ten most important cyber security tips for your users. Retrieved from https://www.cybintsolutions.com/10-important-cyber-security-tips-users/.

FBI. (2016). Cyber Crime. Retrieved from https://www.fbi.gov/investigate/cyber

Fisher, D. (2018). Medical practices must be proactive with cybersecurity. *Urology Times*, *46*(4), 38–39. Retrieved from https://search-ebscohost-com.ezproxy.sf.edu/login.aspx?direct=true&db=rzh&AN=128959150&site=ehost-live&scope=site

G DATA Software AG. (2018, March 27). Malware numbers 2017. Retrieved from https://www.gdatasoftware.com/blog/2018/03/30610-malware-number-2017

Greengard, S. (2017). Safe and sound: Addressing the risks of health care in a connected world. *Physician Leadership Journal*, *4*(6), 16–21. Retrieved from https://search-ebscohost-com.ezproxy.sf.edu/login.aspx?direct=true&db=hbh&AN=125811852&site=ehost-live&scope=site

Grossman, S., & Valiga, T. M. (2017). *The new leadership challenge: Creating the future of nursing* (5th ed.). Philadelphia: F.A: Davis Company.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3*(7). doi:10.1016/j.heliyon.2017.e00346

Harman, L. B., Flite, C. A., & Bond, B. (2012). Electronic health records: Privacy, confidentiality, and security. *American Medical Association Journal of Ethics*, *14*(9), 712-719. https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209

Herjavec Group. (2019). *The 2019 healthcare cybersecurity report*. Retrieved from https://www.herjavecgroup.com/wp-content/uploads/2018/11/Herjavec-Group-2019-Healthcare-Cybersecurity-Report.pdf

Hussung, T. (2015). Digitizing healthcare: How technology is improving medical care. Retrieved from https://online.king.edu/healthcare/digitizing-healthcare-how-technology-is-improving-medical-care/

IBM. (2018). *IBM X-Force Threat Intelligence Index 2018* (Rep.). Retrieved from https://www.ibm.com/downloads/cas/MKJOL3DG

Jacinta, K. (2006). An overview of conflict. *Dimensions of Critical Care Nursing*, *25*(2), 22–28.

Kim, L. (2017). Cybersecurity awareness. *Nursing, 47*(6), 65-67. doi:10.1097/01.nurse.0000516242.05454.b4

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology, 9*. doi:10.3389/fpsyg.2018.00039

Kotter, J. P., & Schlesinger, L. A. (2008, July). Choosing strategies for change. *Harward Business Review*, 23-28. Retrieved from https://hbr.org/2008/07/choosing-strategies-for-change

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1-10. doi:10.3233/thc-161263

McAfee. (2018). *Economic Impact of Cybercrime No Slowing Down* (Rep.). Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

McAfee. (2018). *McAfee Labs Threats Report*. *McAfee Labs Threats Report*. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2018.pdf

Myers, C. E. (2017). Elements of change. *Perspectives in Learning*, *16*(1), 15-18. Retrieved from http://csuepress.columbusstate.edu/pil/vol16/iss1/4

Olalere, M., Abdullah, M. T., Mahmod, R., & Abdullah, A. (2015). A review of bring your own device on security issues. *SAGE Open, 5*(2), 215824401558037. doi:10.1177/2158244015580372

Patel, V., & Johnson, C. (2018). *Individuals' use of online medical records and technology for health needs*. The Office of the National Coordinator for Health Information Technology. Retrieved from https://www.healthit.gov/sites/default/files/page/2018-03/HINTS-2017-Consumer-Data-Brief-3.21.18.pdf

Paul, D. (2017). Ransomware in healthcare facilities: The future is now. *Marshall Digital Scholar*,

Retrieved from http://mds.marshall.edu/cgi/viewcontent.cgi?article=1185&context=

mgmt_faculty

Ponemon Institute LLC. (2018). *2018 Cost of data breach study: Impact of business continuity management*. *2018 Cost of data breach study: Impact of business continuity management*. IBM. Retrieved from https://www.ibm.com/downloads/cas/4DNXZYWK

Pope, J. (2016). Ransomware: Minimizing the risks. *Innovations in Clinical Neuroscience*, *13*(11),

37–40. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5300711 /pdf/icns_13_11-12_37.pdf

Savage, K., Coogan, P., & Lau, H. (2015, August). Security response. Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response /whitepapers/the-evolution-of-ransomware.pdf.

SecuLore Solutions. (2019). Indiana Cyber Attacks. Retrieved from https://www.seculore.com/ cyber-attacks-indiana

Symantec. (2018). 10 cyber security facts and statistics for 2018. Retrieved from https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html

Symantec. (2018). *ISTR Internet Security Threat Report*. Symantec. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

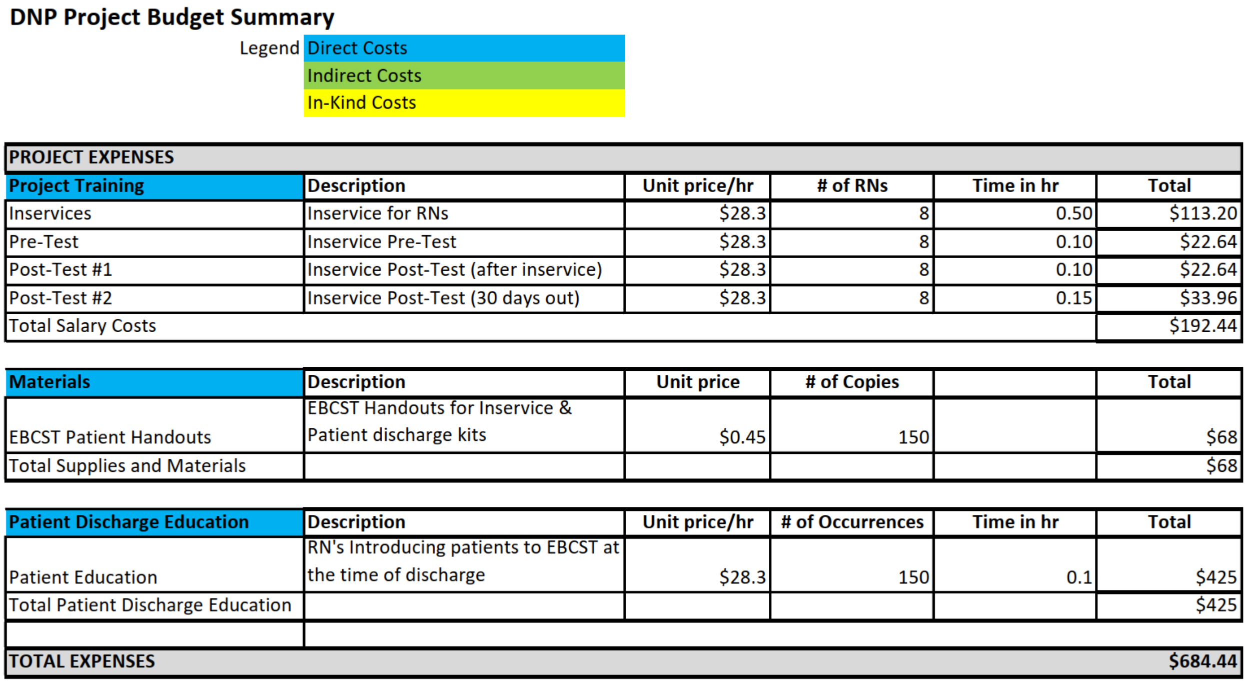
The essentials of doctoral education for advanced nursing practice (AACN). (2006). Retrieved February 20, 2019, from https://www.aacnnursing.org/Portals/42/Publications/DNPEssentials.pdf

The Office of the National Coordinator for Health Information Technology (ONC). (2017). What is a patient portal. Retrieved from https://www.healthit.gov/faq/what-patient-portal.

White, K. M., Dudley-Brown, S., & Terhaar, M. F. (2016). *Translation of evidence into nursing and health care* (2nd ed.). New York, NY: Springer Publishing Company, LLC

Appendix A

Project Budget



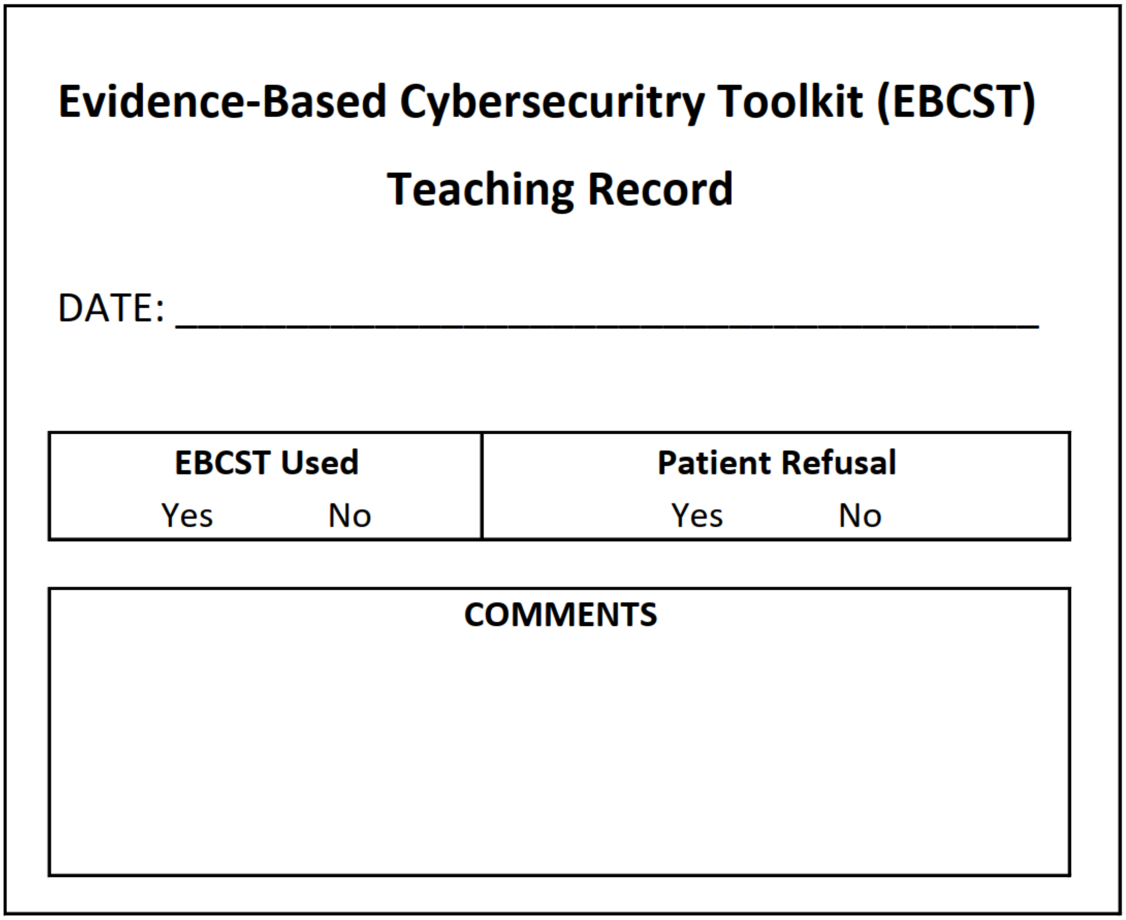
DNP Project Budget Summary

Legend	🟦 Direct Costs
	🟩 Indirect Costs
	🟨 In-Kind Costs

PROJECT EXPENSES					
Project Training	**Description**	**Unit price/hr**	**# of RNs**	**Time in hr**	**Total**
Inservices	Inservice for RNs	$28.3	8	0.50	$113.20
Pre-Test	Inservice Pre-Test	$28.3	8	0.10	$22.64
Post-Test #1	Inservice Post-Test (after inservice)	$28.3	8	0.10	$22.64
Post-Test #2	Inservice Post-Test (30 days out)	$28.3	8	0.15	$33.96
Total Salary Costs					$192.44
Materials	**Description**	**Unit price**	**# of Copies**		**Total**
EBCST Patient Handouts	EBCST Handouts for Inservice & Patient discharge kits	$0.45	150		$68
Total Supplies and Materials					$68
Patient Discharge Education	**Description**	**Unit price/hr**	**# of Occurrences**	**Time in hr**	**Total**
Patient Education	RN's Introducing patients to EBCST at the time of discharge	$28.3	150	0.1	$425
Total Patient Discharge Education					$425
TOTAL EXPENSES					**$684.44**

Appendix B

EBCST Teaching Record



Evidence-Based Cybersecuritry Toolkit (EBCST)

Teaching Record

DATE: ______________________________________

EBCST Used	**Patient Refusal**
Yes No	Yes No

COMMENTS

Appendix C

Pre-Test

PRE-TEST

***Demographic info.** Used only for purposes of this study.*

1. Age: ____ Gender: M / F Occupation: ________________ Living State:_____________

2. Your employment status at Adams Memorial Hospital is:

□ Full-time □ Part-time □ Other

2. Do you have IT background? Yes____ No ______

3. How many personal computers (PC) and/or personal devices i.e. cell phones, ipads, tablets, do you own and use to access the world-wide-web, i.e. check emails, read articles, news, etc.?

□ None □ One □ Two □ Three □ Four or more

4. How many personal computers (PC) and/or personal devices i.e. cell phones, ipads, tablets, you own and use are protected by an antivirus program?

□ None □ One □ Two □ Three □ Four or more

5. In general, which is more important to you: Convenience *or* Privacy & Security?

□ Convenience □ Privacy & Security

*Please answer, on a scale of **0-5,** how much you agree with the following statements. Check the box beside your answer.*

***0**= Not at all **1**=Strongly Disagree **2**=Disagree **3**=Neutral **4**=Agree **5**= Strongly Agree*

I feel, my computer, cellphone, tablet, iPad, is very secure	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
My computer or mobile device has no value to hackers, they do not target me	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
I look who the email is from before I open the email attachment	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
Open Wifi hotspots are reasonably safe to view your electronic health records online	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5

I currently know enough about the basic steps in protecting my personal computers and mobile devices from cyberattacks	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
I regularly clear internet browser search history on my mobile devices and personal computers	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
I am familiar with the concept of cybersecurity	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5

6. Are you interested in receiving outcome information from this project? □ Yes □ No

If yes, please list your email address: ______________________________________

Appendix D

Post-Test

POST-TEST

1. Have you attended the Evidence-Based Cybersecurity Awareness In-services on 00/00/2019?

□ Yes □ No

2. Have participated in piloting the Evidence-Based Cybersecurity Awareness Toolkit during its three-week implementation phase in Spring, 2020?

□ Yes □ No

Please answer, on a scale of ***0-5,*** *how much you agree with the following statements. Check the box beside your answer.*

0*= Not at all* ***1****=Strongly Disagree* ***2****=Disagree* ***3****=Neutral* ***4****=Agree* ***5****= Strongly Agree*

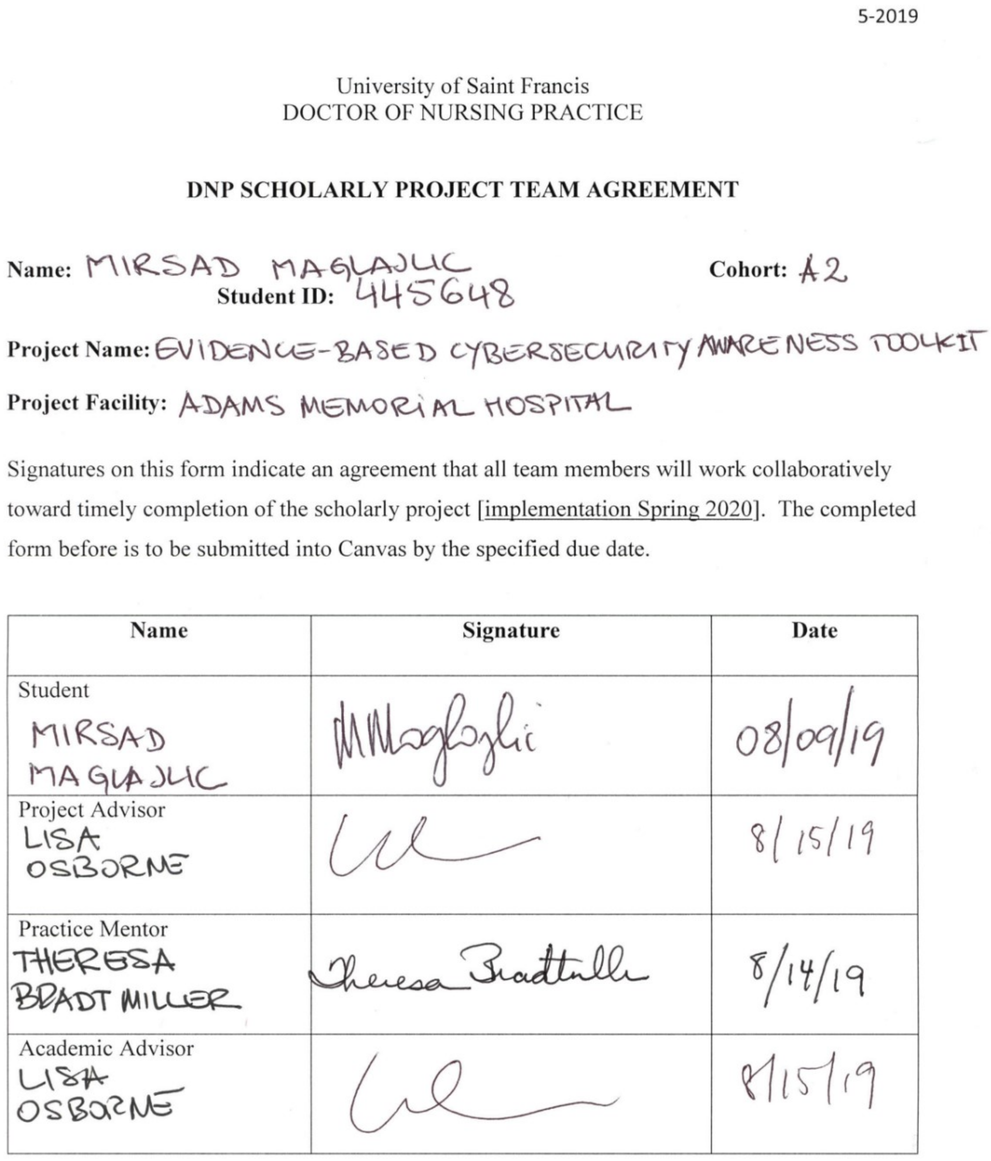
I feel, my computer, cellphone, tablet, ipad, is very secure	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
My computer or mobile device has no value to hackers, they do not target me	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
I look who the email is from before I open the email attachment	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
Open Wifi hotspots are reasonably safe to view your electronic health records online	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
I currently know enough about the basic steps in protecting my personal computers and mobile devices from cyberattacks	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
I regularly clear internet browser search history on my mobile devices and personal computers	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5
I am familiar with the concept of cybersecurity	□ 0 □ 1 □ 2 □ 3 □ 4 □ 5

6. Are you interested in receiving outcome information from this project? □ Yes □ No

If yes, please list your email address: ____

Appendix E

Project Agreement



5-2019

University of Saint Francis
DOCTOR OF NURSING PRACTICE

DNP SCHOLARLY PROJECT TEAM AGREEMENT

Name: MIRSAD MAGLAJLIC **Cohort:** A2

Student ID: 445648

Project Name: EVIDENCE-BASED CYBERSECURITY AWARENESS TOOLKIT

Project Facility: ADAMS MEMORIAL HOSPITAL

Signatures on this form indicate an agreement that all team members will work collaboratively toward timely completion of the scholarly project [implementation Spring 2020]. The completed form before is to be submitted into Canvas by the specified due date.

Name	Signature	Date
Student MIRSAD MAGLAJLIC	MMaglajlic	08/09/19
Project Advisor LISA OSBORNE		8/15/19
Practice Mentor THERESA BRADT MILLER	Theresa Bradtmiller	8/14/19
Academic Advisor LISA OSBORNE		8/15/19

Appendix F

Informed Consent

INFORMED CONSENT FORM

Evidence-Based Cybersecurity Awareness Toolkit

Explanation and the Purpose of the Research

My name is Mirsad Maglajlic. I am a graduate student nurse anesthetist at the University of Saint Francis (USF) in Fort Wayne, Indiana. I am conducting a scholarly Doctor of Nursing Practice (DNP) study with the express purpose of translating evidence into practice. My DNP project advisor is Dr. Lisa Osborne.

In the light of ongoing cybersecurity threats on the healthcare industry and the consumers of healthcare services, this scholarly project is aimed at raising awareness and educating both providers and consumers about evidence-based guidelines in securing personal devices as a safety step in preserving and protecting the electronic health records.

I would appreciate your participation in this study, as it will aid in making recommendations for improving the teaching of healthcare professionals on the subject of evidence-based cybersecurity recommendations and guidelines.

DNP Project Consists of the Following Procedures:

1. Administration of a questionnaires
   a. Pretest will be administered immediately prior to the educational in-service.
   b. First post-test will be administered upon completion of the in-service.
   c. Second post-test will be administered approximately 30 days following the in-service.
   d. Each questionnaire will be in a multiple-question format or Likert scale
   e. Each questionnaire will take approximately 10 minutes to complete.
2. Evidence-Based Cybersecurity Awareness Toolkit (EBSCT) In-service
   a. Educational in-service will be scheduled in advance at your facility of employment and you will be informed of the time, and place
   b. Educational in-service will take approximately 30 minutes
3. A time-limited integration of EBSCT and patient education upon discharge
   a. Participating staff (a discharge team) will provide patients at discharge with a EBSCT handout
   b. Participating staff (a discharge team) will also provide a basic explanation about EBSCT to patients upon discharge
   c. A time-limited integration of EBSCT and patient education phase of this DNP project will be piloted one time for 3 consecutive weeks.
4. An adequate number of participants is required for this scholarly study which reflects a minimum of 5 participants.

DNP Project Risks and Benefits

1. This scholarly study does not involve any foreseeable risks or discomforts such as the inconvenience of time requirements, anxiety regarding sensitive questions, or additional costs that the participants may incur as a result of participation.
2. This study does not include compensation.

Protection of Participants' Identity

1. Participants in this study will not be identifiable, directly or indirectly.
2. Any data collection will be conducted anonymously.
3. Final results of the data analysis may be shared with USF DNP faculty members and Adams Memorial Hospital senior leadership team.

Freedom to Withdraw

1. The participation in this study is completely voluntary and that participants may withdraw from the study at any time and for any reason without penalty.
2. P articipation or decision not to participate will not affect treatment or involve penalty or loss of benefits to which the participants are otherwise entitled to
1. Information obtained through pre- and post-tests from subjects who choose to withdraw from this study will be excluded from the final study analysis.

Once the study is completed, we would be glad to give the results to you. In the meantime, if you have any questions, please contact us at:

Attn. Mirsad Maglajlic
2701 Spring St, Fort Wayne, IN 46808
Phone 260-466-0825
Email: maglajlicm@cougars.sf.edu

If you have any complaints about your treatment as a participant in this study, please call or write:

IRB Chairperson
University of Saint Francis
2701 Spring Street
Fort Wayne, Indiana 46808
Phone: (260) 399-7700
Administration email: DFILLER@sf.edu

I have received an explanation of this study and agree to participate. I understand that my participation in this study is strictly voluntary.

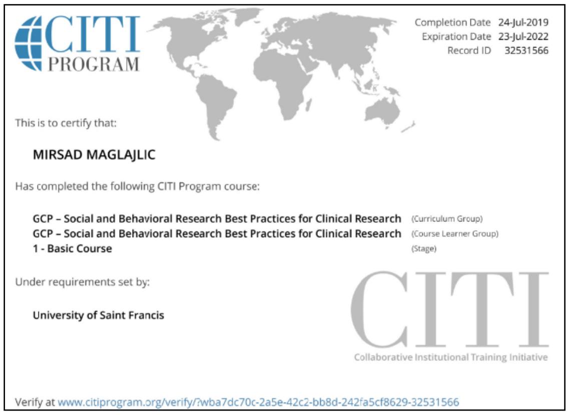
Name ________________________________

Date ________________________________

**This research project has been approved by the University of Saint Francis' Institutional Review Board for the Protection of Human Subjects for a one-year period.*

Appendix G

CITI Training



CITI PROGRAM

Completion Date 24-Jul-2019
Expiration Date 23-Jul-2022
Record ID 32531566

This is to certify that:

MIRSAD MAGLAJLIC

Has completed the following CITI Program course:

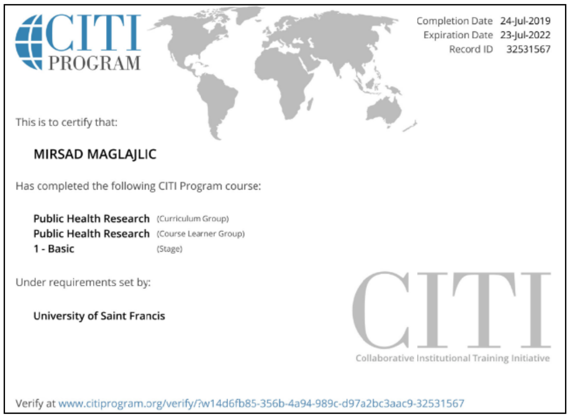
GCP – Social and Behavioral Research Best Practices for Clinical Research (Curriculum Group)
GCP – Social and Behavioral Research Best Practices for Clinical Research (Course Learner Group)
1 - Basic Course (Stage)

Under requirements set by:

University of Saint Francis

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?wba7dc70c-2a5e-42c2-bb8d-242fa5cf8629-32531566



CITI PROGRAM

Completion Date 24-Jul-2019
Expiration Date 23-Jul-2022
Record ID 32531567

This is to certify that:

MIRSAD MAGLAJLIC

Has completed the following CITI Program course:

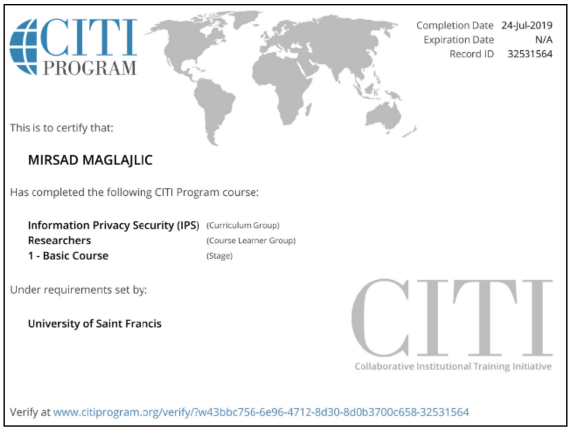
Public Health Research (Curriculum Group)
Public Health Research (Course Learner Group)
1 - Basic (Stage)

Under requirements set by:

University of Saint Francis

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?w14d6fb85-356b-4a94-989c-d97a2bc3aac9-32531567



CITI PROGRAM

Completion Date 24-Jul-2019
Expiration Date N/A
Record ID 32531564

This is to certify that:

MIRSAD MAGLAJLIC

Has completed the following CITI Program course:

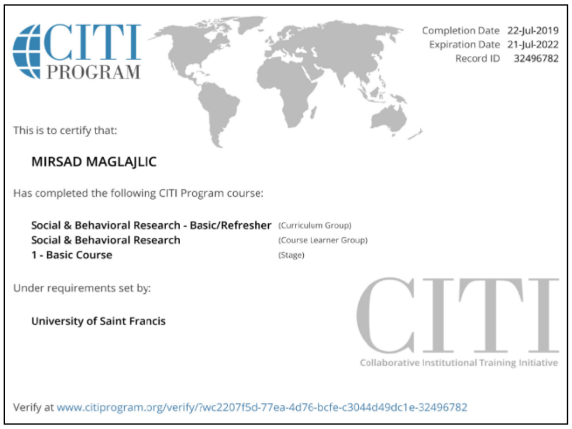
Information Privacy Security (IPS) (Curriculum Group)
Researchers (Course Learner Group)
1 - Basic Course (Stage)

Under requirements set by:

University of Saint Francis

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?w43bbc756-6e96-4712-8d30-8d0b3700c658-32531564



CITI PROGRAM

Completion Date 22-Jul-2019
Expiration Date 21-Jul-2022
Record ID 32496782

This is to certify that:

MIRSAD MAGLAJLIC

Has completed the following CITI Program course:

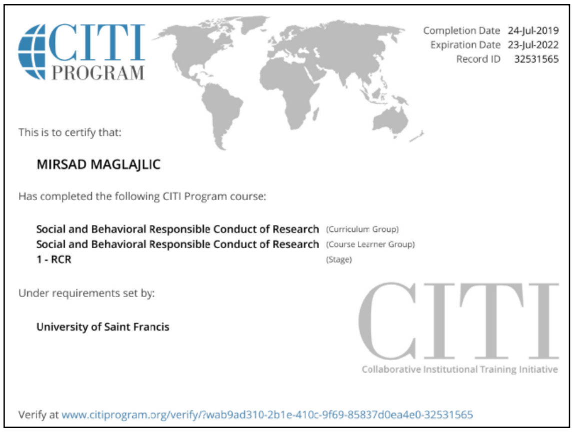
Social & Behavioral Research - Basic/Refresher (Curriculum Group)
Social & Behavioral Research (Course Learner Group)
1 - Basic Course (Stage)

Under requirements set by:

University of Saint Francis

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?wc2207f5d-77ea-4d76-bcfe-c3044d49dc1e-32496782



CITI PROGRAM

Completion Date 24-Jul-2019
Expiration Date 23-Jul-2022
Record ID 32531565

This is to certify that:

MIRSAD MAGLAJLIC

Has completed the following CITI Program course:

Social and Behavioral Responsible Conduct of Research (Curriculum Group)
Social and Behavioral Responsible Conduct of Research (Course Learner Group)
1 - RCR (Stage)

Under requirements set by:

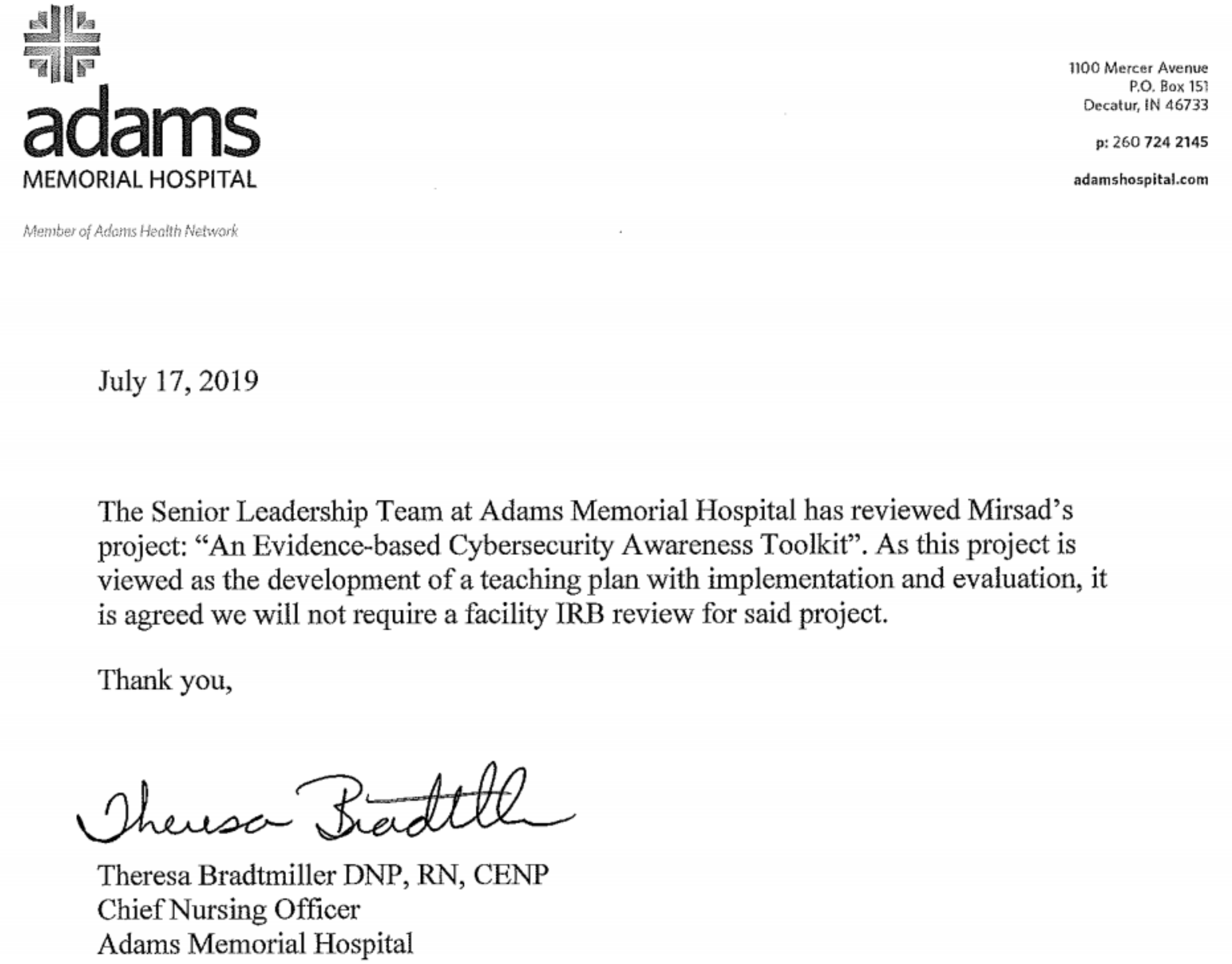
University of Saint Francis

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?wab9ad310-2b1e-410c-9f69-85837d0ea4e0-32531565

Appendix H

AMH IRB



adams
MEMORIAL HOSPITAL

Member of Adams Health Network

1100 Mercer Avenue
P.O. Box 151
Decatur, IN 46733

p: 260 724 2145

adamshospital.com

July 17, 2019

The Senior Leadership Team at Adams Memorial Hospital has reviewed Mirsad's project: "An Evidence-based Cybersecurity Awareness Toolkit". As this project is viewed as the development of a teaching plan with implementation and evaluation, it is agreed we will not require a facility IRB review for said project.

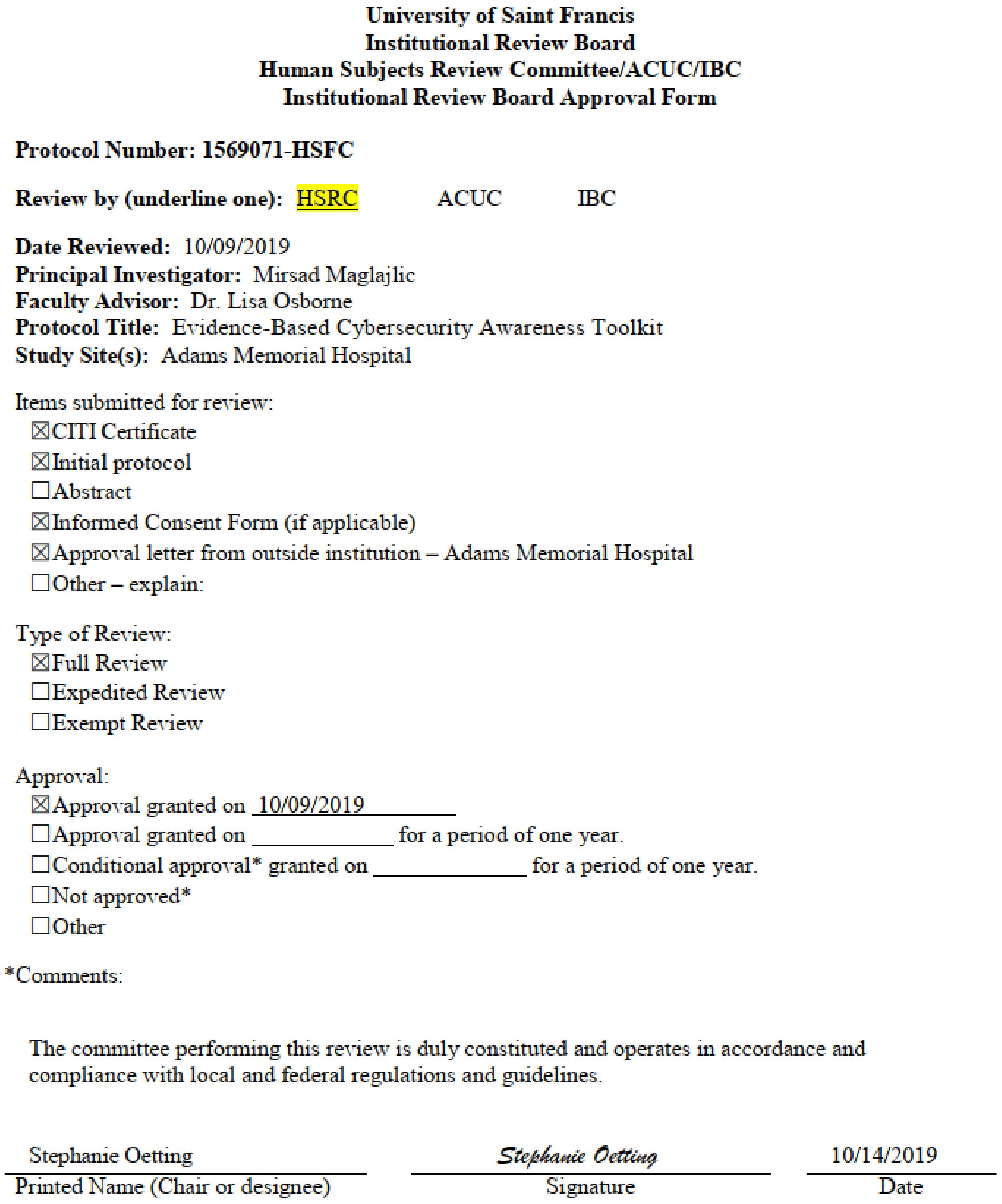
Thank you,

Theresa Bradtl

Theresa Bradtmiller DNP, RN, CENP
Chief Nursing Officer
Adams Memorial Hospital

Appendix L

USF IRB



University of Saint Francis
Institutional Review Board
Human Subjects Review Committee/ACUC/IBC
Institutional Review Board Approval Form

Protocol Number: 1569071-HSFC

Review by (underline one): HSRC ACUC IBC

Date Reviewed: 10/09/2019
Principal Investigator: Mirsad Maglajlic
Faculty Advisor: Dr. Lisa Osborne
Protocol Title: Evidence-Based Cybersecurity Awareness Toolkit
Study Site(s): Adams Memorial Hospital

Items submitted for review:
☒CITI Certificate
☒Initial protocol
☐Abstract
☒Informed Consent Form (if applicable)
☒Approval letter from outside institution – Adams Memorial Hospital
☐Other – explain:

Type of Review:
☒Full Review
☐Expedited Review
☐Exempt Review

Approval:
☒Approval granted on 10/09/2019
☐Approval granted on ______________ for a period of one year.
☐Conditional approval* granted on ______________ for a period of one year.
☐Not approved*
☐Other

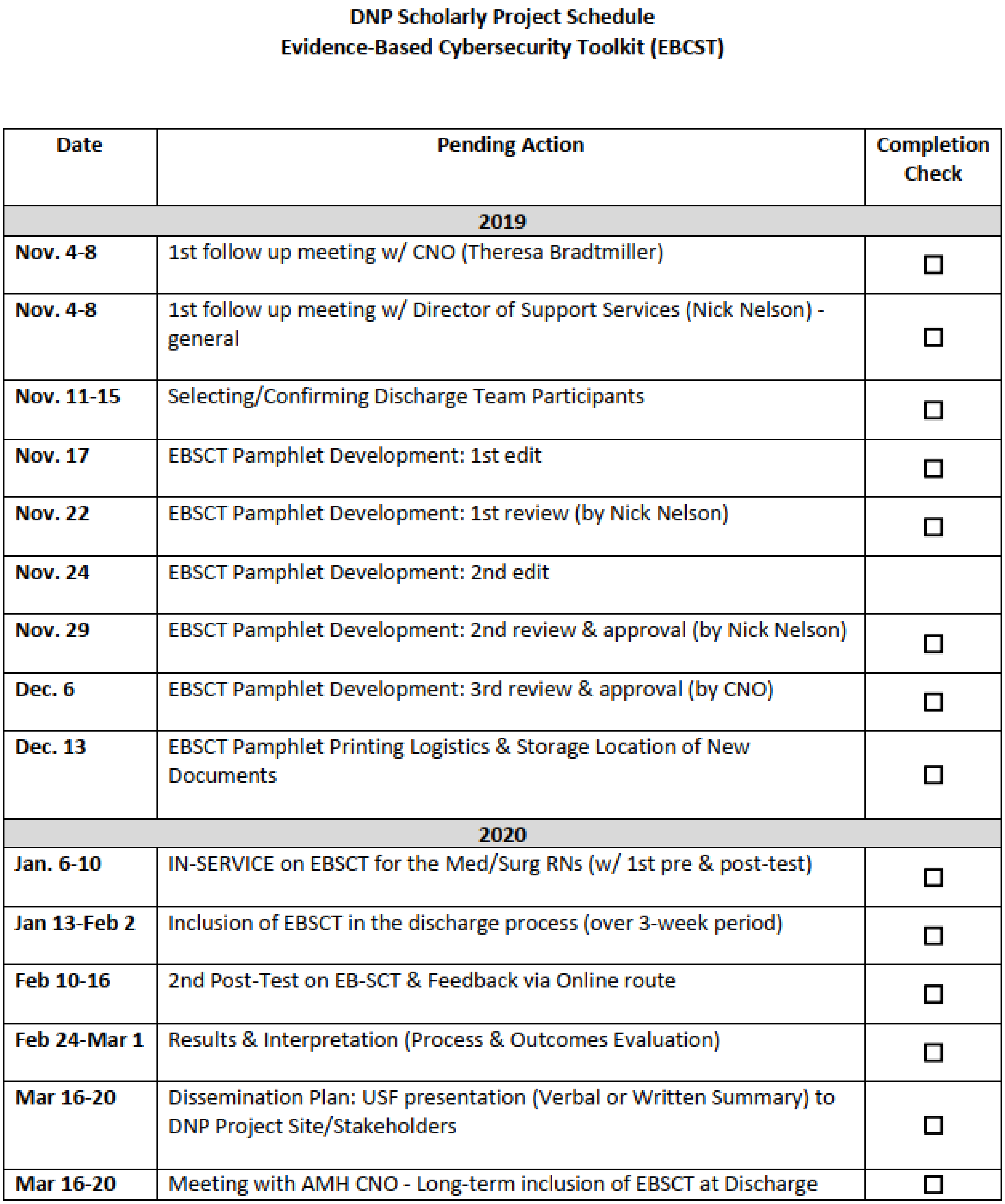
*Comments:

The committee performing this review is duly constituted and operates in accordance and compliance with local and federal regulations and guidelines.

Stephanie Oetting	Stephanie Oetting	10/14/2019
Printed Name (Chair or designee)	Signature	Date

Appendix M

Project Schedule

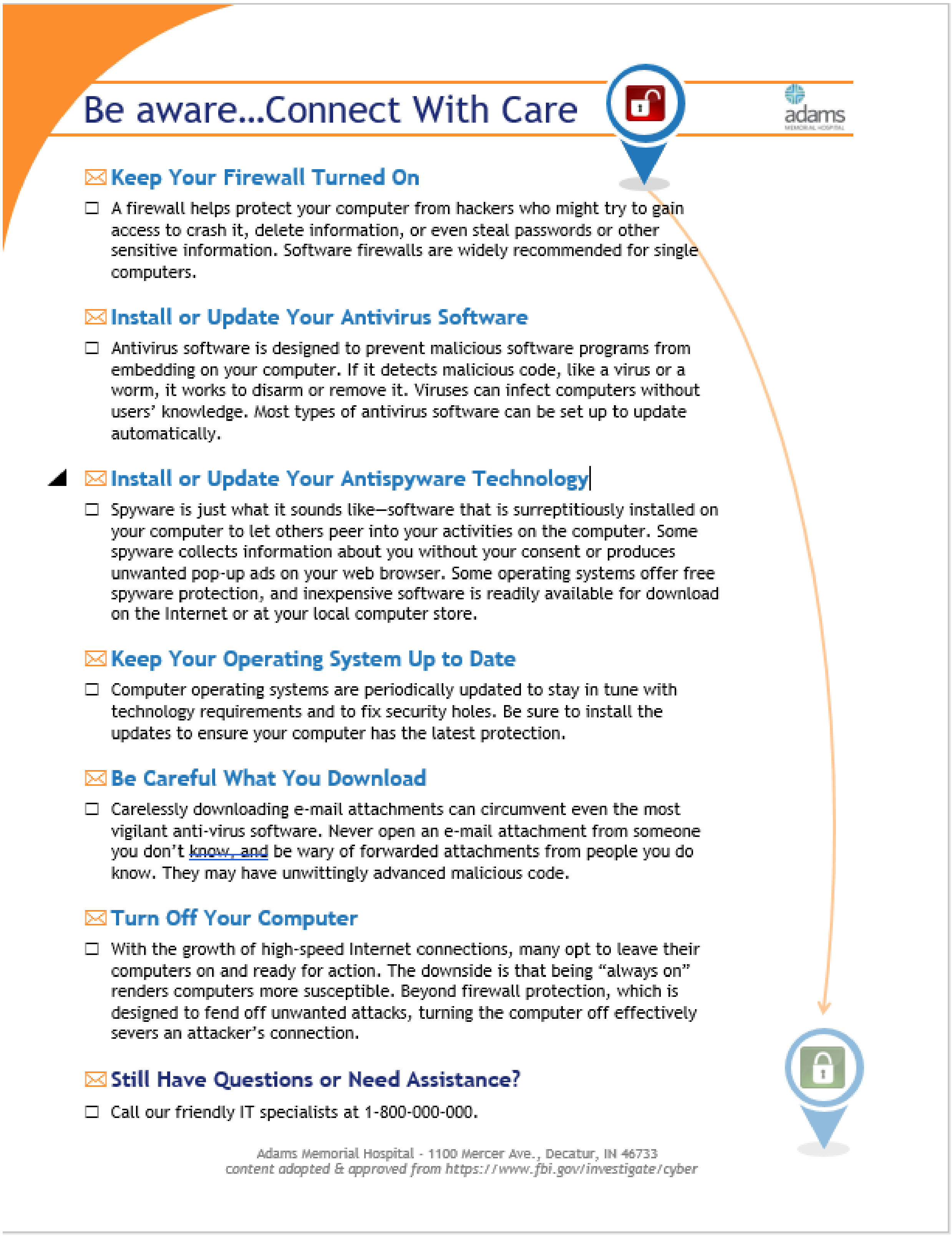


DNP Scholarly Project Schedule
Evidence-Based Cybersecurity Toolkit (EBCST)

Date	Pending Action	Completion Check
	2019	
Nov. 4-8	1st follow up meeting w/ CNO (Theresa Bradtmiller)	□
Nov. 4-8	1st follow up meeting w/ Director of Support Services (Nick Nelson) - general	□
Nov. 11-15	Selecting/Confirming Discharge Team Participants	□
Nov. 17	EBSCT Pamphlet Development: 1st edit	□
Nov. 22	EBSCT Pamphlet Development: 1st review (by Nick Nelson)	□
Nov. 24	EBSCT Pamphlet Development: 2nd edit	
Nov. 29	EBSCT Pamphlet Development: 2nd review & approval (by Nick Nelson)	□
Dec. 6	EBSCT Pamphlet Development: 3rd review & approval (by CNO)	□
Dec. 13	EBSCT Pamphlet Printing Logistics & Storage Location of New Documents	□
	2020	
Jan. 6-10	IN-SERVICE on EBSCT for the Med/Surg RNs (w/ 1st pre & post-test)	□
Jan 13-Feb 2	Inclusion of EBSCT in the discharge process (over 3-week period)	□
Feb 10-16	2nd Post-Test on EB-SCT & Feedback via Online route	□
Feb 24-Mar 1	Results & Interpretation (Process & Outcomes Evaluation)	□
Mar 16-20	Dissemination Plan: USF presentation (Verbal or Written Summary) to DNP Project Site/Stakeholders	□
Mar 16-20	Meeting with AMH CNO - Long-term inclusion of EBSCT at Discharge	□

Appendix N

EBCST



Be aware...Connect With Care

✉ Keep Your Firewall Turned On

☐ A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers.

✉ Install or Update Your Antivirus Software

☐ Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users' knowledge. Most types of antivirus software can be set up to update automatically.

✉ Install or Update Your Antispyware Technology

☐ Spyware is just what it sounds like—software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store.

✉ Keep Your Operating System Up to Date

☐ Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.

✉ Be Careful What You Download

☐ Carelessly downloading e-mail attachments can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don't know, and be wary of forwarded attachments from people you do know. They may have unwittingly advanced malicious code.

✉ Turn Off Your Computer

☐ With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection.

✉ Still Have Questions or Need Assistance?

☐ Call our friendly IT specialists at 1-800-000-000.

Adams Memorial Hospital - 1100 Mercer Ave., Decatur, IN 46733
content adopted & approved from https://www.fbi.gov/investigate/cyber