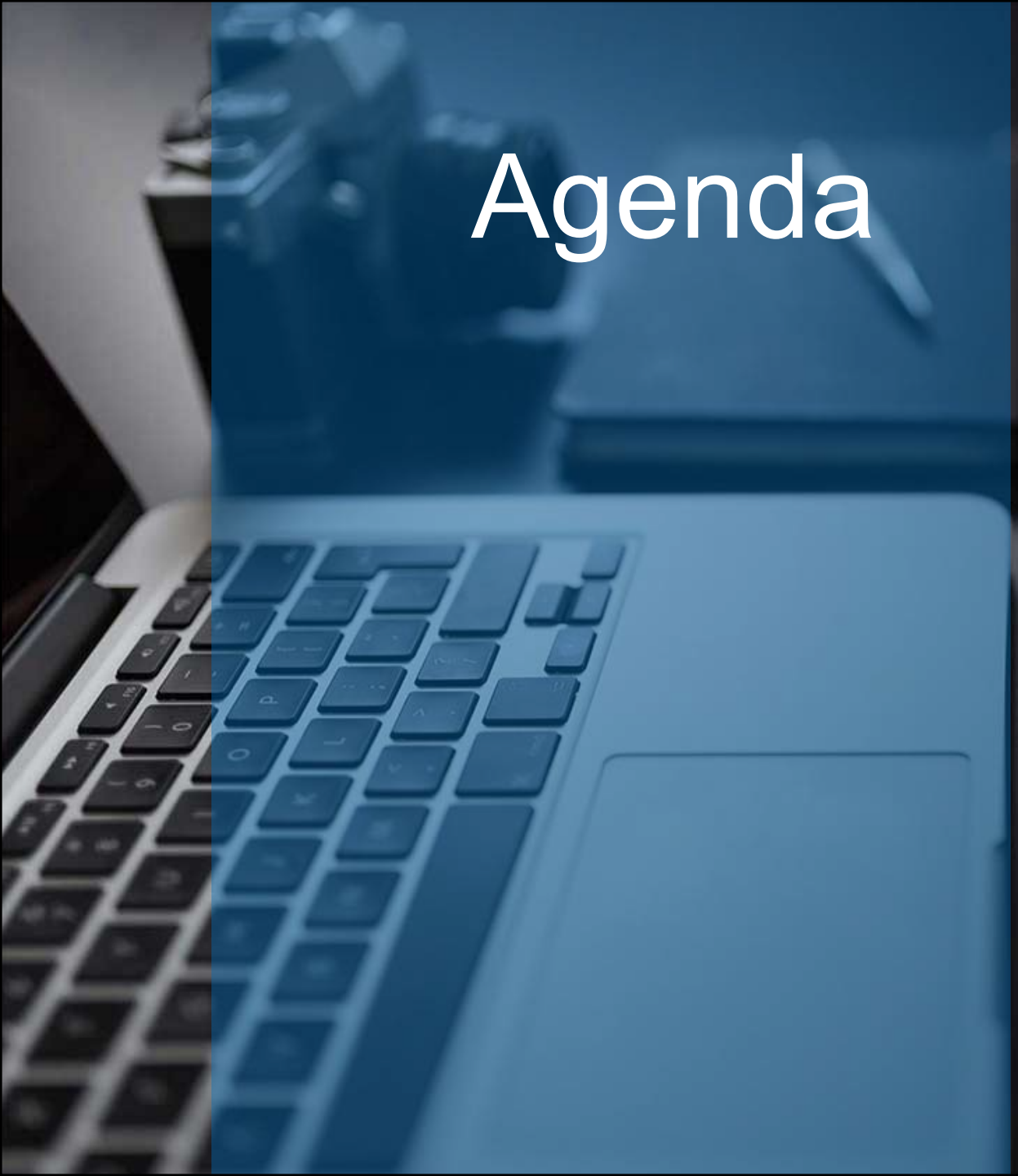
Evidence-Based Cybersecurity Toolkit
Nurs 785

Mirsad Maglajlic, BSN, GSRNA

DISCLOSURE

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 evidence-based cybersecurity awareness toolkit 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.

DNP Project Implementation Plan



Agenda

01 Problem Statement

Background of the problem, practice-knowledge gap identified.

02 DNP Project Overview

Scope Project team, setting, target population, summary of expected outcomes, risk analysis, ethical considerations, IRB approval.

03 Relevant Frameworks

Supporting evidence and literature that inform the DNP scholarly project.

04 Implementation Methods

Project type with elements of implementation.

05 Evaluation & Recommendations

Methods of evaluation and future directions.

Problem Statement

Background of the Problem and Identified Gaps

Healthcare Under Cyber Attack

$8 Million per Data Breach

In 2017, the cost of an average cyberattack data breach to a U.S. company.

Healthcare Targeted 1000% ▲

Since 2017, the United States is targeted the most.

Healthcare became the most targeted industry.

196 Days to Discover a Breach

In 2017, it took an average of one hundred-ninety-six days for the breach to be discovered.

8+ Million Malware Threats

The number of uniquely identified malware threats has risen from 0.13 to 8.4 million in the last decade. Nearly 1000 malware specimens discovered every hour.

(G Data Software; 2018 McAfee, 2018; Ponemon Institute LLC, 2018; Symantec, 2018)

Cyberattacks

Ransomware!

9 Hospitals, Clinics, and Healthcare Centers

Adams, Allen, DeKalb, Hancock, Jefferson, & St. Joseph County

Disruption of healthcare services, EHR inaccessible, database and patient records breaches, financial losses in thousands of dollars

(SecuLore Solutions, 2019)

EHR Consumer Access

2 50% have accessed and viewed their EHR at least once

1 In 2017, 52% of healthcare consumers nationwide were offered online access to personal electronic health records (EHR)

3 30% used an electronic device such as a smart phone or a tablet to view EHR

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; Patel & Johnson, 2018)

Practice & Knowledge Gap

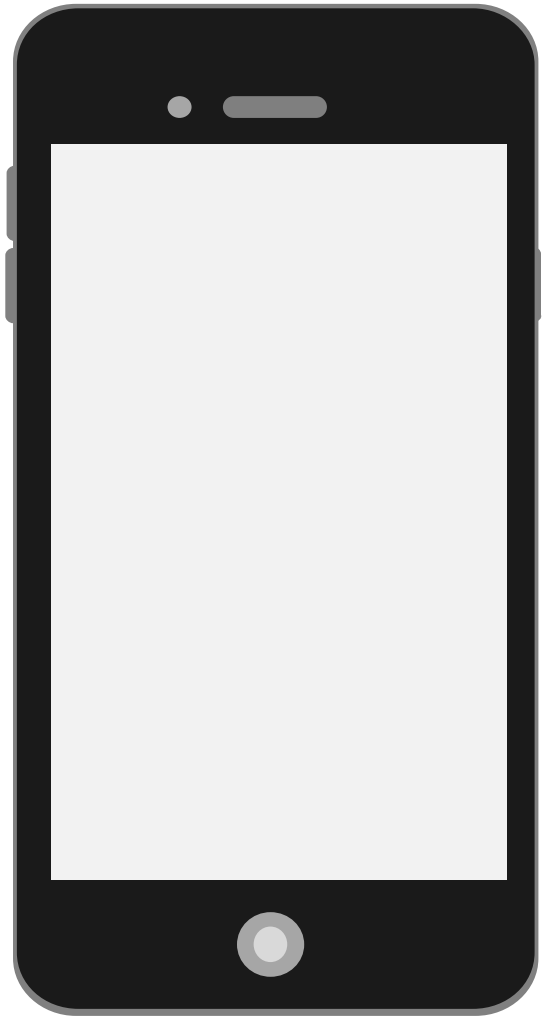
Gap Identified

Lack of awareness of the essential cybersecurity principles in keeping personal and mobile devices safe when accessing personal EHR online

The consumers of health care services are frequently offered an easy and convenient way to access their personal EHR online.

Consumers of healthcare are not being educated as to how to access their personal EHR safely.

Standardized policies nationwide do not exist that require or hold health providers accountable to educate the end-system users (patients) about the basic cybersecurity principles when accessing the personal health information online.



(Symantec, 2018)

Research Question

The PICOT Question for the 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

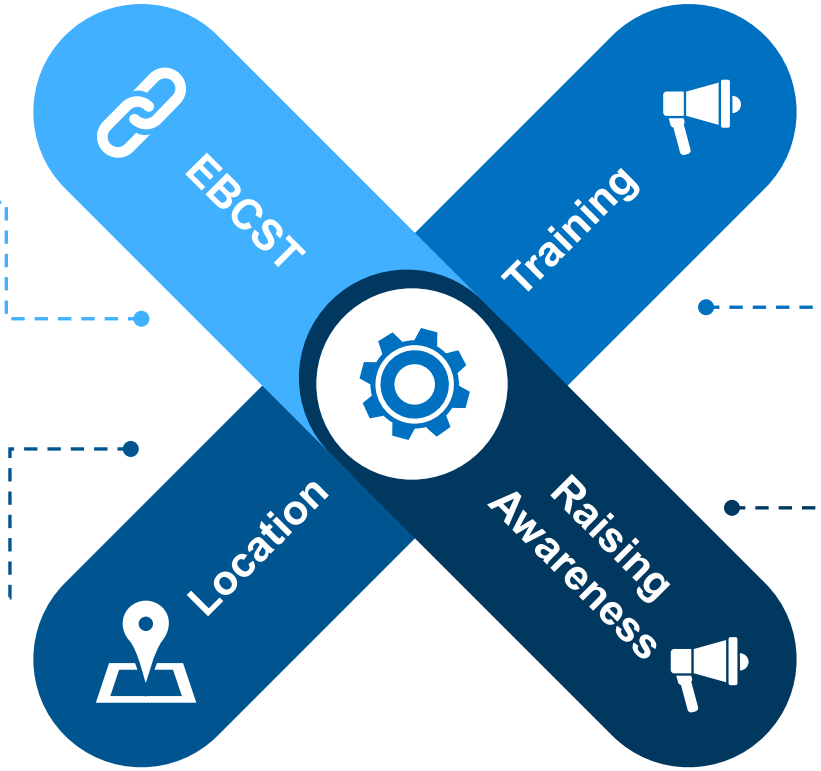
DNP Project Overview

Purpose & Aims

Scope

Synthesis of EBCST

This DNP project is focused on synthesizing an evidence-based cybersecurity awareness toolkit (EBCST).



Train Medical-Surgical RNs

EBCST will be used to train medical-surgical unit registered nurses (RN).

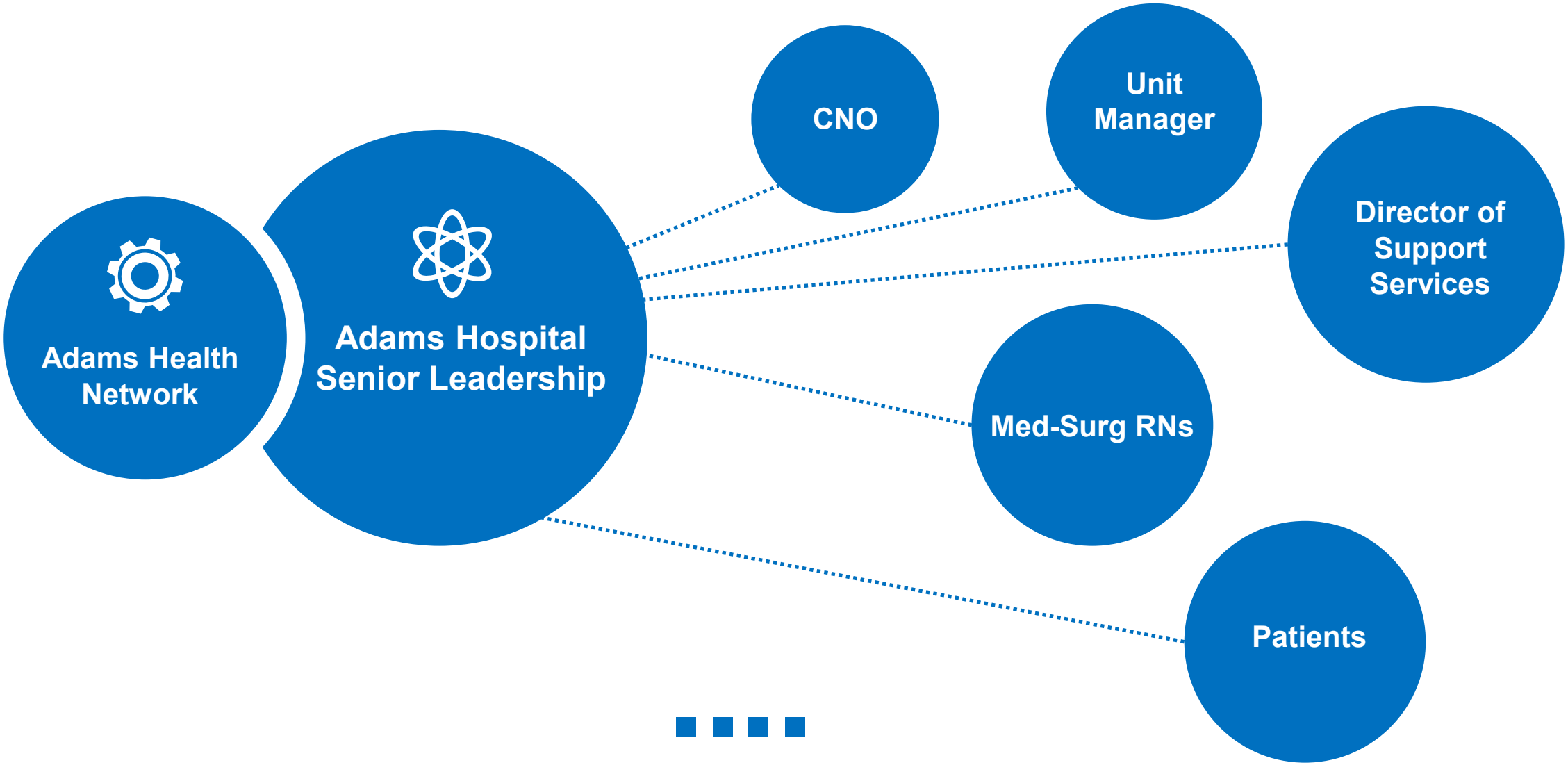
Implementation Site

Adams Memorial Hospital (AMH)
Medical-Surgical Unit

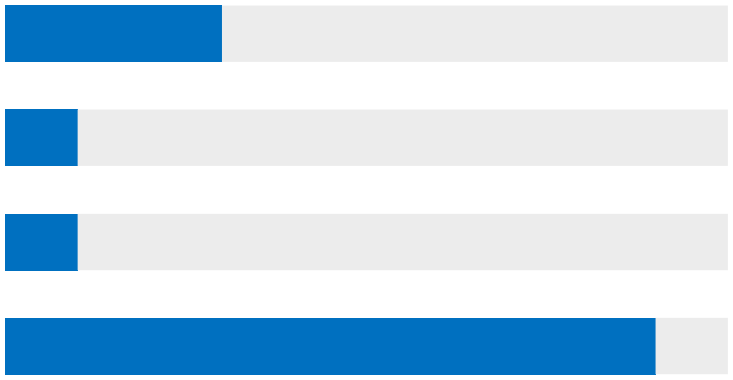
Medical-Surgical RNs Educate Patients to EBCST

Upon completion of the evidence-based cybersecurity training, participating RNs will be qualified to raise awareness and educate patients on how to keep the personal and mobile devices safe when accessing personal EHR..

Stakeholders



Risk & Ethical Considerations

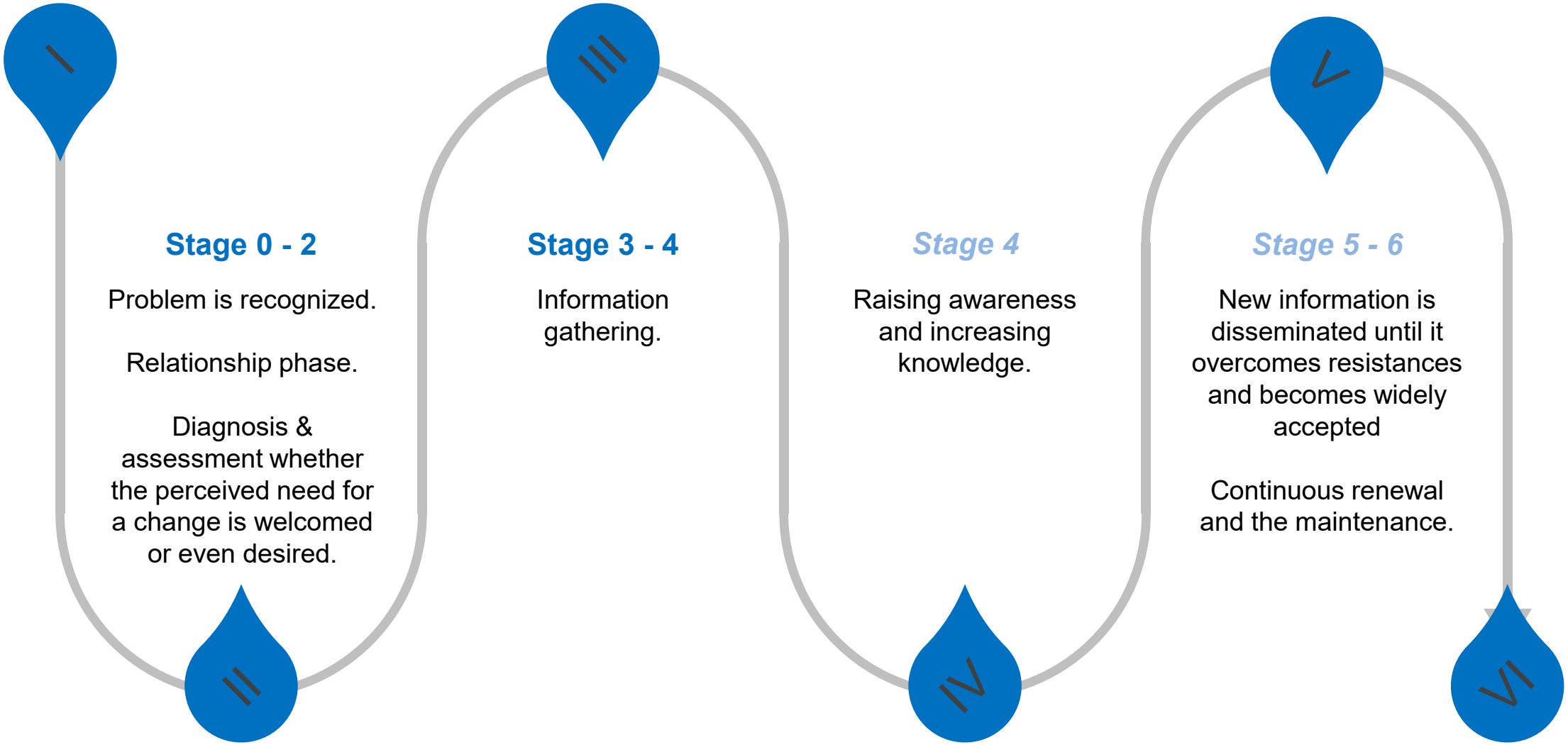


Med	**Stakeholder's Lack of Support**
Low	**Participants Dropout Risk**
Low	**Patient Risk**
High	**Implementation Risk – COVID19**

Theoretical Frameworks

Theoretical concepts & supporting literature

Havelock's Theory of Change



Stage 0 - 2

Problem is recognized.

Relationship phase.

Diagnosis & assessment whether the perceived need for a change is welcomed or even desired.

Stage 3 - 4

Information gathering.

Stage 4

Raising awareness and increasing knowledge.

Stage 5 - 6

New information is disseminated until it overcomes resistances and becomes widely accepted

Continuous renewal and the maintenance.

Project Implementation

Project type & process steps

2-Phase Implementation

Participants Inclusion/Exclusion Criteria

INCLUSION CRITERIA

- Medical-surgical registered nurses (RN)
- Part-time or full-time
- Employed at Adams Health Network

EXCLUSION CRITERIA

- Nursing students obtaining clinical training at Adams Memorial Hospital
- Temporary agency nurses
- Recently hired nurses who are still in training or orientation.

Phase I

- ✓ EBCST In-service
- ✓ Presentation in person
- ✓ Presentation via PowerPoint
- ✓ Medical-surgical RNs will receive a copy of the EBCST pamphlet and EBSCT teaching record.
- ✓ Objective is for the medical-surgical RNs to become familiar with EBCST and evidence-based guidelines in securing personal and mobile devices from cyber threats.

Phase II

- ✓ Medical-surgical RN project participants raising awareness and educating patients about EBCST at the time of discharge.
- ✓ Following each patient discharge, the medical-surgical RN will fill out the EBCST teaching record and place it in a secured, designated box.
- ✓ EBCST teaching records will be collected by the project manager once a week and digitalized

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 mobile applications and 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. Only download mobile applications from established, trustworthy sources. Mobile applications 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?

- ☐ Visit US-CERT, U.S. Computer Emergency Readiness Team, *https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf*

Adams Memorial Hospital · 1100 Mercer Ave, Decatur, IN 46733

Cyber-guidelines adopted from https://www.fbi.gov/investigate/cyber

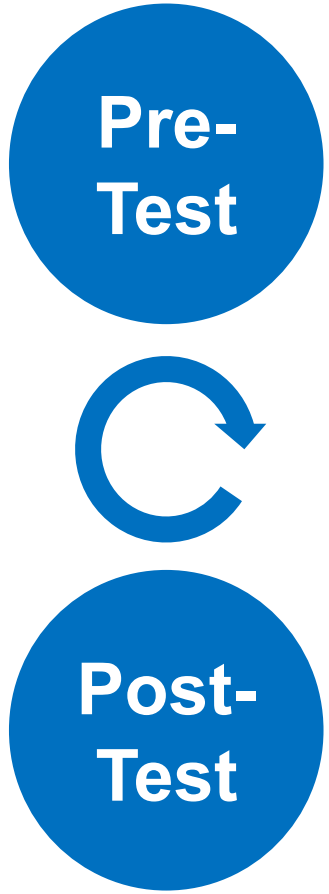
Measuring Tools & Data Collection 1

1. Pre-Test

- Administered and collected prior the in-service
- Printed/hard copy format
- Administered one time
- Measured will be the knowledge and perceptions
- No relevant and or published measurement scale was found
- A self-created instrument was designed instead
- The instrument mimics primarily the Likert scale format
- Seven Likert formatted questions
- Top portion - basic demographic information
- Bottom portion – assessment of knowledge and perception

2. Post-Test

- Administered & collected upon completion of the in-service and 2nd time electronically online 30 days after the in-service
- Printed/hard copy format & electronic
- Administered two times
- Same setup as the pre-test
- Excludes demographics section
- Seven Likert formatted questions



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

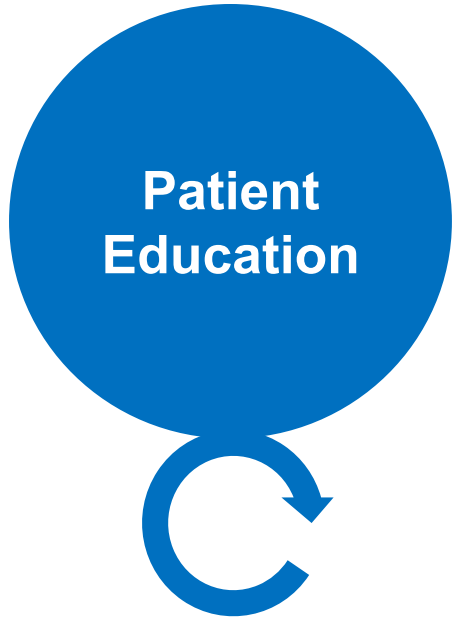
6. Are you interested in receiving outcome information from this project? ☐ Yes ☐ No

If yes, please list your email address: _____

Measuring Tools & Data Collection 2

3. EBCST Teaching Record

- Printed/hard copy format, color coded
- Part of every patient discharge packet
- Filled out by medical-surgical RNs upon discharge
- Deposited by medical-surgical RN in a secured box
- Assesses the frequency of EBCST patient teachings vs. the number of patient discharges
- Assesses if EBCST patient teaching was omitted due to patient refusal
- EBCST teaching records will be collected and digitalized by the project manager weekly



Appendix B

EBCST Teaching Record

Evidence-Based Cybersecuritry Toolkit (EBCST)

Teaching Record

DATE: _____

EBCST Used		Patient Refusal	
Yes	No	Yes	No

COMMENTS

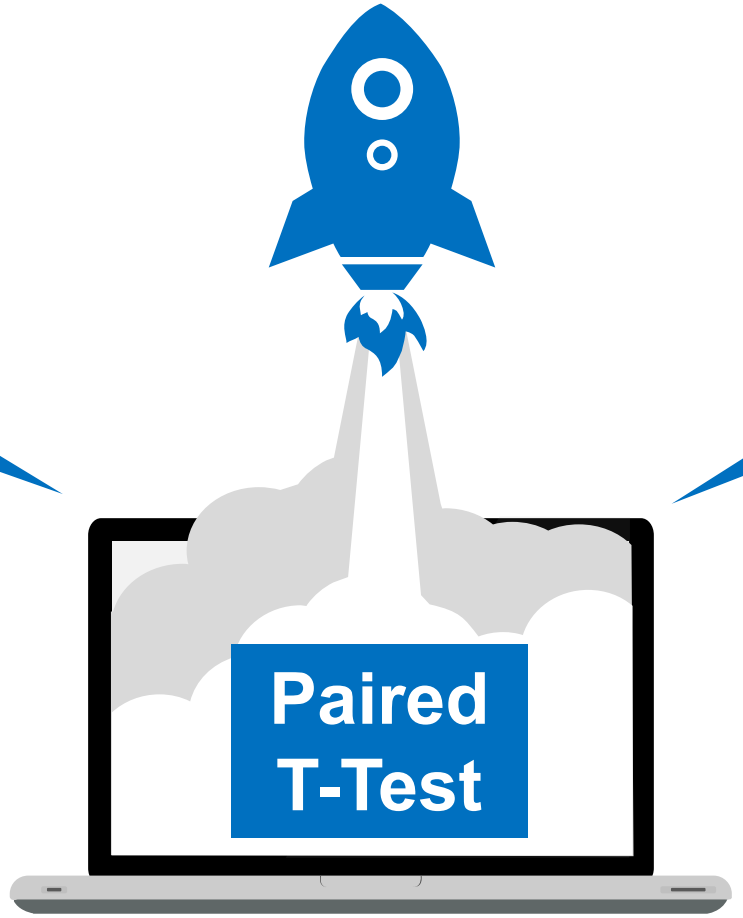
Evaluation

Methods and steps

IBM SPSS Statistics v.25

Pre-Test

Post-Test



The objective of this analysis is to learn if knowledge has been gained as a result of the educational in-service provided and if the change is statistically significant.

Statistical difference with p-value of less than 0.05

Dissemination Plan

Adams Memorial Hospital

- AMH leadership personnel during final meeting. Results will be provided in print.
- Clinical staff final correspondence and result sharing via email

AMH

USF

DNP faculty

- Executive Summary will be shared with the DNP project facility.
- PowerPoint presentation

DNP Project Recommendations

Evidence-Based Cybersecurity Awareness Toolkit

Future Direction

HEALTH POLICY DEVELOPMENT

Vital component in translating evidence-based research into clinical practice

Health Policy

UNIVERSAL APPLICABILITY

DNP project is applicable to any healthcare organization that offers healthcare consumers online access to EHR

Project Versatility

WEAKEST LINK IN CYBERSECURITY

Human error has been identified as the weakest link in the chain of all cybersecurity measures - it demands continuous attention

Human Error

DNP Repository

DNP PROJECT REPOSITORY

Lack of similar DNP projects in DNP repositories and online databases

Inform

DISSEMINATION CHALLENGE

Additional research is needed to learn more about the effective methods of implementation and dissemination of the EBCST within the healthcare industry

(Fisher, 2018; Greengard, 2017; Hadlington, 2017; Kim, 2017; King et al., 2018; McAfee, 2018)

THANK YOU

References

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

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

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

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

References

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

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

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.

References

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 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.