2019

Cybersecurity best practices for management of protected health information in research environments

Carlye A. Hatwood

Cybersecurity Best Practices for Management of Protected Health Information in Research Environments

by

Carlye A. Hatwood MSN, MHA, BSN, RN

A DNP PROJECT

Submitted in partial fulfillment of the requirements for the
Degree of Doctor of Nursing Practice
to
The School of Graduate Studies
of
The University of Alabama in Huntsville

HUNTSVILLE, ALABAMA
2019

CYBERSECURITY BEST PRACTICES

In presenting this DNP project in partial fulfillment of the requirements for a doctoral degree from The University of Alabama in Huntsville, I agree that the Library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by my advisor or, in his/her absence, by the Director of the Program or the Dean of the School of Graduate Studies. It is also understood that due recognition shall be given to me and to The University of Alabama in Huntsville in any scholarly use which may be made of any material in this DNP project.

Cindy A. Hall

ud

03/06/2019

Date

DNP PROJECT APPROVAL FORM

Submitted by Carlye A Hatwood in partial fulfillment of the requirements for the degree of Doctor of Nursing Practice and accepted on behalf of the Faculty of the School of Graduate Studies by the DNP project committee.

We, the undersigned members of the Graduate Faculty of The University of Alabama in Huntsville, certify that we have advised and/or supervised the candidate on the work described in this DNP project. We further certify that we have reviewed the DNP project manuscript and approve it in partial fulfillment of the requirements for the degree of Doctor of Nursing Practice.

030619 Susan Alexander Committee Chair
(Date)

DNP Program Coordinator

College of Nursing, Associate Dean for Graduate Studies

College of Nursing, Dean

Graduate Dean

ABSTRACT
The School of Graduate Studies
The University of Alabama in Huntsville

Degree: Doctor of Nursing Practice College: Nursing

Name of Candidate: Carlye A. Hatwood

Title: Cybersecurity Best Practices for Management of Protected Health Information in Research Environments

Innovation and the persistence of cybercriminals seeking sensitive healthcare data, termed Protected Health Information (PHI), poses an ongoing security threat to healthcare organizations (Zissis, & Lekkas, 2010). Healthcare systems are utilizing cloud-based storage for PHI, which is emerging in academic settings where PHI is used for health research projects. Adoption of cloud-based storage platforms has created additional risks and threats to PHI (Evans, Maglaras, He, & Janicke, 2016). Healthcare is often lagging behind other industries in proactive cybersecurity methodologies (Gunter, Liebovitz, & Malin, 2011). A need for proactive tools and resources focusing upon the human element in protection of HPI in the cloud environment exists (Edwards, Hofmeyr, & Forrest, 2016). The DNP project achieved three objectives:

1. Development of an evidence-based toolkit on cybersecurity best practices for management of PHI within the academic health research environment.
2. Creation of a Data Management Security Plan for an academic health research environment that needs to manage PHI for analytics using cloud-based data storage services.
3. Construct a cloud-based storage environment for managing PHI for analytics, which

utilizes evidence-based industry standards from The Health Information Trust Alliance (HITRUST) Risk Management Framework, National Institute of Standards and Technology (NIST) cybersecurity and is in compliance with CMS guidelines. Locsin's Technological Competency as Caring in Nursing was used as the conceptual framework for the DNP project (Smith & Parker, 2015). The outcomes achieved from the DNP project can be utilized assist health researchers in academic environments in protecting PHI.

ACKNOWLEDGMENTS

Thank you to Dr. Alexander and Dr. Imsand for their support, input, feedback and guidance throughout the completion of this scholarly project. Thank you to all of the UAH nursing faculty members that assisted me in creating a solid foundation with their knowledge, tools, and support. To all of my family, friends, and colleagues I am appreciative, grateful, and humbled to have received their support, knowledge, laughter, and inspiration to conquer my educational endeavors.

TABLE OF CONTENTS

Page

SECTION I: DNP PROJECT

Cybersecurity Best Practices for Management of Protected Health Information in Research Environments

Identification of the Problem

Each day, thousands of attempts are made by cybercriminals to steal sensitive protected Health Information (PHI) data (Gunter, Liebovitz, & Malin, 2011). The risk of data breaches continues to rise as criminals become more strategic in their attempts to acquire PHI. Due to the wide array of databases that contain a variety of data types, provisioning of appropriate user access is one of the many security layers utilized within organizations. Identity and Access Management (IAM) is the process used within to manage user access for database systems within entities. IAM staff is typically responsible for assigning role-based access procedures, which help with monitoring compliance with Health Insurance Portability and Accountability Act of 1996 (HIPPA) regulations (Gunter, Liebovitz, & Malin, 2011).

End users may be required to have multiple login and password credentials if access to multiple data systems are needed, resulting in end users managing multiple sets of login credentials. The tasks of recalling usernames and passwords associated with the multiple sets of login credentials can create a serious risk for data breaches (Mansfield, 2003). The risk for data breaches occurs when staff utilize unsecure methods to remember their multiple sets of credentials (Mansfield, 2003). Examples of unsecure methods demonstrated by end users include: (a) writing down login/password information and putting in an unlocked desk drawer or taping it to a computer they often use, (b) utilizing someone else's login/password credentials because they forgot their own, and (c) using simple generic passwords (Mansfield, 2003). These actions can result in unintentional data breaches when username and password credentials are obtained by individuals' known as cybercriminals who are seeking to acquire protected data unlawfully.

Phishing is another tactic utilized by cybercriminals, who target unsuspecting staff through emails/phone calls. The contact to unsuspecting end users by these criminals, who seek to acquire login credentials, may seem quite legitimate and are a frequent source of unintentional data breaches (Centers for Medicare and Medicaid Services [CMS], 2009). The emails/phone calls appear to be legitimate and responding to them with the login/passwords can result in an unintentional data breach. This method is a low cost, low effort yet effective method for gaining access to secured data sources within healthcare entities.

Public and private sector healthcare facilities, and academic health research environments often utilize multiple software data applications for decision-making, clinical research, and business analytics, all of which may contain PHI. Database storage technology continues to advance providing additional options beyond onsite data servers. Many organizations are now increasing their use of cloud databases for securing PHI. This is often more cost effective, eliminates physical space constraints, and offers secure remote access (Zissis, & Lekkas, 2010). There is a wide array of cloud-based service providers offering the ability to store PHI data. The cloud-based storage environment creates another potential way for cybercriminals to attempt to acquire PHI or other sensitive data. The cybercriminals seek to utilize this PHI to commit financial and medical identity theft (Kwon & Johnson, 2014).

The rise in the use of cloud data storage for PHI requires enhanced data security policies and procedures (Zissis, & Lekkas, 2010). Centers for Medicare and Medicaid Services (CMS) and other healthcare agencies have specific guidelines for protection of PHI. Academic research environments that wish to use CMS data must meet compliance requirements defined by CMS, which necessitates the adoption of policies and procedures that describe how PHI is managed and accessed.

Despite increasing use of datasets containing PHI in academic health research environments, a lack of tools or guides for the development of cloud data security policies and procedures persists. Due to the lack of guidance and education regarding the protection of PHI in cloud-based platforms, workarounds are utilized (Cser, 2016). Workarounds may lead to an increased risk for organizations resulting in unintentional data breaches involving PHI. There is a need for assistance in constructing cloud-based research environments that balance safety with accessibility for personnel. In addition, it supports a need for the development of a toolkit, supported by a deep review of current evidence that will assist nurse researchers in accessing, migrating, and managing datasets containing valuable PHI for project needs. The purpose of the Doctor of Nurse Practice (DNP) project is to implement best-practice guidelines for cybersecurity in the design and deployment of a cloud-based platform using PHI in academic health research. Objectives for the DNP project are:

a. Creation of a Data Management Security Plan for an academic health research environment that needs to manage PHI for analytics specifically using cloud-based data storage services.
b. Construct a cloud-based storage environment for managing PHI for analytics, which utilizes evidence-based industry standards from the HITRUST Risk Management Framework, National Institute of Standards and Technology (NIST) cybersecurity and is in compliance with CMS guidelines.
c. Creation of cybersecurity best practices toolkit (framework) for management of PHI within the academic health research environment that

need to use PHI for analytics specifically using cloud-based data storage services.

Review of the Evidence

A review of the evidence was conducted, and the literature review included: ProQuest, EBSCOHost, MEDLine, and CINAHL. The keywords used during the search were: (a) cybersecurity, (b) data breaches in healthcare, (c) PHI data protection, (d) NIST 800-53, (e) cloud data storage, (f) academic research using PHI, (g) management on PHI, (h) cloud-based services, and (i) Health Information Trust Alliance. The initial number of articles retrieved was 2,987 publications. After applying filters: (a) language (English only), (b) peer-reviewed journals, and (c) dates within the past 10 years; the outcome decreased to 766. Utilization of the Boolean search criteria assisted in identifying the final 52 publications for review to support this project. The review of the literature identified three themes supporting the need for this project:

- increase in the risk of data breaches within healthcare by cybercriminals;
- use of cloud-based platforms for risk reduction and flexible data access; and
- description of common risk factors for data breaches including identity and access (IAM) configuration and human elements.

Healthcare Data Breaches

There continues to be a rise in the frequency of data breaches spanning a wide array of industries (Evans et al., 2016). In 2015, approximately 80 million records that included personal information was stolen from Anthem Inc., which is the second largest health insurer within the United States (Edwards, Hofmeyr, & Forrest, 2016). The US Office of Personnel Management reported that personal information of 21.5 million federal employees was compromised in 2015 (Edwards, Hofmeyr, & Forrest, 2016).

The rise in acuity and a fast-paced technology "rich" environment inadvertently creates potential risks of data breaches by staff. Healthcare, as a profession is often lagging behind other professions in implementing advanced cybersecurity prevention technology (Gunter, Liebovitz, & Malin, 2011). The electronic health record, although it has been associated with improved coordination of care, it also provides another risk for data leaking of PHI (Edwards, Hofmeyr, & Forrest, 2016).

Information security assessments are an important element in protecting data that organizations conduct to determine potential risks for data breaches. Data is categorized based on the type of information, and the level of security needed to protect the data. Federal, state, and local laws have been established in an effort to help prevent data breaches. Whenever data breach events occur, there are regulatory requirements that must be followed for disclosure of the event(s).

Growth in Cloud-Based Services

The rapid growth of the use of cloud-based services has created new challenges for the information security field in protecting data (Zissis, & Lekkas, 2010). Different methods of detecting threats and mitigation strategies to protect data in a virtual cloud-based environment are utilized when compared to physical storage of data onsite (Zissis, & Lekkas, 2010). Access and availability of data are two areas that increase vulnerability when storing data in a cloud-based setting (Zissis, & Lekkas, 2010). Cost-effectiveness, automation of data redundancy, and standardized central security controls are several benefits to utilizing cloud service providers (Zissis, & Lekkas, 2010).

The United States Federal government established the Federal Risk and Authorization Management Program (FedRAMP), which provide a standardized approach to authorization,

security assessment and continuous monitoring for cloud-based products and services (CMS, 2011). The Health Information Trust Alliance (HITRUST) Cybersecurity Framework (CsF) is an information security control model that utilizes risk analyses to assist organizations with strengthening their cybersecurity risk management (HITRUST Alliance, 2016). To ensure there are a consistent process for assessing CMS information systems, and the security of the information assets, a set of guidelines is set forth by the NIST (800-53 Revision A) (CMS, 2009). In addition, CMS requires specific encryption standards for data at rest and in transit when computing in the cloud to further protect PHI (CMS, 2011).

Human Risk and IAM

Despite the advancements within cybersecurity over the past 25 years, there is still a risk factor from human error made by an employee who is misguided and inadvertently leaks protected data (Evans, Maglaras, He, & Janicke, 2016). Cybercriminals capitalize on human error and gaps identified in improving the education for healthcare staff on how to protect PHI. The human risk factor for potential data breaches is a global concern. There was a rise in healthcare data breaches by 101% between 2013 and 2014, with human error identified as the root cause in 93% of them (Evans et al., 2016). Cybercriminals utilize PHI data to commit financial and medical fraud (Kwon, & Johnson, 2014). Faculty, nurses and other healthcare providers need have to policies and procedures, which guide their practice surrounding appropriate access, utilization, and overall management for protecting PHI.

Despite all of the technical security measures organizations put in place, one critical security risk creates a bigger threat. The human element often poses the greatest risk factor as it is considered to be the weakest link in securing the environment (CMS, 2009). Managing user access to multiple databases can become challenging due to many factors including (a) type of

data (being stored), (b) level of security needed for the type of data, (c) infrastructure capability, and (d) internal policies (Gunter, Liebovitz, & Malin, 2011).

User access is compounded by multiple database systems utilized to provide care, within the hectic and complex healthcare environment. Hoping to capitalize on the human vulnerability to gain PHI, social engineering tactics are used by criminals who: (a) pose as help desk personnel, (b) use phishing emails, and (c) other methods (CMS, 2009). There is a gap in the literature review for proactive tools and resources that focus on the human element need for guidance, education on cybersecurity, particularly in the cloud-based environment (Edwards, Hofmeyr, & Forrest, 2016).

Implementation

Setting

The project setting was the College of Nursing for a university in the southeastern United States. A commercially-available cloud platform vendor was used for the construction of the PHI data storage environment.

Timeline

The project was completed 10 weeks commencing after approval was received from the Institutional Review Board.

Conceptual/Theoretical Framework

The conceptual framework supporting used to support this project was Locsin's Technological Competency as Caring in Nursing. It is based on creating a seamless synchronization between technologies and caring in nursing (Smith, & Parker, 2015). A cybersecurity toolkit supporting cloud-based analytics of PHI within an academic research will help in preventing potential data breaches. Having an environment that enables analytics of PHI,

within an academic research setting, can provide valuable insight and guidance that can potentially impact nursing practice by "knowing" of the patient, which could improve patient quality and outcomes (Smith, & Parker, 2015).

Achieving technological competency occurs with an enhanced understanding and utilization of PHI and protection of this sensitive data within a cloud-based environment. It provides the ability to obtain PHI data sets from CMS, which can be instrumental with population health predictions, and extrapolation of the data that can lead to an enhanced the understanding of the patients and transformation of nursing practice when utilizing the technology (Locsin, & Purnell, 2015). There are five assumptions that guide this theory:

- Persons are caring by virtue of their humanness.
- The ideal of wholeness is a perspective of unity.
- Knowing persons is a multidimensional process.
- Technologies of health and nursing are elements for caring.
- Nursing as a discipline and a professional practice (Locsin, & Purnell, 2015).

The data analytics and cloud- based technology provides a gateway to explore further the knowledge of the person using PHI for data analytics with the unpredictable and ever-changing pathways of humans (Locsin, & Purnell, 2015). Due to the paradigm shift with the healthcare reimbursement insurance model, hospitalizations are often shorter while the acuity of the patients has increased. Using technology as a pathway for analytics of PHI the future of nursing practice could potentially include an increase in the efficiency of time spent on the care of patients. Expanding the capabilities of data analytics is essential as the healthcare landscape for nursing practice is changing. With the creation of a cybersecurity best practices for management of PHI

toolkit (framework), the academic health research environment will be able to leverage cloud-based data storage services technology with the expansion of analytics with PHI.

Safety/Confidentiality

The nature of the project does not require the use of human subjects or the use of secondary data obtained from human subjects.

Objectives

The literature review provided the evidence-based support for the three identified objectives that were implemented for this DNP project. Review and cross-reference of the evidence-based cybersecurity compliance standards resulted in the creation of a Sample Data Management Plan (SDMP). The project investigator compared the cybersecurity compliance requirements for healthcare data acquisitions from CMS versus Public data. The cybersecurity elements applicable to PHI/PII data are generally more stringent when compared to elements applied for general publicly available data.

The investigator completed the construction (configuration) of the Cloud Service Provider (CSP) platform using the SDMP that focused on cybersecurity elements specific to PHI/PII data sets, applied to publicly available data sets. Finally, the investigator designed a toolkit for the CSP environment for those who may not have the knowledge of custodian of the data to ensure compliance with data protection criteria. The timeline for the implementation of all three objective was achieved by January 31, 2019.

Sample Data Management Plan (SDMP)

The creation of an SDMP (Appendix B) for an academic health research environment that needs to manage PHI for analytics specifically using cloud-based data storage services was completed. The SDMP utilized applicable elements related to protecting PHI/PII found within

the CMS Data Management Security guidelines, NIST Standards 800-53, and FedRamp standards. The elements identified in the SDMP were applied to publicly available data sets for the configuration within the CSP environment.

Construction of a Cloud-Based Storage Environment

The construction of a cloud-based storage environment for managing PHI for analytics utilizing the SDMP was achieved. The construction of the cloud-based storage environment was done within a commercially available CSP environment. The CSP was constructed to be in a ready state to manage PHI data analysis within it. The SDMP was utilized to guide the construction of the CSP.

PHI Toolkit

The creation of cybersecurity best practices toolkit (framework) for management of PHI within the academic health research environment that need to manage PHI for analytics specifically using cloud-based data storage services was completed. The evidence for the completion of this objective includes a flow chart visual guide (Appendix C) and PHI toolkit (Appendix D).

Evaluation

Satisfactory completion of the DNP Project stems from meeting the objectives to produce the deliverables and construct the storage platform.

Sample Data Management Plan

The outcome for this objective was executed with the creation of a cybersecurity Sample Data Management Plan SDMP (Appendix B). The SDMP was designed for an academic health research environment that needs to manage PHI for analytics specifically using cloud-based data storage services. The SDMP was created from elements within several cybersecurity evidence-

based publicly available data sources. The SDMP contains applicable elements applicable to protect PHI/PII found within the CMS Data Management Security guidelines, NIST Standards 800-53, and FedRamp standards. The Research Data Assistance Center (ResDAC, 2019) is a CMS contractor that was established in 1996 (ResDAC, 2019). Government, non-profit, for profit and academic researchers that are interested in CMS data can receive free assistance from them. ResDAC provides a number of tools, and resources for managing PHI CMS data that was leveraged with the creation of the SDMP (ResDAC, 2019). The elements identified in the SDMP were applied to publicly available data sets for the configuration within the CSP environment.

There are four major process categories outlined within the CMS Data Management Security Plan provided by ResDAC: (a) storage of data files, (b) electronic transmission/data sharing, (c) data breaches and (d) data destruction (ResDAC, 2019). In addition to the CMS Data Management Security Plan, elements from other evidence-based cybersecurity guidelines found within NIST Standards 800-53, and FedRamp standards were utilized. Each of the elements within the SDMP has a series of questions/guidelines that were used in the construction/configuration of the CSP storage environment. Each of these elements provides guidance for ensuring safeguards are in place for security and privacy with PHI/PII data (CMS, 2011). It is important to note that cybersecurity guidelines are continuing to be updated. The shift within healthcare with the use of cloud-based storage and changes to the tactics used by cybercriminals requires continual vigilance to protect PHI. The SDMP was used as a guide for the construction of the cloud-based storage environment.

Construction of a Cloud-Based Storage Environment

The construction of a cloud-based storage environment for managing PHI for analytics, which utilizes evidence-based industry standards was completed. Standards from the HITRUST

Risk Management Framework, FedRAMP, and NIST cybersecurity framework were utilized to ensure compliance with CMS guidelines was met. The CSP was constructed to be in a ready state to manage PHI data analysis within it.

The SDMP (Appendix B) was utilized to guide the construction of the CSP. It can be used with different vendors, although there may be some vendor specific nuances that may vary. There were also proprietary properties within the CSP that limited some of the self-service manipulations of it. Within the CSP there is a cloud-based application, which is utilized for creating a data warehouse, allowing the user(s) to store data sets, perform of data analysis, queries, and generate reports within the secure environment (Google Cloud "What is BigQuery", 2019). This application was utilized to be able to import a publicly available data set used for validation of the security configuration settings. The outcome for this objective was the implementation of the cloud-base storage environment, and it was completed within a CSP environment.

Security and access controls configuration. Understanding the type of data, setting, user(s), and access requirements was important to assess for the configuration process (Cser, 2016). It was identified that the data would be various PHI data sets for analytics, which would be utilized by a single user in an academic research environment. The data analysis would occur only within the cloud-based storage environment so no additional onsite data storage was needed.

Cloud-based security failures or risks occur when there is an intentional or unintentional data breach, unavailability of data, or when there is a loss of confidentiality (Soman, 2011). It is vital to assess the security and access controls within cloud-based platforms for potential vulnerabilities. The availability of cloud-based environments allows the data to be accessed

from almost any computer with internet capability creates a security risk. Viruses and other malware including worms and trojans can potentially be transmitted from the host computer to the cloud-based platform (Soman, 2011). The viruses may also capture the keystrokes of the user, and potentially lead to the cybercriminals obtaining login and password information (Soman, 2011). Healthcare organizations, similar to other entities must protect their data and be vigilant against potential cyber-attacks.

Performing a security and access control assessment is one method that is used to decrease the risk associated with storing PHI data in physical or cloud-based storage environment (Murphy, 2015). Security and access controls specific to the CSP storage environment were completed. Within the CSP, IAM settings, authentication, role selection, encryption security, and risk standards were validated to ensure compliance with CMS guidelines. The CSP vendor utilizes evidence-based industry standards from the HITRUST Risk Management Framework, NIST cybersecurity, and is in compliance with CMS guidelines. The CSP maintains a HITRUST certification (Google Cloud "Standards, Regulations & Certifications", 2017). In addition to HITRUST validation, the CSP is FedRamp authorized. FedRamp is a government-wide program that created standardization for assessing security, authorization, and monitoring for cloud-based services and products (FedRAMP, 2018).

The CSP enlisted the services of Coalfire Systems a Third-Party Assessment Organization (3PAO) to perform a comprehensive assessment of the security control features for FedRAMP compliance (Coalfire, 2018). The results are documented in a FedRAMP Security Assessment Report (SAR). It was notated that CSP is compliant with FedRAMP Moderate baseline standards that are measured against the NIST SP800-53 Revision 4 security controls (Coalfire, 2018).

The Moderate level of compliance examines the security measures used by the CSP to prevent "loss of confidentiality, integrity, and availability which would result in serious adverse effects on customer operations, assets, or individuals" (Coalfire, 2018). The Coalfire Assessment documentation and verification from the FedRAMP government website served as validation for this CSP attainment of FedRamp authorization (FedRamp, 2019).

Encryption significantly reduces the risk of the information being viewed by unauthorized individuals with security controls to protect the data (Murphy, 2015). The security standards within the CSP align with the CMS federal requirements for data at rest and in transit (Google Cloud "Data in Transit", 2017). CSP offered the option for customer-managed encryption keys if the customer wanted to manage their own encryption process (Google Cloud "Encryption at Rest", 2018) . The CSP has a comprehensive multi-layer security infrastructure in place for data protection (Google Cloud "Infrastructure Security Design Overview", 2018). For this DNP project objective, the best practice guidelines provided by the CSP with their embedded encryption services were utilized. It was verified that the CSP met the 256-bit standard encryption to protect the data at rest and in transit which is required by CMS for PHI/PII data (CMS, 2011).

Access control is an important security control aspect that some organizations overlook, which can pose a security risk (Bond, 2015). It is important to understand who will need to access this data and from where will they be accessing this data. Supporting infrastructure that may include additional computer terminals and internet bandwidth assessment is important (Bond, 2015). For this project, the CSP would be adequately supported by the University's existing infrastructure.

Understanding who will need access, and their role with the analysis of the data, was a key component for configuring the CSP environment. Considering the needs of the individual related to the prospective data, it was determined how to identify the appropriate role within CSP to assign. Role-based access models are frequently used within healthcare environment (Murphy, 2015). This type of access model allows for the level of access to be established based on the role of the individual (Murphy, 2015). The role-based model for access was utilized within the CSP (Google Cloud "Using IAM Securely", 2019). Selecting the appropriate role for the individual is based on the expectations on capability to carry out certain functions such as: (a) data analysis, (b) writing code sequences, (c) exporting data, (d) importing data, (e) report writing, or (f) viewing the data outcomes (Murphy, 2015).

Ingress of a public dataset into the CSP cloud-based application within the secure environment was completed. Migration of the public dataset to the CSP storage provided the foundation for implementing a role-based configuration within the CSP environment. The administrator role is the highest level within the storage environment providing the overarching access to analytics, applications, and additional role additions or deletions. This role was configured with the CSP vendor at the execution of services for this project. Three individual roles were successfully established through the IAM configuration process within CSP: (a) Owner, (b) Editor, and (c) Viewer. The Owner role can create and assign roles within the CSP that are appropriate for each individual. In addition, the owner can read create, update, and delete both datasets and dataset tables (Google Cloud "Understanding Roles", 2019) .

The Owner has the highest level of data access with the ability to carry out the functions of the Editor and Viewer (Google Cloud "Understanding Roles", 2019). The Editor has the next level of data access and control with some of the functions that are the same as the Owner. The

Editor has the ability to manipulate the data (Google Cloud "Understanding Roles", 2019). The Viewer role has the least level of access with the ability to only view the data (Google Cloud "Understanding Roles", 2019). Selecting the appropriate role for the individual is based on the expectations on capability to carry out certain functions such as: (a) data analysis, (b) writing code sequences, (c) exporting data, (d) importing data, (e) etc.

PHI Toolkit

A cybersecurity best practices for management of PHI toolkit was created (Appendix D). The toolkit is based on similar ones developed in healthcare and other industries and incorporated four major elements to address cybersecurity risks. The four evidence-based cybersecurity foundational regulatory elements pertinent to this project included in the toolkit are: (a) HIPPA, (b) NIST Standards, (c) CMS, and (d) FedRamp.

The scope of the toolkit focused on the cybersecurity elements for CSP environment construction for PHI/PII for analytics by academic researchers. The primary goal of the toolkit was to enhance the knowledge of the data owner (custodian) on various resources, and to provide best practices for protecting data. The toolkit contains background, purpose, audience, intended use, role of toolkit, and implementation phases (awareness, assessment, implementation, education). The outcome of this objective was successfully completed.

Application to Practice

The continuous technological advancements within the healthcare environment require nurses to determine the potential implications for the nursing profession. Technology is becoming more and more intertwined within the nurse practice settings making it vital for nurses to understand how to use it, how to protect PHI, and how it will impact nursing care and services. Due to the increased use of cloud/remote storage, within various healthcare entities for

sensitive patient data that is collected, there is a need to ensure policies/procedures are in place. Nursing professionals will need these policies/procedures to guide practices related to data access security for the vast amount of patient data that is collected and stored.

The need for development or refinement of data security policies/procedures to protect sensitive healthcare data stored in a cloud-based environment is part of the toolkit for the DNP project. The toolkit with policies/procedures examples can be a template for other healthcare entities. The advancement of nursing informatics and healthcare technology provides a platform for nursing leaders within clinical practice. *The American Organization of Nurse Executives* (AONE) competency areas supporting this project are Information Management and Technology, Risk Management, and Patient Safety (AONE, 2015).

A deeper understanding of information technology advancements, and the necessity of cybersecurity in using PHI are consistent with competencies of the DNP prepared nurse. Healthcare systems and educational entities strive to improve patient care and meet the ever-changing healthcare landscape (Rutledge, Haney, Bordelon, Renaud, & Fowler, 2014). The DNP nurse will be able to leverage their advance scholarly knowledge to assist in bridging the gap between technology and patient care. Proficiency with technologies and systems used to address gaps in care is necessary for doctorally prepared nurses to influence the future of the nursing profession and advocate for continued quality and safety in patient care (Lilly, Fitzpatrick, & Madigan, 2015).

Additionally, the doctorally-prepared nurse can use clinical expertise in addressing variances found in data, assessing end-user adaptation, and formulating critical questions to advance evidence-based practice capabilities of the technology (Schoville, & Titler, 2015). Cloud-based data storage can also set the foundation for the development of additional technology platforms used to share information. A Health Information Exchange (HIE) is an example of this technology where data is

compiled from various health information systems, allowing for obtaining a more comprehensive patient profile (Zaidan, et al., 2015).

Barriers

Several potential barriers have been identified related to this project. Cloud-based storage is an example of innovative technology. Ensuring the security of PHI requires organizations to accept or reject the new cybersecurity knowledge. Roger's innovation-diffusion model's foundation analyzes the acceptance or rejection of the new innovative technology (Lee, 2004). Leveraging Roger's model at a community level can assist in mitigating resistance to change that can improve the sharing of patient information. There will need to be a strategic plan to manage the potential barriers with the impending changes (Wren, 1995).

Nursing informatics. Bridging the gap with technology is impacting nursing practice requiring adaptation to protect PHI while learning something new. Nursing practice is evolving with the use of cloud-based data storage to perform predictive analytics, population health management, improve efficiency, and to enhance patient safety (McGonigle, & Masterian, 2018). Within healthcare, there is the ability to access a large amount of information also known as Big Data, to be pulled from multiple resources and cross-referenced through advanced analytics. This information would provide meaningful data for nurses and clinicians to have additional knowledge that could lead to improved patient outcomes (Linnen, 2016). It is integral for nurses to understand what informatics is, the cross-section with data and how this applies within their nursing practice (Nagle, et al., 2017). The D (data), I (information), K (knowledge), W (wisdom) –DIKW framework is the evolution of data, which is a small element through the continuum leading to wisdom (McGonigle, & Masterian, 2018). The progression of data to meaningful information, which leads to knowledge that can be integral for making clinical

decisions, is a learning curve for nursing and healthcare staff (McGonigle, & Masterian, 2018). Cloud-based storage with appropriate cybersecurity can be transformational in the care pathways chosen for our patients.

Terminology and technology. Cybersecurity and cloud-based storage introduce a new model of terminology that will need to be integrated into nursing practice. The creation of a foundational building block is needed to effectively align this new technology language with ANA approved language use and clinical best practices (McGonigle, & Masterian, 2018). The new terminology that nursing will be exposed to as a result of this technological paradigm shift in healthcare is a potential barrier. The complexity of healthcare can make it difficult for nurses at all levels to take the time to learn and understand this new terminology. In addition, nursing and healthcare researchers will need to understand how to access, utilize, and practice within a cloud-based technology environment. This technology and cybersecurity framework are not designed to replace the need for human thinking and processing of the information, but rather to be an additional resource. Technology is not perfect and will potentially fail, which will require the need for a backup plan to ensure quality patient care continues.

Dissemination

The cybersecurity best practices for management of PHI toolkit (framework) and completed Data Management Security Plan will be two mechanisms for the dissemination of this DNP project. The flow chart guidance overlay document will provide a high-level pathway to share the work of this DNP project with other academic research institutions. In addition, the outcomes of this project have been shared with the business intelligence director and data security leader of a county health system. Although the county health system does have policies and procedures in place for healthcare data security, they benefited from the sharing of

information on this topic. Cybersecurity in healthcare requires continual monitoring, revision of policies/procedures, and implementation of mechanisms to ensure the security of healthcare data.

Additional opportunities may present itself after completion of this DNP project to further disseminate the outcomes. Dissemination may include scholarly journals, applicable professional conferences with presentations, poster displays, and sharing findings with other remote/rural entities that may not be aware of advancements in cloud-based services. The scholarly work done as a DNP prepared advanced practice nurse must be adequately disseminated to positively affect nursing practice and patient outcomes.

Sustainability

Tools. Sustainability involves attaining and maintaining nursing practice competency with technology. There is a vital interdependency with clinical scholarship and research (Fitzpatrick, & Whall, 2005). Nurses and clinical researchers within the academic entities need to remain abreast of the increased use of cloud-based services and the importance of cybersecurity. Supporting information literacy, that will aide in the growth and sustainability of this DNP project, will include the following tools: (a) flow chart overview guide, (b) cybersecurity toolkit, and (c) Sample Data Management Plan template (Zabel, 2004).

DNP Mentorship. The DNP project is only one example of the continued growth, evidence-based research, technology, and practice standards, which are influencing the nursing profession. One of the important roles of APN/DNPs, based on the acquisition of advanced knowledge, is to guide practice and share this new knowledge with professional colleagues to further improve the quality of care and safety of the patients (AACN, 2015). APN/DNPs are leaders who are integral to shaping the culture of the organization with the power of effective communication in sharing new knowledge (Yukl, 2010). Mentorship is another methodology in

which the foundation for sustainability of the DNP project can occur.

Effective mentorship requires effective communication, establishment of goals, mutual respect, willingness to learn, willingness to share, and active listening (Thompson, 2008). Mentorship allows the APN/DPN to impart new knowledge, DNP project outcomes, and advancements in the nursing profession with new nurses. There are many tools and guides to assist APN/DNP nurses to become effective mentors (Dreher, & Glasgow, 2011). DNP/APN(s) can set the foundation for sustainability of this project as a mentor and can be instrumental in bridging generational or cultural gaps by teaching (Billings, & Halstead, 2012).

SECTION II: DNP PROJECT PRODUCT

I. Professional Journal Selection

Scope of Journal

The Online Journal of Nursing Informatics (OJNI) is a professional, international quarterly peer-reviewed journal that is available complimentary in an electronic format (OJNI, 2017). OJNI was launched in 1996 and was acquired by the Healthcare Information and Management Systems Society (HIMSS) Foundation in 2014 attracting readers throughout 49 countries (OJNI, 2017).

B. Aims of Journal

The OJNI focuses on nursing informatics and the application to the field of nursing to enhance the knowledge and practice of nurses in diverse settings (OJNI, 2017). It is a volunteer-led online journal that supports submissions from nursing scholars, nursing leaders, students, and nurse informaticians (OJNI, 2017). The aim of the OJNI is to address both the practical and theoretical areas of nursing informatics in their articles (OJNI, 2017). The author guidelines have been provided directly from OJNI for submission (Appendix A).

References

American Association of Colleges of Nursing (AACN) (2015). The doctor of nursing practice: Current issues and clarifying recommendations. Retrieved from http://www.aacnnursing.org/Portals/42/DNP/DNP-Implementation.pdf?ver=2017-08-01-105830-517.

American Organization of Nurse Executives (AONE). (2015). AONE Nurse Executive Competencies. Chicago, IL: Retrieved from: http://www.aone.org/resources/nurse-leader-competencies.shtml.

Billings, D. & Halstead, J. (2012). *Teaching in nursing: A guide for faculty (4th ed.)*. St. Louis, MO: Elsevier/Saunders.

Bond, J. (2015). *The enterprise cloud best practices for transforming legacy IT.* Sebastopol, CA: O'Reilly Media.

Carnegie Mellon University (2016). *Guidelines for data classification.* Retrieved from https://www.cmu.edu/iso/governance/guidelines/data-classification.html.

Centers for Medicare & Medicaid Services (CMS) (2018). *Data administration.* Retrieved from https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/DataAdmin/index.html.

Centers for Medicare & Medicaid Services (CMS) (2009). *Information security assessment procedure.* Retrieved September 10, 2018, from https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information Technology/InformationSecurity/Downloads/Assessment_Procedure.pdf.

Centers for Medicare & Medicaid Services (CMS) (2011). *Cloud computing standard.* Baltimore, MD: Office of the Chief Information Security Officer. Retrieved from Technology/InformationSecurity/Downloads/RMH_VIII_32_Cloud_Computing.pdf.

Centers for Medicare & Medicaid Services (CMS) (2016). *Data disclosures and Data Use Agreements (DUAs).* Retrieved from https://www.cms.gov/Research-Statistics-Data-and-Systems/Files-for-Order/Data-Disclosures-Data-Agreements/Overview.html.

Cser, A. (2016). *Create your cloud security technology strategy and road map current security strategies and road maps are inadequate to mitigate cloud risk.* Cambridge, MA: Forrester Research, Inc.

Coalfire (2018). *Coalfire Assesses Google Cloud Platform for FedRAMP JAB Authorization.* Retrieved from https://www.coalfire.com/News-and-Events/Press-Releases/Google-Cloud-Platform-FedRAMP-JAB-Authorization.

DHHS Office for Civil Rights (2016). *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework.* Retrieved from https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

Dreher, H. M. & Glasgow, M.E. S. (2011). *Role development for doctoral advanced nursing practice.* New York New York, NY: Springer Publishing Co.

Edwards, B., Hofmeyr, S. & Forrest, S. (2016). *Hype and heavy tails: A closer look at data breaches.* Retrieved from https://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_edwards.pdf.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667-4679. doi:http://dx.doi.org.elib.uah.edu/10.1002/sec.1657.

FedRAMP (2018). *CSP Authorization Playbook.* Retrieved from https://www.fedramp.gov/assets/resources/documents/CSP_Authorization_Playbook_Getting_Started_with_FedRAMP.pdf.

FedRAMP (2019). *FedRamp authorized products FedRamp at a glance*. Retrieved from https://marketplace.fedramp.gov/#/products?sort=productName.

Fitzpatrick, J. J. & Whall, A. L. (2005). *Conceptual model of nursing: Analysis and application* (4th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Google Cloud (2017). *How Google Protects Your Data in Transit.* Retrieved from https://cloud.google.com/blog/products/gcp/how-google-protects-your-data-in-transit.

Google Cloud (2017). *Standards, Regulations & Certifications*. Retrieved from https://services.google.com/fh/files/misc/2017_google_services_800-53_letter.pdf.

Google Cloud (2019). *Using IAM Securely*. Retrieved from https://cloud.google.com/iam/docs/using-iam-securely.

Google Cloud (2019). *Understanding Roles*. Retrieved from https://cloud.google.com/iam/docs/understanding- roles.

Google Cloud (2019). *What is BigQuery.* BigQuery. Retrieved from https://cloud.google.com/bigquery/what-is-bigquery.

Gunter, C. A., Liebovitz, D., & Malin, B. (2011). Experience-based access management: A life-cycle framework for identity and access management systems. *IEEE Security & Privacy*, *9*(5), 48–55. http://doi.org/10.1109/MSP.2011.72.

Healthcare Information and Management Systems Society (HIMSS) (2019). *Online Journal Nursing Informatics submissions: Author guidelines.* Retrieved from https://www.himss.org/ojni/author-submission-guidelines?ItemNumber=28276.

HITRUST Alliance Inc. (2016) *Healthcare sector cybersecurity implementation guide v1.* Retrieved from https://www.uscert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly, 38*(2), 451. Retrieved from https://elib.uah.edu/login?url=https://search-proquest-com.elib.uah.edu/docview/1521627277?accountid=14476.

Lee, T. (2004). Nurses' adoption of technology: Application of rogers' innovation-diffusion model. *Applied Nursing Research : ANR, 17*(4), 231-238. Retrieved from https://elib.uah.edu/login?url=https://search-proquest-com.elib.uah.edu/docview/67139615?accountid=14476

Lilly, K., Fitzpatrick, J., & Madigan, E. (2015). Barriers to integrating information technology content in doctor of nursing practice curricula. *Journal of Professional Nursing : Official Journal of the American Association of Colleges of Nursing, 31*(3), 187-199. doi:http://dx.doi.org.elib.uah.edu/10.1016/j.profnurs.2014.10.005.

Linnen, D. (2016). The promise of big data: Improving patient safety and nursing practice. *Nursing2016, 46*(5), 28-34.

Locsin, R. C., & Purnell, M. (2015). Advancing the theory of technological competency as caring in nursing: The universal technological domain. *International Journal for Human Caring*, *19*(2), 50-54.

Mansfield, S. (2003). Password proliferation alleviated. *Security, 40*(9), 39-40. Retrieved from https://elib.uah.edu/login?url=https://search-proquest-com.elib.uah.edu/docview/197800984?accountid=14476.

McGonigle, D. & Mastrian, K. (2018). *Nursing informatics and the foundation of knowledge*(4th ed.). Burlington, MA: Jones & Bartlett Learning.

Murphy, S.P. (2015). *Healthcare information security and privacy.* New York New York, NY: McGraw-Hill Education.

Nagle, L., Sermeus, W., & Junger, A. (2017). Evolving role of the nursing informatics specialist. *Studies in Health Technology and Informatics, 232*, 212-221.

National Institute of Standards and Technology (NIST) (2017). *About NIST.* Retrieved from https://www.nist.gov/about-nist.

National Institute of Standards and Technology (NIST) (2017). *Policies and notices.* Retrieved from https://www.nist.gov/policies-notices.

National Institute of Standards and Technology (NIST) (2018). *Cybersecurity framework.* Retrieved from https://www.nist.gov/cyberframework/framework.

National Institute of Standards and Technology (NIST) (2013). *NIST special publication 800-53 revision 4 security and privacy controls for federal information systems and organizations.* Retrieved from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf.

National Institute of Standards and Technology (NIST) (N.D). *Special publication 800-53 (Rev. 4) security controls and assessment procedures for federal information systems and organizations AC-1 access control policy and Procedures*. Retrieved from https://nvd.nist.gov/800-53/Rev4/control/AC-1.

Online Journal of Nursing Informatics (OJNI) (2017). *Welcome to OJNI.* Retrieved from https://ojni.org/index.html.

Research Data Assistance Center (ResDAC) (2019). *Data management plan guidelines.* Retrieved from https://www.resdac.org/sites/resdac.umn.edu/files/CMS%20DPSP%20Data%20Management%20Plan%20Guidelines_1.pdf.

Research Data Assistance Center (ResDAC) (2019). *Data privacy safeguard program office of enterprise data & analytics division of data and information dissemination overview.* Retrieved from https://www.resdac.org/sites/resdac.umn.edu/files/CMS%20DPSP%20Program%20Overview_1.pdf.

Rutledge, C. M., Haney, T., Bordelon, M., Renaud, M., & Fowler, C. (2014). Telehealth: Preparing advanced practice nurses to address healthcare needs in rural and underserved populations. *International Journal of Nursing Education Scholarship, 11* doi:http://dx.doi.org.elib.uah.edu/10.1515/ijnes-2013-0061.

Schoville, R. R., & Titler, M. G. (2015). Guiding healthcare technology implementation: A new integrated technology implementation model. *Computers, Informatics, Nursing : CIN, 33*(3), 99-107; quiz E1. doi:http://dx.doi.org.elib.uah.edu/10.1097/CIN.0000000000000130.

Siedlelman, L. (2019). *Differences between RIF, LDS, and PUF data files.* Retrieved from https://www.resdac.org/articles/differences-between-rif-lds-and-puf-data-files.

Smith, M. C. & Parker, M. E. (2015). *Nursing theories and nursing practice* (4th ed.). Philadelphia, PA: F.A. Davis.

Soman, A.K. (2011). *Cloud-based solutions for healthcare IT.* Ensfield, NH: Science Publishers.

Stanford University (2015). *HIPAA security: Security management policy.* Retrieved from https://uit.stanford.edu/security/hipaa/security-management-policy.

Stanford University (N.D). *Risk classifications* Retrieved from https://uit.stanford.edu/guide/riskclassifications.

Thompson, L. (2008). *Making the team* (3rd ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Wren, J. (1995). *The leader's companion: Insights on leadership through the ages.* New York: The Free Press.

Yukl, G. (2010). *Leadership in organizations* (7th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

Zabel, D. (2004). A reaction to information literacy and higher education. *Journal of Academic Librarianship, 30 (1), 17-21.*

Zaidan, B. B., Haiqi, A., Zaidan, A. A., Abdulnabi, M., Kiah, M. L. M., & Muzamel, H. (2015). A security framework for nationwide health information exchange based on telehealth strategy. *Journal of Medical Systems, 39*(5), 51. doi:http://dx.doi.org.elib.uah.edu/10.1007/s10916-015-0235-1.

Zissis, D., & Lekkas, D. (2010). Addressing cloud computing security issues. *Future Generations Computer Systems, 28* (3), 583-592.doi:https://doi.org/10.1016/j.future.2010.12.006.

APPENDIX A

OJNI Author Guidelines

OJNI Submissions: Author Guidelines-Directly From OJNI: https://ojni.org/index.html.

We welcome voluntary submissions on a rolling basis. Manuscripts must represent original, unpublished material and represent a functional area of nursing informatics. Letter of inquiries to the OJNI Editorial Team are welcome. Manuscripts undergo a double blind, peer review process. A decision to publish is based upon the reviews.

Manuscript Requirements

- Submit a blind copy (no author information should appear on the manuscript)
- Submit manuscript according to the APA 6th edition style guide
- Submit Manuscript Overview: Provide a 250 word abstract, five key words and identify themes, compelling quotes and statistics as a standalone file
- Submit images, tables and graphs separately. Tables and graphs must be submitted as an image (no wider than 500 pixels). Click here to learn how to convert tables/ graphs into an image.

Manuscripts are received with the understanding that they have not been previously published and are not under consideration for publication in any other journal. All manuscripts are subject to editing. The author assumes final responsibility for the content of the manuscript, including responding to author queries.

Cover Letter Requirements

- Title of Manuscript
- Name of authors (include credentials)*
- Contact information including: address, phone number, email address

*The principal author will be contacted regarding the manuscript.

References

OJNI requires all references to be submitted in APA 6th edition format. APA requires the references to be cited in two different ways, within the text and in a reference list at the end of the paper.

Please ensure that all citations are complete before submission and are no more than five years old. For examples, rules and requirements, consult the 6th edition of the *Publication Manual of the American Psychological Association.*

Submitting the Manuscript

OJNI converted to an electronic submission and peer review system. To review detailed instructions on how to submit your manuscript, click here. To submit your manuscript, click here .

If you do not receive confirmation of your submission within 5 days, please contact OJNI.

Principal Author's Responsibilities

Upon acceptance for publication, the principal author will:

- Approve the e-galley (electronic proof) and assume responsibility for the accuracy of the material as it appears
- Submit written e-mail approval for the e-galley as edited within the timeframe designated by OJNI
- Provide a biographical sketch for each author
- Grant permission to publish the manuscript and assign issue copyright to OJNI in writing via-email

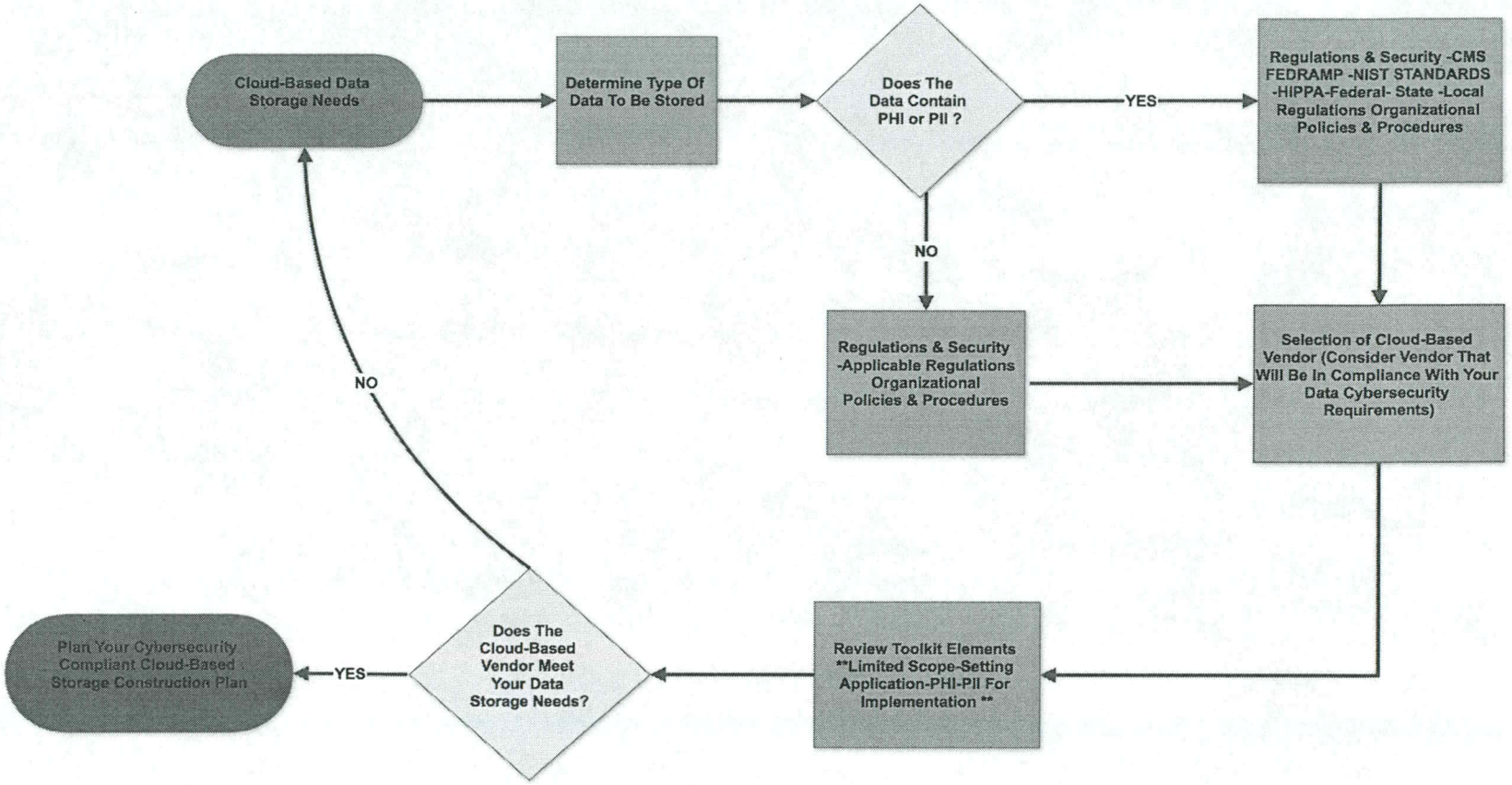
APPENDIX B

Sample Data Management Plan - PHI/PII Cybersecurity Cloud-Based Implementation

Element	CMS (ResDAC, 2019)	FedRAMP (FedRamp, 2018)	NIST 800-53 Standards (NIST, 2018)	Action/Validation
torage and Protection of PHI/PII Data Files	**Storage of CMS Data Files- CMS** 1.Who will have the main responsibility for organizing, storing, and archiving the data? 2. Explain the infrastructure (facilities, hardware, software, other) that that will secure the CMS data files 3. Explain your organization's system or process to track the status and roles of the research team. 4. Describe your organization's physical and technical safeguards used to protect CMS data files (including physical access and logical access to the files). **CMS- Cloud Computing Security** The cloud portion of a CMS system may receive an Authorization to Operate (ATO) from the General Services Administration (GSA) or the Federal Risk and Authorization Management Program (FedRAMP)-	Federal Risk and Authorization Management Program (FedRAMP)- Authorization to Operate (ATO)- Alignment crosswalk with NIST 800-53 Standards	**MEDIA PROTECTION- CRYPTOGRAPHIC PROTECTION-NIST 800-53 Standards** The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	The University determined that the single data owner will be responsible for organizing, storing, and archiving the data. A CSP was selected to be the infrastructure that will secure the CMS data files. The role-based access management system within the CSP storage environment will be the process for potential future roles of a research team. Three potential roles: Owner, Editor, Viewer was added in the CSP storage environment and tested with publically available data. The CSP vendor selected is compliant with FedRAMP ATO standards and it was validated on the FedRAMP government website. The CSP vendor selected was compliant with the encryption (cryptographic) data mechanisms at rest and in transit as required by CMS and aligned in meeting NIST 800-53 Standards.
ata ansmission/Sharing	**Data Sharing, Electronic Transmission, Distribution-CMS** 1. Explain how your organization will tailor and restrict data access privileges based on an individual's role on the research team. 2. Explain the use of technical safeguards for data access (which may include password protocols, log-on/log-off protocols, session time out protocols, and encryption for data in motion and data at rest).	Federal Risk and Authorization Management Program (FedRAMP)- Authorization to Operate (ATO)- Alignment crosswalk with NIST 800-53 Standards	**Access Control - NIST 800-53** The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-12, SC-13.	The organization has decided to use a role –based access model that is supported by the CSP vendor to tailor and restrict data access privileges based on their role on the research team. The CSP has a IAM process that includes a authentication, username and password process for data access . The CSP vendor selected was compliant with the encryption (cryptographic) data mechanisms at rest and in transit as required by CMS and aligned in meeting NIST 800-53 Standards. The CSP vendor selected is compliant with FedRAMP ATO standards and it was validated on the FedRAMP government website.
ata Breaches	**Data Reporting And Publication –CMS** Who will have the main responsibility for notifying CMS of any suspected incidents wherein the security and privacy of the CMS data may have been compromised? Please describe and identify your organization's policies and procedures for responding to potential breaches in the security and privacy of the CMS data? **Privacy and confidentiality** **to protect against accidental and nefarious access to information)- CMS Cloud Computing Security** How Does CSP protect privacy and confidentiality to protect against accidental and nefarious access to information?	Federal Risk and Authorization Management Program (FedRAMP)- Authorization to Operate (ATO)- Alignment crosswalk with NIST 800-53 Standards	**INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION NIST 800-53** The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system. Supplemental Guidance: Wireless signals may radiate beyond the confines of organization- controlled facilities. Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. Scans are not limited to those areas within facilities containing information systems, but also include areas outside of facilities as needed, to verify that unauthorized wireless access points are not connected to the systems. Related controls: AC-18, IA-3.	The data owner faculty member will be responsible for notifying CMS of any suspected or potential breech incidents that is supported by University policies and the data owner will collaborate with the University CIO as indicated by policies. The CSP vendor selected is compliant with FedRAMP ATO standards and it was validated on the FedRAMP government website.
M	**Storage of CMS Data Files- CMS** Explain your organization's system or process to track the status and roles of the research team.	Federal Risk and Authorization Management Program (FedRAMP)- Authorization to Operate (ATO)- Alignment crosswalk with NIST 800-53 Standards	**Access Control-The organization employs automated mechanisms to support the management of information system accounts- NIST 800-53** Identification and Authentication process within CSP **Access Control- Monitors privileged role assignments;-NIST 800-53** Role-Based Access Model within CSP **Access control- procedures [Assignment: organization-defined frequency].- NIST 800-53** Explain The Access Control Procedures in place within CSP **Access Control-Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;- NIST 800-53** Explain the Roles configured within CSP for Access utilizing the Role Base Model	The CSP has a IAM process that includes a authentication, username and password process for data access. The role-based access management system within the CSP storage environment will be the process for potential future roles of a research team. Three potential roles: Owner, Editor, Viewer was added in the CSP storage environment and tested with publically available data. The CSP vendor selected is compliant with FedRAMP ATO standards and it was validated on the FedRAMP government website.

APPENDIX C

Toolkit Flowchart Guide



APPENDIX D

Cybersecurity Best Practices For Management of PHI Toolkit

TABLE OF CONTENTS

Page

Background

The toolkit was created to assist with an identified knowledge gap focused on cybersecurity within a CSP environment with PHI/PII data. There was a need to enhance the knowledge within an academic research environment as the university embarked on data analytics using PHI/PII datasets. The creation of this toolkit is one of the identified objectives for the final DNP project.

Purpose

The development of this toolkit provides another tool within health academia to leverage with the construction of a CSP environment that supports PHI/PII. The evidence-based resources contained in this toolkit is similar to other toolkits developed in healthcare and other industries used to address cybersecurity risks.

Audience

Academic researchers who have a limited knowledge on resources/guidelines for protecting PHI/PII within a CSP environment.

Intended Use

The intended use of this toolkit is to serve as a scope limited guide with resources for protecting PHI/PII data within CSP environment. Although, the scope of this toolkit guide is limited it may be applicable with protecting non-PHI/PII data. Protecting PHI/PII has more stringent security requirements than publicly available data, which allows the application of elements within this toolkit to potentially be utilized with other types of data.

In addition, with the increase focus with healthcare on population health, impact of health on economics, social determinants of health, and development of health information exchanges the toolkit can serve as a resource for protection of data.

It is not intended to be an all-inclusive resource as there may be more or potentially less regulations that will need to be adhered to depending on factors that include: type of data, CSP, state laws, local regulations, and organizational policies/procedures. Cybersecurity risks and threats are continuing to change which may also impact the rules, laws, regulations that will need to be followed (Murphy, 2015).

Role of Toolkit

The role of the toolkit is to disseminate evidence-based knowledge and resources about best practices for management of PHI. In addition, the toolkit provides resources for the construction (configuration) of CSP environment for data analysis with PHI/PII data. The toolkit also provides a foundation for continued expansion and use across different CSP vendors, settings, and within healthcare.

Nurse informaticists and academicians can use this toolkit to lead, teach, and further support the increase use of CSP environments within various nursing practice settings. Alignment and/or modification of paper-based HIPPA, patient privacy, and confidentiality practices for application to CSP environments is also facilitated by the use of toolkits (Murphy, 2015). Vigilance in the protection of PHI/PII for any setting is crucial as the cybersecurity threats continue to change with the rise in technology within healthcare.

Implementation Phases

A. **Awareness**

a. Data Elements- Academic researchers need to understand the various data elements collected as primary PHI and with the acquisition of secondary PHI data. Understanding the type of data is essential for determining what regulations, laws, policies, and processes to follow to ensure the data remains

secure. Exploring questions surrounding the data needs for example: Are there any data elements being collected or within datasets that would be classified as PHI/PII according to CMS?

i. ***Resources-***

1. CMS, Health Human Services (HHS) for data classification standards).

b. Data Needs- The need to collect this data and where this data will be obtained from is important to be aware of to help with the identification of the cybersecurity requirements that need to be adhered to. The collection and use of confidential and sensitive PHI/PII should be only what is needed to carry out the duties you are performing (Murphy, 2015).

i. *Resources*

1. HIPPA/Healthcare Privacy Federal Laws- https://www.hhs.gov/hipaa/for-professionals/index.html.
2. FedRAMP- https://www.fedramp.gov/documents/
3. Siedlelman, L.-Differences between RIF, LDS, and PUF Data Files-https://www.resdac.org/articles/differences-between-rif-lds-and-puf-data-files.
4. Research Data Assistance Center (Resdac) (2019). *Data Management Plan Guidelines.* Retrieved from: https://www.resdac.org/sites/resdac.umn.edu/files/CMS%20DPSP%20Data%20Management%20Plan%20Guidelines_1.pdf.

5. CMS- https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_32_Cloud_Computing.pdf.

B. Assessment

a. Storing and Securing PHI Data- Data containing PHI/PII requires adherence to federal, state, and local regulations governing healthcare data (CMS, 2011). It is important to understand the rules and regulations governing the storage of PHI in a CSP environment (CMS, 2011). Responsibility for adhering to the protection, privacy, regulations for PHI/PII data does not change because the storage of the data is in the cloud instead of paper (Murphy, 2015). There are encryption standards requiring adherence for additional protection of the data being stored (NIST, 2013). Determining the mechanism of for storing the data there are many elements to consider beyond the capacity of the environment that will be utilized.

i. ***Resources***

1. CMS- https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_32_Cloud_Computing.pdf
2. Carnegie Mellon University -*Guidelines for Data Classification-*

https://www.cmu.edu/iso/governance/guidelines/data-classification.html.

3. Stanford University-PHI Data Classification and Appropriate Cloud Storage Environment Selection- https://uit.stanford.edu/guide/riskclassifications
4. HIPPA- https://www.hhs.gov/hipaa/index.html
5. HIPPA Security Guidelines- https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf
6. PHI-Federal Privacy -https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected
7. Data Privacy-NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
8. Data Privacy- Research Data Assistance Center (Resdac) Data Privacy Safeguard Program Office of Enterprise Data & Analytics Division of Data and Information Dissemination Overview- https://www.resdac.org/sites/resdac.umn.edu/files/CMS%20DPSP%20Program%20Overview_1.pdf.

9. Summary of the HIPAA Security Rule https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
10. Breech Prevention-Encryption -https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html
11. Security Encryption Technical safeguards https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf?language=es

C. **Roles and Access Needs**

a. Role Based Access- Determining the specific roles and responsibilities for the data will be instrumental with the configuration of access within the CPS storage environment (Murphy, 2015). It will be important to understand will the identified roles be accessing the CPS storage environment outside of the work environment. Supporting infrastructure that may include: devices, internet availability, internet bandwidth, and help-desk support will also need to be considered for each of the roles. Role based access configuration is a common methodology utilized, which supports HIPPA monitoring and compliance procedures (Gunter, Liebovitz, & Malin, 2011).

i. ***Resources***

1. NIST 800-53 Access Control -Security Controls and Assessment Procedures for Federal Information Systems and Organizations https://nvd.nist.gov/800-53/Rev4/control/AC-1.

D. Policies and Procedures

a. Policies & Procedures- Policies and procedures are often the framework that guides the tasks you perform within your organization. It is important to remember that policies and procedures do not exempt you from adhering to federal, state or local regulations related to cybersecurity for protecting PHI/PII data (Soman, 2011). CMS may request to see the policies that will govern the protection of PHI/PII data stored in CSP environment (CMS, 2011).

Collaborating and leveraging policies, guidelines and structures from other universities may be helpful. Stanford University is both a world renowned school and medical entity has created charts to assist researcher in identifying PHI data and the appropriate cloud storage environment that has appropriate protection (Stanford, N.D) Stanford University has a HIPPA security management plan which may be a reference resource for the development of polices for protecting PHI (Stanford, 2015). It will be important to review policies on a regular basis to ensure they align with any changes in regulations.

i. ***Resources***

1. CMS- Policy- Information Security-Section 4: IntegratedInformationSecurityandPrivacyPolicies- https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-

Technology/InformationSecurity/Downloads/IS2P2.pdf#page34.

2. Stanford University- HIPPA Security Management Policy- https://uit.stanford.edu/security/hipaa/security-management-policy.
3. Carnegie Mellon University -*Guidelines for Data Classification*- https://www.cmu.edu/iso/governance/guidelines/data-classification.html.
4. Stanford University-PHI Data Classification and Appropriate Cloud Storage Environment- https://uit.stanford.edu/guide/riskclassifications.
5. NIST 800-53 Access Control -Security Controls and Assessment Procedures for Federal Information Systems and Organizations https://nvd.nist.gov/800-53/Rev4/control/AC-1.

E. CSP Vendor Selection

CSP Vendor Selection- There are several CSP vendors available when you are ready to make a selection that could potentially meet your data storage needs. It is important to be diligient in reviewing the prospective CSP ensuring they will meet the security compliance regulations for PHI/PII data (Soman, 2011). CMS provides several resources for security requirements to assist you in asking the CSP pertinent questions (CMS, 2011). Ultimately as the data owner

it will be your responsibility to ensure the appropriate vetting, security and privacy compliance requirements are in place.

i. ***Resources***

1. HIPPA/Healthcare Privacy Federal Laws- https://www.hhs.gov/hipaa/for-professionals/index.html.
2. FedRAMP- https://www.fedramp.gov/documents/.
3. CMS- https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_32_Cloud_Computing.pdf.
4. NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
5. Summary of the HIPPA Security Rule- https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

F. Implementation

Implementation Plan -After making the CSP selection for your PHI-PII data storage you will be ready create an implementation plan. The CSP should be a partner with you as begin to identify the steps for implementation (Murphy, 2015). Before constructing the cloud-based environment, it will be

important to ensure that there have been no recent changes to regulations governing PHI/PII data. After the configurations have been completed within the CSP environment, testing the cybersecurity settings will be important. Testing with publicly available non-PHI/PII data provides an opportunity for validation or to make changes without compromising PHI/PII data.

G. Additional Educational Resources-

i. *Resources*

1. General Cybersecurity Resources

a. HHS-Cybersecurity-https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html.

b. HHS-HIPPA-https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf?language=es.

c. NIST Cybersecurity Framework-https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

d. NIST Cybersecurity Framework Learning-https://www.nist.gov/cyberframework/online-learning/components-framework.

e. NIST Cybersecurity Framework Questions and Answers- https://www.nist.gov/cyberframework/questions-and-answers#basics.

f. HHS-NIST-CSF-HIPPA Crosswalk- https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf?language=es.

g. HITRUST -Healthcare Sector Cybersecurity Implementation Guide v1- https://www.uscert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.

h. CMS- Data Administration- https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/DataAdmin/index.html.