

Seattle University

ScholarWorks @ SeattleU

Master of Arts in Criminal Justice Theses

Criminal Justice, Criminology, and Forensics

2020

Information security compliance in a healthcare setting: A user behavior pilot study

Carla T. Panattoni
Seattle University

Follow this and additional works at: <https://scholarworks.seattleu.edu/macj-theses>

Recommended Citation

Panattoni, Carla T., "Information security compliance in a healthcare setting: A user behavior pilot study" (2020). *Master of Arts in Criminal Justice Theses*. 5.
<https://scholarworks.seattleu.edu/macj-theses/5>

This Thesis is brought to you for free and open access by the Criminal Justice, Criminology, and Forensics at ScholarWorks @ SeattleU. It has been accepted for inclusion in Master of Arts in Criminal Justice Theses by an authorized administrator of ScholarWorks @ SeattleU.

Date: June 25th, 2020


I, Carla Panattoni, hereby submit this work as part of the requirements for the degree of:

Master of Arts in Criminal Justice

It is entitled:

Information security compliance in a healthcare setting: A user behavior pilot study

This work and its defense approved by:

Chair: Dr. Peter Collins _____ 

Member: Dr. Matthew Hickman _____ 

Member: Dr. Cris Ewell _____ 

Graduate Director: Dr. Elaine Gunnison _____ 

Information security compliance in a healthcare setting: A user behavior pilot study

Carla T. Panattoni

Seattle University

Abstract

Human behavior is known to be one of the weakest links to information security and a likely cause of incidents that may lead or contribute to the loss or compromise of sensitive information (Ahmad, & Ismail, 2010; Akhunzada, Kam, 2015; Aloul, 2012; Cain, Edwards, & Still, 2018; Long, 2013; Narayana, Sookhak, & Anuar, 2015; Pike, 2011; Seidenberger, 2016). The Health Insurance Portability and Accountability Act (1996) requires healthcare organizations to comply with national standards to reduce the likelihood of a privacy breach. Online stolen data markets, where cybercriminals operate in the dark web, advertise, sell, share, and trade sensitive personally identifiable information for nefarious purposes (Chertoff, 2017; Holt et al., 2016). The 29-statement pilot study survey replicates the Safa et al. (2015) survey and was administered to 39 UW Medicine (UWM) employees via the UWM Research Electronic Data Capture online survey application. The survey statements are based on the Theory of Planned Behavior, the Protection Motivation Theory, and the Safa et al. (2015) employee information security conscious care behavior model. The UWM pilot study statements were modified, and results are presented ($n = 32$). Descriptive statistics are provided, as well as lessons learned, which will be incorporated into a larger-scale survey deployment. This is a timely study to determine how best to reduce the likelihood of a user error or a cyber adversary exploiting a weakness that could lead to or cause a global catastrophic cyber event that could potentially trigger further political, economic, and social volatility.

Keywords: *compliance, privacy breach, information security controls, electronic protected health information, dark web, cybersecurity, threat vector, risk management*

Table of Contents

Abstract 2

Information security compliance in a healthcare setting: A user behavior pilot study 6

 Organizational Measures to Protect Patient Information from Threat Adversaries 6

 Information Security Control Countermeasures 8

 Theoretical Constructs and the Conscious Care Behavior Model 9

 UW Medicine Pilot Study 10

Literature Review 11

 U.S. Healthcare Public Law and the State of Healthcare in America 11

 HIPAA Privacy, Security, and Breach Notification Rules 13

 National Healthcare Expenditures 13

 National Incentives to the Healthcare and Public Health Sector 15

 UWM New Employee Orientation: Compliance and Information Security Training 16

 Information Security Behavior Toward Compliance 17

 Employee Information Security Conscious Care Behavior 17

 The Underground Economy and Stolen Data Markets 18

 User Behavior as a Threat to Information Security 19

 Telemedicine and User Compliance with Information Security Controls 20

 Change Management Security Controls 21

 Theory of Reasoned Action 21

INFORMATION SECURITY COMPLIANCE	4
Theory of Planned Behavior	22
Protection Motivation Theory.....	23
Employee Information Security Conscious Care Behavior	25
Social Norms and Knowledge Sharing	26
Method	26
Research Design.....	27
The Research Electronic Data Capture Online Survey Application.....	28
Sampling and Demographics	28
UWM Pilot Test Administration.....	30
Results.....	31
Discussion.....	39
Conclusion	40
Limitations of Existing Research.....	40
Future Integration of the Structural Equation Model.....	41
Directions for Future Research	41
Large-Scale Survey Hypotheses	42
User Behavior and the Healthcare and Public Health Cyber Dependencies	43
Healthcare and Public Health Sector Cyber Preparedness	45
Healthcare Sector Cyber Event Preparedness.....	47
References.....	51

INFORMATION SECURITY COMPLIANCE	5
Appendix A.....	78
Appendix B.....	81
Appendix C.....	83
<i>HIPAA Protected Health Information Identifiers</i>	83
Appendix D.....	84
<i>U.S. Cybersecurity & Infrastructure Security Agency</i>	84

Information security compliance in a healthcare setting: A user behavior pilot study

Research suggests that human error is one of most likely causes of data breaches (Ajzen, 1991; Albrechson et al., 2010; Box, et al., 2014; Furnell et al., 2010; Ghazvine et al., 2016; Kowlkowaska et al., 2013; Rhee et al., 2009; Safa, et., al, 2015; Safa et al., 2016; Siponen et al., 2014; Thomson et al., 1998; Veiga et al., 2017). Since there is scant research about user formation and compliance in healthcare settings, this is a timely pilot study to broaden our understanding about user behavior compliance to reduce the likelihood of a privacy breach (Kruse, 2017; Safa et al., 2015; Safa et al., 2016). The complex legal and regulatory nature of healthcare delivery is examined, as well as how healthcare organizations train and educate employees about their responsibilities to preserve sensitive protected health information (PHI) and electronic PHI (ePHI).

Organizational Measures to Protect Patient Information from Threat Adversaries

Healthcare employees are considered a threat adversary or threat vector because users may inadvertently or deliberately (malice, laziness, or apathy) exploit administrative, technical, and physical vulnerabilities or weaknesses that can trigger an incident that leads to or causes a privacy breach (Ewell, 2018). Other types of threat vector attacks include the misuse of operating systems; the installation of malicious software; data interception; sabotage; physical attacks, supply chain disruptions, and the violation of implied trust among business associates and contractors (Ewell, 2018).

Healthcare organizations that bill or receive reimbursement for providing patient care are mandated, under the penalty of federal law, to adhere to the national privacy (Privacy Rule), information security (Security Rule), and breach notification (Breach Notification) standards set forth in the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Centers for Disease Control and Prevention, 2017; HHS.gov, 2017; Office of Civil Rights, U.S. Department

of Health & Human Services, 2017; Department of Health and Human Services, 2013). Due to the Healthcare and Public Health Sector's transition toward the exponential increased use of electronic medical records, HIPAA and other regulatory controls ensure that healthcare organizations protect and preserve confidential protected health information that reside in information systems from unauthorized access. Educating and training the healthcare employee workforce about the HIPAA Security, Privacy, and Breach Notification rules (i.e., the administrative, physical, and technical security controls or countermeasures) is a means to modify user behavior toward compliance with information security controls and reduce the likelihood of a cyber threat exploiting a vulnerability to gain unauthorized access to hard-copy PHI or soft-copy ePHI. This research is about how organizations determine whether or not users are modifying behavior toward the implementation of organizational security controls. The UWM pilot study is an unique opportunity, in a dedicated healthcare environment, to disseminate a modified version of the Safa et al. (2015) survey, analyze the data, and prepare for a larger-scale survey to measure user behavior compliance with information security controls (Safa email, 2018).

It is instructive to explain what is meant when one refers to hard-copy PHI and it includes information that could identify a patient who is seeking medical treatment, including hand written patient notes; health insurance cards; fax or printed materials (outpatient instructions, medication orders, and health history); photographs; x-ray films; or patient prescriptions. Soft-copy electronic media is an example of ePHI and include a patient's electronic medical record, images (mammography, retinal scans, and medical device monitoring reports), voice recordings, photographic images (tattoos, scars, birthmarks, and injuries), and video recordings. Private healthcare industry business associates also support patient care delivery by providing goods and services, and must also employ compliance and information security controls or countermeasures

to protect confidential information from unauthorized access to information systems and assets. For instance, business associates may provide storage for hard-copy PHI, such as medical records and office buildings that host proprietary research about the new coronavirus disease (COVID) outbreak that was reported in Wuhan, China (Centers for Disease Control and Prevention, 2020). Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization, officially recognized the name, COVID-19 on February 11, 2020 (Ghebreyesus, 2020). Facility officials could mandate that employees display and utilize an electronic badge access system to enter and exit from non-public areas. Instituting username and password login requirements is another security control to protect ePHI residing in confidential information systems, such as computer desktops, laptops, mobile devices, and other assets, such as medical devices.

Information Security Control Countermeasures

To demonstrate compliance with federal and state law, regulatory requirements, and legal obligations, healthcare delivery organizations and their contracted business associates, mandate that new employees attend compliance and information security training. UWM new employees become familiar with the organizational compliance policies that guide user behavior and are instructed with examples about the types of administrative, technical, and physical threats that users may encounter. Users are also instructed how to modify their behavior to recognize a cyber threat and apply UWM administrative, technical and physical security controls or countermeasures to reduce the likelihood of a risk; i.e., sharing confidential usernames and passwords, from leading to the unauthorized viewing of ePHI that is associated with a family member, friend, celebrity, or rival (McLeod & Dolezel, 2018; Maennel, Maeses, & Maennel, 2018).

At University of Washington Medicine (UWM), Compliance Policies are the

organizational resources that explain how the organization complies with federal and state law, regulatory requirements, and legal obligations. UWM expects employees to comply with data stewardship obligations and sign the UWM Privacy, Confidentiality, and Information Security Agreement (UW Medicine, 2020). In addition, the UWM Information Technology (IT) Services and Security (ITS-Security) organization publishes Information Security Standards, which cascade from the UWM Compliance Policies. UWM ITS-Security Information Security Standards provide a procedural approach and guide a user on how to implement a security control, such as how to encrypt an email, request a new business associate be added to an approved email domains list, or how to process a request a security review for a new third-party software that is being considered for official UWM use.

Creating an organizational culture about user behavior compliance is essential to protecting the confidentiality, integrity, and availability of confidential information systems. Confidentiality refers to protecting sensitive patient data from unauthorized access and disclosure (Glossary, Computer Security Resource Center, National Institute of Standards and Technology, 2019). Integrity refers to assuring that data are protected from modification or being destroyed (Glossary, Computer Security Resource Center, National Institute of Standards and Technology, 2019). Availability refers to assuring that information systems are readily accessible to authorized users (Glossary, Computer Security Resource Center, National Institute of Standards and Technology, 2019).

Theoretical Constructs and the Conscious Care Behavior Model

Theories are a means to predict and explain human behavior. This UW Medicine pilot test survey, which included a total of 39 participants serving with the UWM Information Technology Security-Security (ITS-Security) organization, is replicated with permission from the Safa et al. (2015) survey (email, 2018). The theory of planned behavior (TPB), the protection

motivation theory (PMT), and the employee conscious care behavior model were the three major survey statement items included in the Safa et al. (2015) survey. The Safa et al. (2015) large scale survey included respondents serving with six Malaysian industries, including IT and Telecommunications (86%), Finance and Insurance (48%), Retail (36%), Healthcare (25%), Education (11%), and Hotel (6%). The TPB research suggests that attitude, subjective norms, and perceived behavioral control predict and explain user behavior (Ajzen, 1985 and 1991; Al-Omari, El-Garyar, & Deokar, 2012; Box et al., 2014; Chau & Hu, 2001; Huang and Chuang, 2007; Humaidi & Balakrishnan, 2017; Liao et al., 2007; Siponen et al., 2014; Suhwan Jeon et al., 2011; Uffen & Breitner, 2013). The PMT is deemed one of the most important theories to explain how users consider protective measures (Anderson & Agarwal, 2010; Cabrera et al., 2006; Cox, 2012; Durkcikova, et al., 2011; Infinedo, 2014; Lee & Larson, 2009; Pi et al., 2013; Ryan, et al., 2010; Safa et al., 2015; Safa et al., 2016; Salgado et al., 2013; Siponen et al., 2015; Suhwan et al., 2011; Woon & Kankanhalli, 2007).

UW Medicine Pilot Study

A 29-statement four point Likert-type pilot test survey was administered to 39 UWM employees serving with the UWM ITS-Security organization (N = 600). The UWM pilot test was a modified version of the Safa et al. (2015) survey because UWM promotes the use and reference of UWM Compliance and UWM ITS-Security Information Security Standards. The UWM Research Electronic Data Capture (REDCap) online survey platform disseminated the 29-statement pilot study to respondents via email and to protect the anonymity of respondents, no direct identifiers were collected. The Safa et al. (2015) pilot test included 32 respondents who were associated with information technology experts. Descriptive statistics from the UWM pilot test ($n = 34$) are compared with the Safa et al. (2015) survey ($n = 212$). Lessons learned are presented to prepare for a larger-scale survey deployment at UWM (Limitations). In the

conclusion section, parallels are drawn from the current global COVID-19 pandemic crisis and the planning necessary to prevent a major cyber incident, which could also disrupt patient care delivery and potentially cause harm or death, as well as perpetrate local, regional, domestic and international economic, political, and social conflict.

Literature Review

U.S. Healthcare Public Law and the State of Healthcare in America

The original intent of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, was to assist individuals when changing employment. Due to the increasing use and dependence upon the Internet and electronic media, the information security and compliance privacy of protected health information, there are national administrative, technical, and physical standards that are required to protect and preserve the confidentiality, integrity and availability of individually identifiable protected health information (Centers for Disease Control and Prevention, 2017; HHS.gov, 2017; Office of Civil Rights, U.S. Department of Health & Human Services, 2017; and Department of Health and Human Services, 2013). Table 1 identifies the types of covered entities (CEs) that accept or receive payment for patient care services (Health Insurance Portability and Accountability Act, 1996). CEs, including business associates (BAs) and BA subcontractors, adhere to HIPAA Rules when ePHI is created, received, or transmitted (Department of Health and Human Services, 2019). Individuals and businesses, commonly known as business associates (medical device manufacturers), are also required to protect the privacy and security of PHI and ePHI (Centers for Medicare & Medicaid Services, 2019; Food and Drug Administration, 2020). CEs comply with the Rules' requirements to protect the privacy and security of PHI and are required to notify privacy officials when there is a suspected loss or compromise of PHI and ePHI.

In Washington State, after a data breach is discovered, there is a required mandatory

notification to the Washington State Attorney General for affected individuals within 45 calendar days (Washington State Legislature, 2020). Patient privacy rights allow patients to view and modify their medical records; for instance, patients who opt to pay cash for medical treatment may elect to preclude PHI from being shared with a health payor for reimbursement. If a patient reviews their record and discovers an error, then the patient may request a modification.

Table 1

HIPAA Covered Entities (CEs)

CE Identity	CE Category
Healthcare Providers	Physicians and other licensed (DEA) providers Healthcare Clinics Psychologists Chiropractors Nursing Homes Rehabilitation Centers Pharmacies Dentists
Hybrid Entities*	CEs with academic medical centers that teach students (not covered) and conduct patient care (covered); retailers with on-site pharmacies (covered)
Business Associates**	Providing the appropriate administrative, physical, organizational, and technical safeguards to protect ePHI (HITECH Act, 2009)
Health Plans	Insurance Health maintenance organizations Private health State & federal government healthcare
Healthcare Clearinghouses ***	Billing Adjusting prices Community health management information systems, community health information systems, and "value-added" networks and switches

Note. * Porter et al. (2018). ** Porter et al. (2018). *** Creating, transmitting, facilitating, processing, receiving, storing ePHI, and transforming non-standard data on behalf of a healthcare entity.

HIPAA Privacy, Security, and Breach Notification Rules

The HIPAA Privacy Rule refers to the national standards and safeguards (administrative, physical, and technical) to protect patient privacy, as well as create opportunities for patients to set limits and conditions on the use and disclosure of PHI (Office of Civil Rights, U.S. Department of Health & Human Services, 2016). Patients possess rights to review their medical records and petition to request errors to be corrected (Office of Civil Rights, U.S. Department of Health & Human Services, 2016). The HIPAA Security Rule provides national standards that CEs, business associates, hybrid entities, and healthcare clearinghouses are required to implement, monitor, and manage. For instance, the HIPAA Security Rule applies national administrative, technical, and physical standards that must be applied when confidential patient care data, such as ePHI is created, transmitted, shared, received, and stored or archived (Porter, Trevors, & Vrtis, 2018). The HIPAA Breach Notification Rule requires CEs, vendors of ePHI, and their third-party service providers, to notify the Federal Trade Commission of a data breach, the unauthorized disclosure or viewing of over 500 patient records within 60 days of notification of the discovery (Public Law 111-5, 2011; Koczkodaj et al., 2018).

National Healthcare Expenditures

The U.S. National Health Expenditure Accounts (NHEA) aggregates statistics about the state of Healthcare and Public Health Sector expenditures and includes medical and dental services (inpatient and outpatient home health), facility renovations, patient care delivered in correctional facilities, and medical research and development (U.S. Department of Health and Human Services, 2018). Types of healthcare and public health expenditures included 62% for inpatient hospital care; 34% for private healthcare insurance; 10% for personal out-of-pocket expenses; and 8% for third-party payers and programs (U.S. Department of Health and Human Services, 2018). The NHEA also measures medical care consumption, financial investments,

information communication technologies investments, procurement, and non-commercial healthcare research (Department of Health and Human Services, 2017). Healthcare expenditures is an important issue because it demonstrates the financial gains that cybercriminals are seeking, and therefore are ruthless in their efforts to break-in to steal, corrupt, or ransom ePHI. Nation states, especially during the COVID-19 pandemic, continue a relentless pursuit to steal ongoing U.S. vaccine research and development.

In 2017, healthcare expenses increased by 3.9% to \$3.5 trillion (U.S. Department of Health and Human Services, 2018). This indicates the degree to which the Healthcare and Public Health Sector contributes to the overall U.S. economy. Appendix C provides the list of the individually identifiable health information (18 specific direct identifiers) that, if disclosed or viewed by an unauthorized person, violates a patient's right to privacy (U.S. Government Printing Office, 2020). The U.S. Healthcare and Public Health Sector accounted for approximately 18% of the gross domestic product (GDP) to the U.S. economy (McAfee & Lewis, 2018). Due to the economic vitality of the Healthcare and Public Health Sector, internal (disgruntled users) and external cyber criminals pose a threat to the confidentiality, integrity, and availability of sensitive and confidential information systems. McAfee and Lewis estimate that when hospitals experience a data breach, the ensuing financial costs include years of costly litigation, reputational damage, and a locality could suffer from the loss of tax revenue when exemplary employees resign, are hired out-of-state, and families relocate elsewhere which may reduce local tax revenues (McAfee & Lewis, 2018).

In 2019, healthcare data breaches were estimated to cost \$4 billion (Hulme, 2020). Cybercrime costs were estimated to be one percent or \$600 billion of the world's GDP (McAfee & Lewis, 2018). The healthcare and financial sectors are highly regulated industries and costs associated with recovery from a data breach are estimated to be \$408 per data record for

healthcare and \$208 per data record for the financial sector (Cost of a 2018 Data Breach Study: Global View, 2018; Sulleyman, 2017).

National Incentives to the Healthcare and Public Health Sector

The Health Information Technology for Economic and Clinical Health (HITECH) Act (2009) incentivizes the Healthcare and Public Health Sector to adopt and integrate new technology and reduce healthcare costs, improve productivity, and reduce the likelihood of an incident leading or contributing to a privacy breach (Department of Health and Human Services, 2009). Business associates who manufacture and maintain medical devices are also required to comply with security controls (Food and Drug Administration 2020). Health Information Technology for Economic and Clinical Health Act of 2009 incentivized the healthcare sector to adopt, upgrade, and integrate technology and earmarked approximately \$19 billion for the adoption for electronic medical record (EMR) or electronic health records (EHR) systems (Atasoy & Ganju, 2018). An EMR is a digitized version of a patient's health record (Sahney & Sharma, 2018). Adopting EMRs could increase clinician productivity, patient care delivery, and reduce redundant processes and duplication-of-effort.

Due to the complex nature of an EMR sending, receiving, or storing ePHI in and through other systems, the security and privacy becomes crucial because if one system becomes unavailable due to a cyber incident, patient care delivery or public health efforts may be disrupted or harmed. Replacing antiquated user-operated hospital paging systems for instance, reduces the risk of inadvertent disclosures of confidential information (Mehrzaad & Barza, 2015; Lee et al., 2010; Reddy et al., 2005; Wu et al., 2012). Another benefit of adopting state-of-the-art technology solutions includes reducing the likelihood of patient medication errors (Health and Human Services, 2009). The privacy, security, and breach notification rules depend greatly upon user behavior compliance with organizational information security controls, such as system

monitoring for anomalous behavior and the timely application of security updates to EMR systems.

UWM New Employee Orientation: Compliance and Information Security Training

The UWM mandatory new employee orientation (NEO) is an opportunity to promulgate the organization's mission, vision, and value statements, which could mitigate risk to confidential information systems and improve information security behavior compliance. The UWM presentation offers examples about how to comply behavior toward the implementation of security controls. Creating complex passwords, reporting suspected phishing emails to the UW Medicine Help Desk, alerting managers when a device is misplaced or lost, reporting privacy concerns (unethical behavior, waste, fraud, or abuse), and utilizing a badge access system to restrict access to data centers, pharmacies, and patient units (nursery and inpatient psychiatric unit). Through the NEO Program, explaining employee behavior expectations via the UWM Compliance Polices and the ITS-Security Information Security Standards are the means to educate users about how to apply the administrative, physical, and technical countermeasures to decrease the likelihood of a weakness from being exploited by an adversary and adversely impacting confidential information systems and assets.

Once new employees complete the NEO training and enter into their new position, UWM evangelizes continued information security through the UWM Compliance Policy program Intranet, email updates, and leadership news. Types of UWM compliance policies that educate employees include Compliance Auditing and Monitoring Policy; Reporting and Non-Retaliation Policy; Compliance Investigation Policy; Corrective Action Policy; Government Investigations Policy; Compliance Risk Policy; Identity Theft Prevention Policy; and Social Media Networking Policy (UWM Compliance Program Policies, 2019). The UWM ITS-Security organization, in response to UWM Compliance Program Policies, creates, seeks approval for,

and manages Information Security Standards and provide users with step-by-step procedures on how to comply user behavior toward the implementation of information security controls (UW Medicine Information Security Standards, 2019). Types of UWM ITS-Security Standards include Electronic Communications, which refers to electronic mail and instant messaging. The Incident Management Standard refers to how to identify a potential privacy breach and report suspicious activities, such as a fire, flood, active shooter, terrorist attack, or natural disaster.

Information Security Behavior Toward Compliance

Security controls are user behavior countermeasures that reflect the practical day-to-day administrative, physical, environmental, and technical procedures that users integrate into their daily workflow, and are designed to reduce the likelihood of a weakness (administrative, technical, or physical) from being exploited by an adversary (internal user threat or external) and disrupting or causing an incident that may lead or contribute to a privacy breach. Research suggests that there are positive associations when users are trained and provided the resources to implement and manage information security controls (Anderson & Agarwal, 2010; Ajzen, 1991; Ajzen & Fishbein, 1980; Ajzen, 1991; Ajzen, 2019; Fishbein & Ajzen, 2010; Furnell & Clarke, 2012; Humaidi et al., 2017; Liao, Chen, & Yen, 2007; Infinedo, 2014; Kolkowska & Dhillon, 2013; Rhee, Kim, & Ryu, 2009; Rogers, 1983; Safa, et al., 2015; Safa, Von Solms, & Furnell, 2016; Suhwan, Kim, & Joon, 2011). Whether one is a medical student, clinician, analyst, team-lead, manager, or director, security control implementation is key to compliance and reduces the risk. Security controls can stem from organizational policies, which are an effective means to mitigate and reduce the risk of an information security incident (Safa, et al., 2016).

Employee Information Security Conscious Care Behavior

Employee information security conscious care behavior (ISCCB) is a model to examine how users think about their information security skills to comply with information security

controls, which can reduce the risk of an incident leading or causing the loss or compromise of confidential information. Users who report a phishing attempt, change a password, or escort visitors are complying with information security controls and reducing the likelihood of an incident. The Safa et al. (2015) ISCCB model aims to reduce the likelihood of an incident by improving information security compliance behavior. Attitude, subjective norms (TPB), threat appraisal and self-efficacy (PMT) impact user behavior. In addition, information security awareness, organizational policy, and user experience also mitigate risk (Safa et al., 2015). Cyber hygiene refers to user information security practices that reduce the likelihood of risk and improve self-efficacy (George & Emmanuel, 2018). The ISCCB model is the primary source for the UWM pilot survey (Appendix B).

The Underground Economy and Stolen Data Markets

The estimated mean value of stolen ePHI in the dark web, where law enforcement cannot monitor, is reported to be between approximately \$250 to \$1000 for a complete medical health record (Office of the Chief Information Security Officer, DHHS, 2019). Stolen data markets enable criminal activities such as committing pharmaceutical, financial, medical, and insurance fraud (Holt, Smirnova, & Chua, 2016). Organizational email systems cannot stem the flow of unwanted and malicious email. Email phishing attempts are a means by which malicious hackers attempt to create a sense of urgency and an unsuspecting user may be asked to do something immediately, such as revealing a username and password without confirming the emergent demand (Cohen, 2019; NIST Special Publication 800-53, Revision 4, 2015).

Al-Omari et al. (2012) suggests that 80% of security incidents are attributed to user behavior. User security controls include reviewing the sender's email address and that may be the first indication that it is a fraudulent email when the email address ends in '.ru' (Russia) or '.ro' (Romania), for instance. A cyber adversary may employ a threat tactic such as proclaiming

that a user's email will be disabled or deleted to being late with updating their username and password. When users do not adhere to, forget, ignore, or delay the application of a phishing security control, then the likelihood that a user may click an unknown link or attachment may increase. Unwittingly, a cyber adversary may gain unauthorized access and/or permit the injection of malicious software (malware) into the computer's hard drive, which then, freely permits the cyber adversary to navigate undetected through a secure network to view, corrupt, modify, extract, or hold confidential data for ransom (Coventry et al., 2018). Data privacy is another driver behind information security controls, which are designed to reduce human error (Coventry et al., 2018). Yet, despite an increasing reliance on technology solutions, privacy breaches are increasing (Al-Omari et al., 2012).

User Behavior as a Threat to Information Security

Narayana Samy et al. (2010) emphasizes that human error is a major threat to information security in the healthcare sector. Research suggests that information security incidents in healthcare settings are attributed to poor employee information security skills, including lack of awareness, inappropriate information security behavior, inadequate monitoring, and poor enforcement (Ahlan et al., 2011; Da Veiga & Martins, 2015; Safa et al., 2016). Users may fail to recognize the scope of an information security threat due to ignorance, apathy, and poor information security behavior (Cox, 2012). Assuring user compliance with information security controls is also important when patient care is provided beyond brick-and-mortar research institutions, medical clinics, and medical centers. Due to the global COVID-19 pandemic, many industries, including healthcare, are contracting with video conferencing service providers, such as Cisco WebEx, Microsoft Inc. Teams, and Zoom Inc., to accommodate work-from-home employees. Ensuring that users behavior toward the implementation of technical, administrative, and physical security controls includes assuring that a healthcare entity contracts for HIPAA-

compliant Telehealth services (HIPAA Journal, 2020).

Telemedicine and User Compliance with Information Security Controls

As healthcare organizations continue to manage under new COVID-19 business practices, compliance and information security leaders must create, promulgate, train, and bring user awareness about the requirement to protect the confidentiality, integrity, availability, and security architecture of new telemedicine services, such as Zoom, Inc., Cisco WebEx, WebMD, or Microsoft 365 Teams. Secure telemedicine networks provide virtual connections to view, converse, and perform a virtual medical examination. Collecting information remotely from patient glucose or cardiac monitors may also be part of telemedicine protocols, as well as sending prescriptions for medications to local pharmacies. Ongoing privacy and information security training, education, and awareness is essential to inculcate a user-compliant culture when many employees have transitioned to work-from-home environments. The term ‘secure’ refers to legal and industry-standard encryption technologies that prevent data, whether in transit or archived, from being decipherable (Washington State Legislature, 2020).

Serving the patient care population under the COVID-19 pandemic conditions includes contracting for and assuring the secure integration of HIPAA-compliant telemedicine services. User behavior compliance includes assuring that a service provider business agreement includes meeting HIPAA Privacy and Security requirements, as well as regulatory requirements and legal obligations. According to the U.S. Federal Bureau of Investigation (FBI), teleconferencing systems are also vulnerable to being hijacked or “Zoom-bombed,” which entails malicious hackers gaining unauthorized access to a video session and disrupting it by displaying hate, violence or threatening messages, or pornographic images (Setera, 2020).

As telemedicine services continue to gain popularity and serve as another means to conduct patient care during the COVID-19 pandemic, it is also serving vulnerable patient

populations who must remain at home, are residing in remote regions or in secure facilities, such as rehabilitation centers, long-term nursing facilities, and prisons. Zoom reported that since December 2019 the maximum number of daily meeting participants (free and paid subscriptions) was approximately 10 million. By March 2020, there were approximately 200 million daily meeting participants (Yuan, 2020).

Change Management Security Controls

Change management refers to the application of security controls to assure that the security and privacy of confidential information systems and assets meet federal and state law, as well as regulatory requirements and legal obligations. Information technology change management refers to the lifecycle change of acquiring, testing, deploying, servicing (applying operating system updates), and retiring confidential information systems and assets, such as servers, laptops, and medical devices. When change management security control protocols are not applied, or are ignored, delayed, forgotten, or incomplete, vulnerabilities could be exploited by a cyber adversary and lead to a cyber incident that causes a privacy breach to confidential information systems and assets.

Theory of Reasoned Action

The Theory of Reasoned Action (TRA) refers to how people process, assess, and think about behavior performance. TRA characteristics include attitude, motivation, perceptions, and the user's self-efficacy (Cartwright, 1949; Smith, 1947; Katz & Stotland, 1959). The theory also proposes that intentions toward a behavior influence the performance of a behavior (Ajzen, 1985 and 1991; Liao et al., 2007; Uffen and Breitner, 2013). During the 1950s, human behavior researchers applied TRA to predict and explain intentions toward a behavior (Cartwright, 1949; Katz & Stotland, 1959). User attitude (favorable or unfavorable evaluation) is a predictor of user behavior compliance (Ajzen, 1991; Safa et al., 2015). TRA was the precursor to the Theory of

Planned Behavior (TPB), which builds upon TRA and improves our knowledge about behavioral processes that impact self-confidence, behavior formation, and motivation toward behavior (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975).

Theory of Planned Behavior

TPB is associated with information security behavior compliance and the mutually supporting attributes are self-efficacy, perceived behavioral control, and attitude (Ajzen, 1975; Fishbein and Ajzen, 1980; Ajzen, 1985; Ajzen, 1987; Ajzen, 1990; Ajzen 2019; Ajzen and Fishbein, 2010; Safa et al., 2015, 2016). TPB is one of the theoretical constructs represented in the UWM pilot test survey. TPB involves five independent determinants of intention or motivation; they are: 1) perceived behavioral control; 2) subjective norms; 3) attitude; 4) intention formation; and 5) decision making (Ajzen, 1991). Non-motivational factors also impact intention, including skills, resources, time, and social norms (Ajzen, 1985).

Perceived behavioral control refers to one's perceptions about the ease or difficulty to perform a behavior as well as to situations in which an individual lacks sufficient control over the compliance behavior (Chau and Hu, 2001). Lending support from Bandura (1977 & 1982), the concept of perceived self-efficacy also plays a role in which an individual considers one's self-confidence to successfully perform a behavior. Attitude refers to users' cognitive processes to evaluate an idea or a belief, condition, situation, setting, person, place, or thing (Box et al., 2014; Siponen et al., 2014; Suhwan Jeon et al., 2011). Attitude represents the predisposition toward the behavior intention. User attitude is influenced by organizational cultural norms, which supports user compliance toward information security control adoption (Huang and Chuang, 2007; Al-Omari, El-Garyar, & Deokar, 2012; Humaidi & Balakrishnan, 2017). Attitude can be explicit (conscious awareness) or implicit and could impact beliefs and perceptions about information security compliance (Albrechtsen and Hovden, 2010). Subjective norms refers to perceived

social pressures to conform to expected group social norms.

The study of human behavior compliance asserts that the TPB reliably predicts and explains user formation behavior toward compliance and positively impacts employee information security conscious care behavior (Safa et al., 2015; Uffen & Breitner, 2013). When an intention is strong, the behavior is more likely to be performed (Ajzen, 1990; Ajzen, 1991; Suhwan, Kim, & Joon, 2011). Perceived behavioral control is defined as the degree to which a person perceives that the decision to engage in a behavior is under their control. Users examine their competencies (administrative and technical) about applying behavior toward compliance requirements (Humaidi & Balakrishnan, 2017; Safa et al., 2015). Ajzen (1991) points out that when there is a strong intention to engage in a behavior, then there is an even stronger motivation to perform it.

Protection Motivation Theory

Two attributes associated with the Protection Motivation Theory (PMT) are threat appraisal (coping appraisal) and self-efficacy. PMT is one of the most powerful explanatory theories to predict user intentions to apply protective actions (Anderson et al., 2010). PMT is also a reliable theory from which to test user behavior intentions toward compliance with information security controls (Cabrera et al., 2006; Cox, 2012; Durkcikova, et al., 2011; Infinedo, 2014; Lee & Larson, 2009; Pi et al., 2013; Ryan, et al., 2010; Safa et al., 2015; Safa et al., 2016; Salgado et al., 2013; Siponen et al., 2015; Suhwan et al., 2011; Woon & Kankanhalli, 2007). The Safa et al. (2015) research model included the TPB, PMT, and the employee ISCCB model into the Malaysian industry 2015 survey.

Threat appraisal refers to the cognitive process by which users may perceive personal vulnerabilities or weakness, such as lack of self-confidence or fear of reprisal. If a user perceives threats from the organization, such as a reprimand, retraining, or termination, then users may ask

someone else to evaluate the requirement to apply a security control or delay reporting an anomaly. Delaying the notice to a supervisor or colleague could pose an increased risk to a confidential information system. Coping appraisal refers to how users cope with the level of perceived risk to the confidentiality, integrity, and availability of confidential information systems and assets. Users may be reluctant to apply a countermeasure if procedures are poorly understood, vague, or estimated to be unimportant, immaterial, or negligible. Users may not perform a security control due to apathy, laziness, poor information security skills, busyness, or lack of understanding. Sometimes users may be unaware that some risks may be associated at a higher level within an organization (Woon & Kankanhalli, 2007).

Self-efficacy refers to the individual's confidence to achieve information security compliance through their organizational training, knowledge, experience, education, and experience (Humaidi & Balakrishnan, 2017). Self-efficacy is associated with social cognitive theory and refers to how one may feel about one's knowledge, experience, and skill competencies. Users consider what they perceive from others, as well as intrinsic or extrinsic motivations (Johnston & Warkentin, 2008; Workman et al., 2008). Self-confidence is an important characteristic that influences one's motivation toward behavior formation and intention (Ajzen, 1991; Bandura, 1977; Bandura et al., 1977; Bandura 1982). Research suggests that coupled with institutional information security awareness training, user behavior can be modified toward alignment with an organizational culture of compliance (Ifinedo, 2014; Lee & Larsen, 2009; Woon & Kankanhalli, 2007). Self-efficacy is a dominant predictor of an employee's intention to comply with information security controls (Siponen et al., 2014; Siponen et al., 2015).

Computer self-efficacy refers to one's confidence to learn and contribute to information security (Stajkovic & Luthans, 1998). Computing self-efficacy skills are learning competencies, such as computer engineering, coding, system security, writing standard operating procedures,

and promoting ethical compliance (Davis et al., 1989; Gist, Schwoerer, & Rosen, 1989; Potosky, 2002). When self-efficacy is weak, users may be reluctant to share this information because of embarrassment and may be averse to asking for assistance. Computer self-efficacy can change and improve through training and information security knowledge sharing (Bease and Salanova, 2006; Safa et al., 2016). Information security training and awareness is known to positively affect an attitude toward user behavior compliance (Abawajy, 2014; Bryce & Fraser, 2014; Dineve and Hu, 2007; Infinedo; 2014; Safa et al., 2015). Response efficacy refers to one's belief that adhering to information security controls reduces enterprise risk and threats posed by cyber adversaries (Siponen et al., 2014).

Employee Information Security Conscious Care Behavior

Employee information security conscious care behavior (ISCCB) is the process by which users think about and assess compliance with information security controls (Safa et al., 2015). Knowledge sharing and consulting with subject matter experts positively impacts user compliance (Cox, 2012; Furnell & Clarke, 2012; Safa et al., 2015; Safa et al., 2016). Some users may care about what others perceive in social situations – especially among groups (Huang & Chuang, 2007). An intention is a cognitive decision to conform to behavior toward compliance (Safa et al., 2016). ISCCB are known to reduce user apathy, laziness, lack of knowledge, or discontentment (Safa et al., 2015).

Employee ISCCB model is as an important attribute of the UWM pilot study because it is known to have a positive association toward compliance and can contribute to reducing the enterprise risk (Albrechtsen, 2007; Albrechtsen and Hovden, 2010; Bélanger et al., 2017; Box and Pottas, 2014; Furnell and Clark, 2012; Ghaznini & Shukur, 2016; Kolkowska and Dhillon, 2013; Humaidi and Balakrishnan, 2017; Rhee et al., 2009; Safa et al., 2016; Safa and Von Soms, 2016; Siponen et al., 2014; Stanton et al., Tomson et al., 1998; Veiga and Martins, 2017).

Information security training and awareness improve user information security countermeasures (Albrechtsen, et al., 2010). Sharing knowledge is known to also improve information security awareness and positively impact information security compliance (Safa et al., 2015; Safa et al., 2016). The Safa et al. (2015) research model incorporates the theoretical constructs associated with TBP (attitude, subjective norms, and perceived behavioral controls) and the PMT (self-efficacy and threat appraisal), as well as information security awareness, organizational policies, and experience and involvement (see Table 14).

Social Norms and Knowledge Sharing

Social norms is an attribute that users exhibit by observing and assessing the social and cultural workplace milieu. Social norms are known to positively impact user behavior toward information security behavior compliance (Li, Zhang, & Sarathy, 2010 and Safa et al., 2016). Social Bond Theory relates to social norms in that people can conform behavior among groups (Hirschi, 1991). When group dynamics support the organizational culture and values toward information security and compliance, users are more likely to commit to sharing knowledge. Research suggests that sharing knowledge improves information security (Bai et al., 2017; Chen et al., 2015; D'Arcy et al., 2009; Dojkovski, Lichtenstein, & Warren, 2012; Fishbein & Ajzen, 2010; Ghaznini & Shukur, 2016; Katz & Stotland, 1959; Kelokunnas & Kuusisto, 2003; Safa et al., 2015; Safa et al., 2016). Research confirms that barriers to knowledge sharing increase enterprise-level risk and reduce user self-efficacy (Amaya, 2013).

Method

The aim of the UWM pilot study was to test the reliability of the secure UWM REDCap survey application and assure that the 29-statement survey could be consistently distributed to 39 UWM ITS-Security information technology and information security professionals. The pilot study provided an opportunity to assess the reliability of the survey instrument and determine if

the data could be reliably exported to the IBM Statistical Package for Social Sciences (SPSS) analysis. Descriptive statistics from the UWM pilot study ($n = 32$) are presented as tables and there are a few comparisons with the Safa et al. (2015) survey ($n = 212$). The Safa et al. (2015) pilot test survey consisted of 32 pilot test participants from the information technology and information security professions.

The UWM pilot study incorporated the theoretical constructs associated with the Theory of Planned Behavior (attitude, subjective norms, and perceived behavioral control), the Protection Motivation Theory (self-efficacy), and information security awareness, organizational policy, and experience and involvement, and the employee ISCCB model (Safa et al., 2015). One of the advantages of performing a pilot test survey is being able to determine if all the survey statements from the Safa et al. (2015) survey were replicated.

Research Design

The UWM pilot study sets the stage for a larger-scale survey deployment and results will contribute to our understanding about user behavior compliance and its impact on reducing the likelihood of an incident leading or contributing to a privacy breach. User behavior is considered the strongest predictor of the compromise to patient privacy and security and is positively associated with compliance toward information security (Rajendran & Shenbagaraman, 2016). This pilot study tested the reliability of REDCap survey application and it afforded an opportunity to review the survey statements and make future changes. A large-scale survey deployment at a major medical center will contribute to the Healthcare and Public Health Sector's understanding about human behavior compliance and greatly improve our understanding about the types of cyber threats posed by cyber criminals, nation states, and transnational organized crime groups that operate in the dark web (Aloul, 2012; Cain, Edwards, & Still, 2018; Holt et al., 2016; Long, 2013; Pike, 2011; Seidenberger, 2016).

The Research Electronic Data Capture Online Survey Application

UWM is part of the Research Electronic Data Capture (REDCap) Consortium, which is headquartered at Vanderbilt University. There are 3,754 active institutions in 131 countries participating in the REDCap consortium and it is a secure (HIPAA-approved) survey application that is capable of administering surveys at multi-sites, including longitudinal clinical trial research studies (Vanderbilt University, 2019). UWM REDCap survey offers survey project design tools, optional survey attributes, validation preferences, and preferences for structured field types (single answer or multiple drop-down menus). UWM REDCap participates in the internal UWM ITS-Security Risk Management Program to ensure compliance with administrative, technical, and physical information security controls.

Sampling and Demographics

UWM participants were selected using a combination of cluster and convenience sampling, a technique that selects a sample based on a similar characteristic (Miller, 1991). Thirty-nine information technology and security professionals agreed to participate in the UWM pilot study and there were a total of thirty-four valid surveys from which to present descriptive statistics (see Table 2).

Table 2

UWM Pilot Study Participants by Age, Education, and IT Security Experience

Characteristic	<i>n</i>
Age	
18-25	2
26-35	2
36-45	2
46-55	13
56-65	15
26-35	2
Education	
Some College	5
Technical Certification	2
Undergraduate Degree	14
Graduate Degree	7
Post-Graduate	2
Some College	5
MD/PhD/JD/Fellowship	4
Years of work experience	
0-2	10
3-9	3
10-15	8
16-20	4
21-more	9
0-2	10

Types of IT and information security staff included, security architecture engineers, risk management analysts, system administrators, part-time interns, digital forensic engineers, risk assessment specialists, incident response subject matter experts, IT managers, senior IT leaders, and data center operations management personnel. REDCap disseminated the 29-statement pilot-test survey via email to 39 information technology and information security employees serving with the UW Medicine ITS-Security organization. Once participants acknowledged the Seattle University Consent to Participate in Research, respondents were given 15 business days to complete the survey. Through the REDCap application, the Principal Investigator sent periodic reminders to respondents who had not started nor completed the survey. No direct identifiers,

such as names, emails, or position titles were identified nor collected by REDCap. Only indirect identifiers were collected, including gender at birth; age; education; years of compliance experience; information security experience; and accessibility to the UWM Compliance Policies and Information Security Standards.

UWM Pilot Test Administration

The UWM pilot survey was administered via the secure REDCap application to 39 UWM information technology and security professionals. Safa et al. (2015) pilot survey ($n = 32$) also included information technology and information security professionals (Appendix B). Both pilot studies examined the reliability and validity of the survey instruments, as well as facilitated feedback from participants. Another purpose of the UWM pilot survey was to determine the feasibility of data collection from the REDCap application and confirm that all the statements from the Safa et al. (2015) survey were incorporated. The UWM pilot study presented an opportunity to gain knowledge about preliminary response patterns, compare descriptive statistics, and uncover any gaps that could be remediated in preparation for a larger-scale survey deployment.

The Principal Investigator contacted the UWM ITS-Security professionals, reviewed the pilot study's purpose, and solicited participation. The Seattle University Consent to Participate in Research was emailed and once participants agreed to participate, the participant names were added to the secure REDCap application. The UWM pilot survey was comprised of a 4-point Likert scale, including 1-Strongly Agree; 2-Agree; 3-Disagree; 4-Strongly Disagree. The Safa et al. (2015) pilot study utilized a 5-point Likert scale, including 1-strongly agree; 2-agree; 3-neither agree or disagree; 4-disagree; and 5-strongly disagree. The Principal Investigator omitted the 'Neither Agree or Disagree' option because of the limited number of participants and as a covered entity, UWM mandates that users comply behavior toward compliance (policies) and

information security controls (UWM ITS-Security Information Security Standards).

Results

Although the survey statements were similar to the Safa et al. (2015) survey, the UWM pilot study statements were modified because UWM underscores the importance of user compliance with UWM Compliance Policies and UWM ITS-Security Information Security Standards. UWM publishes quarterly information security and cybersecurity news bulletins, hosts quarterly ‘All-Hands’ meetings, and ensures that knowledge-based articles are up to date for workforce serving with the UWM Help Desk organization. Other means to inform UWM employees is through public partnerships with law enforcement, the U.S. Department of Health and Human Services, the Department of Homeland Security (Cybersecurity & Infrastructure Security Agency, 2020), and private information sharing and analysis organizations, such as the Health Information Sharing and Analysis Center (Health Information Sharing and Analysis Center, 2020). Tables 2-8 provide side-by-side comparisons with the Safa et al. (2015) survey ($n = 212$) and the UWM pilot test survey ($n = 34$).

Information security awareness, organizational policy, as well as experience and involvement with information security impact user behavior compliance (Ajzen, 1991; Albrechtsen, 2007; Anderson & Agarwal, 2010; Furnell & Clarke, 2012; Infinedo, 2014; Wood & Kankanhalli, 2007; Lee & Larson, 2009; Rhee, 2009; Safa et al., 2015; Safa et al., 2016). Safa et al. (2015) espouses that information security awareness is known to mitigate information security risk. Cox (2012) found that if a user is not exposed to information security awareness, then there is a lack of understanding and appreciation about full scope of risk that could negatively impact the organization. Ongoing compliance policy and information security awareness can positively impact computer self-efficacy (Bease & Salanova, 2006; Safa et al., 2016). Table 3 depicts the survey statements posed by Safa et al. (2015) and modified for the

UWM pilot study survey.

Table 3

Information Security Awareness (ISA) Item Statements

ISA Item	Safa et al., (2015) Survey	UW Medicine pilot study
1	I am aware of potential security threats.	UW Medicine promotes information security awareness
2	I have sufficient knowledge about the cost of information security breaches.	Information security awareness helps me to understand that a risk may lead or contribute to an incident, which could cause the loss or compromise of Confidential information.
3	I understand the risk of information security incidents.	UW Medicine promotes information security awareness.
4	I keep myself updated in terms of information security awareness.	Information security awareness improves my information security compliance behavior.
5	I share information security knowledge to increase my awareness.	Sharing knowledge improves my information security compliance behavior.

Note. ISA = information security awareness.

Information security organizational policy statements were different from the Safa et al. (2015) survey because UWM promotes, educates, and provides updates to users when there are revisions or new information regarding privacy (compliance) policies and UWM ITS-Security Information Security Standards (see Table 4). UWM also incorporates UW administrative policy statements (APS). For example, APS 2.6 is entitled, “Information Security Controls and Operational Practices requires workforce to implement and maintain administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of UW information (University of Washington Policy Directory, 2013).

Table 4

Information Security Organizational Policy (ISOP) Item Statements

ISOP Item	Safa et al., (2015) survey	UW Medicine pilot study
1	Information security policies and procedures are important in my organization.	Organizational compliance policies and information security standards are important to me.
2	Information security policies and procedures affect by behavior.	Compliance policies and information security standards affect my behavior towards compliance.
3	Information security policies and procedures have attracted my attention.	Compliance policies and information security standards attract my attention.
4	Behavior in line with organizational policies and procedures is of value in my organization.	Compliance policies and information security standards teach me how to apply best practices.

Note. ISOP = Information Security Organizational Policy.

The information security experience and involvement means mastering administrative, physical, technical, and environmental skills, as well as applying the relevant security controls to protect Confidential information (see Table 5). UWM promotes cross-organizational collaboration between clinical staff and ancillary clinical care services. Information technology system administrators and data center operations personnel, for instance, monitor systems and applications (uptime and outages) and environmental controls, such as heating, air conditioning, and humidity.

Table 5

Information Security Experience and Involvement (ISEI) Item Statements

ISEI Item	Safa et al., (2015) survey	UW Medicine pilot study
1	My experience increases my ability to have a safe behavior in terms of information security.	My experience ensures my behavior complies with policies and information security best practices.
2	I am involved with information security and I care about my behavior in my job.	My experience helps me to care about protecting UW Medicine Confidential information.
3	My experience helps me to recognize and assess information security threats.	My experience helps me to recognize and information security threat.
4	I can sense the level of information security threat due to my experience in this domain.	Due to my information security-compliance experience, knowledge sharing with co-workers benefits UW Medicine.
5	My experience helps me to perform information security conscious care behavior.	Intentionally omitted.

Note. ISOP = Information Security Experience and Involvement.

UWM promotes information security compliance by ensuring that people, processes, and the internet of medical things conform to legal, regulatory, UWM Compliance Policies and UWM ITS-Security Information Security Standards. Employee attitude consists of positive or negative feelings about information security compliance. UWM fosters communication by recognizing employees for exemplary efforts to protect and preserve UWM Confidential information (see Table 6). Subjective norms survey statements between Safa et al. (2015) and the UW Medicine survey are similar (see Table 7). It is important to gauge how social norms impact information security behavior in healthcare settings.

Table 6

Attitude (ATT) Item Statements

ATT Item	Safa et al., (2015) survey	UW Medicine Pilot Study
1	Information security conscious care behavior is necessary.	My attitude towards information security compliance is positive.
2	Information security conscious care behavior is beneficial.	My attitude about information security compliance is beneficial to UW Medicine.
3	Practicing information security conscious care behavior is useful.	My attitude towards information security compliance affects my behavior.
4	I have a positive view about changing users' information security behavior to conscious care.	My attitude towards information security compliance may influence others to comply their behavior.
5	I believe that information security conscious care behavior is valuable in an organization.	My attitude towards information security compliance is valued by UW Medicine.

Note. ATT = Attitude.

Table 7

Subjective Norms (SN) Item Statements

SN Item	Safa et al., (2015) survey	UW Medicine pilot study
1	Information security policies in my organization are important for my colleagues.	It is important to role-model information security compliance behavior for co-workers.
2	My colleague's information security behavior influences my behavior.	My coworker's information security compliance behavior influences my behavior.
3	Information security culture in my organization influences my behavior.	An information security culture influences my behavior.
4	My boss's information security behavior influences my behavior.	When leader's role model information security compliance behavior, it affects my information security compliance behavior.

Note. SN = Social Norms.

The concept of information security self-efficacy (ISSE) is particularly important because UWM employees, such as clinicians and ancillary staff, hold advanced degrees and board certifications. Faculty and professional staff may also hold advanced degrees and technical certifications. Due to the complex nature of patient care delivery and serving in the information technology and security disciplines, self-efficacy requires users to not only cope with information security threats, but also be capable of applying information security controls to reduce organizational risk (see Table 8).

Table 8

Information Security Self-Efficacy (ISSE) Item Statements

ISSE Item	Safa et al., (2015) survey	UW Medicine pilot study
1	I have the skills to protect my business and private data.	I possess the training and skills to safeguard Confidential information.
2	I have the expertise to protect my business and private data.	I am confident about safeguarding Confidential information.
3	I think the protection of my data is in my control in terms of information security violations.	Protecting Confidential information is within my control.
4	I have the ability to prevent information security violations.	I have the ability to prevent information security violations.

Note. ISSE = Information Security Self-Efficacy.

The employee information security conscious care behavior model merges previous research about the positive associations from the theory of planned behavior and the protection motivation theory to mitigate enterprise risk (Safa et al., 2015). Information security awareness, organizational policies and information security experience and involvement are also part of the ISCCB model. It is essential that healthcare organizations understand human behavior motivation and formation to reduce the likelihood of human errors, mistakes, and apathy. Table 8 presents item statements about how users think about human behavior compliance with information security controls. At UWM, information security and information technology subject matter experts (SMEs) rotate on-call 24 hours a day, 365 days a year. UWM SMEs are trained to respond to user compliance and information security questions. Subject matter expert interventions are a means to improve user information security compliance behavior.

Table 9

Information Security Conscious Care Behavior (ISCCB) Statements

ISCCB Item	Safa et al., (2015) survey	UW Medicine pilot study
1	I consider information security best practices.	Intentionally omitted.
2	Before taking any action that affects information security, I think about its consequences.	I think about how my information security behavior can reduce organizational risk.
3	I talk with security experts before I do something that relates to information security.	I can contact compliance or information security experts before I make a decision.
4	I talk with security experts before I do something that relates to information security.	I consider recommendations made by compliance and information security subject matter experts.
5	To avoid repeating prior mistakes, I consider my previous information security experience.	My information security compliance behavior helps me to avoid making mistakes.

Table 10 depicts the figures for accessibility to accessibility to the UWM Compliance Policies and the UWM ITS-Security Standards.

Table 10

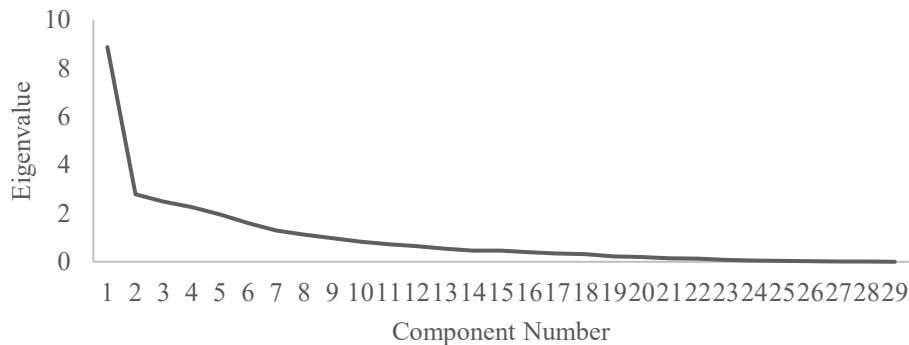
UWM Pilot Survey-Accessibility to Compliance Policies and Information Security Standards

Accessibility	Response	<i>n</i>	Frequency
Accessibility to Compliance Policies	Yes	32	94.4
	No	2	5.6
Information Security Standards	Yes	29	85
	No	5	15

Discussion

There were 39 UWM pilot surveys administered and five were incomplete, which resulted in an 87% response rate (*n* = 34). The Safa et al., (2015) survey included respondents from the healthcare sector at 11.79 %; Telecom/Information Technology (40.5%); Retail (16.98%); Education (5.19%); and Finance/Insurance (22.64%).

The scree plot (see Figure 1) depicts components 1-8 in a downward curve and contains the eigenvalues for each on the vertical y-axis and the number of components on the horizontal x-axis (Cattell, 1966). Once the slope begins to level off, the other remaining items do not contribute to explaining the variance (Cattell, 1966).

Figure 1*UWM Pilot Study Scree Plot***Conclusion****Limitations of Existing Research**

Due to the survey statements being modified from the original Safa et al (2015) survey ($n = 212$), the principal component analysis (PCA) could not be reliably compared and contrasted. The PCA, which is based upon the Pearson correlation coefficient, is a variable reduction technique to identify and explain as few components as possible (Laerd Statistics, 2019). In addition, the ideal sample size recommended should result in no fewer than 150 responses (Laerd Statistics, 2019). Implicit bias was introduced when the Principal Investigator self-selected the 39 UWM ITS-Security information technology and security employees from an estimated total user population of approximately 600 employees (Fowler, Jr., 2009). Closed-ended statements frame static responses and by not offering participants an opportunity to express qualitative statements, our understanding about user behavior formation is incomplete. Participants informally spoke with or emailed the Principal Investigator to suggest future changes. The number of responses ($n = 34$) was not large enough to make or draw meaningful conclusions (Creswell, 1994).

Future Integration of the Structural Equation Model

Due to the limited number of pilot study participants, a structural equation modeling (SEM) was not conducted; however, during a larger-scale survey, the SEM will be introduced. The structural equation modeling would be a key requirement to explore not only multiple relationships, but also to take into account the latent variables, such as information security awareness, information security organizational policy, the perception of risk (perceived behavioral control), and information security experience and involvement (Safa et al., 2015; Zweig & Webster, 2003). SEM may confirm other research, and also reveal positive associations with information security awareness, organizational policy, subjective norms, information security experience and involvement, attitude toward information security, threat appraisal, and self-efficacy (Safa et al., 2015). The Principal Investigator accidentally omitted the Safa et al. (2015) statements associated with the Protection Motivation Theory (PMT), which will have to be introduced when a larger-scale survey is created.

Directions for Future Research

Due to the COVID-19 pandemic many employees are working-from-home while others work in clinic or hospital settings, or there may be a hybrid of both working conditions. It would be important to statistically compare the two types of UWM NEO attendees (in-person versus virtual) and determine if there were risk to confidential information systems (Butler, 2019). Examining data sets from both in-person and virtual training may have implications for information security behavior compliance.

Offering the large-scale survey in a non-English language may improve the likelihood of participation from a large ethnic group. The UW School of Medicine promotes diversity through the Center for Health Equity, Diversity and Inclusion (CEDI), whose mission is to ensure health equity by sponsoring regional partnerships, which are designed to improve educational research

opportunities and patient care delivery (Center for Health Equity, Diversity & Inclusion, 2018).

If the large-scale survey was introduced in a non-English language, then, perhaps survey participation may increase for UWM employees for whom English is not their first language.

The Principal Investigator is interested in collaborating with the CEDI and UWM Human Resources to determine the feasibility of administering the survey in a non-English language.

Large-Scale Survey Hypotheses

The large-scale survey would be offered for approximately 30 business days to accommodate UWM employees who may be on personal leave, family leave, sick leave, or are temporarily unavailable due to other mission-essential priorities. It is known that UWM administers a variety of surveys and some workforce members may experience survey burnout. Therefore, to encourage survey completion, the Principal Investigator would offer \$15 Starbucks egift cards to 50 participants.

It will be also important to arrange virtual or phone qualitative interviews with leadership to gain a better understanding about any administrative, technical and physical limitations of deploying a large-scale survey. In addition, it will be important to arrange virtual or phone qualitative interviews with the UWM pilot study participants to gain an appreciation for the challenges encountered while taking the survey. The Principal Investigator will host a virtual meeting to solicit additional feedback from survey participants, as well as other organizational leadership who may have an interest in participation, i.e., members of the Seattle University Crime & Justice Center. Finally, presenting the information at a community forum of healthcare professionals, cybersecurity and law enforcement officials, and non-profit groups at the Seattle University sponsored Crime and Justice center may also enhance the quality, reliability, and validity of the large-scale survey. In a larger-scale survey, statistical modeling analysis will either be the statement of *null* (H_0) and signified by \leq , $=$, or \geq , the alternate, or other of *null* (H_a),

as signified by $<$, \neq , $>$ (Fisher, 1956, Newman, Ed., 1956; Larson & Farber, 2006). The following hypotheses under consideration include:

- **H1:** Information Security (IS) awareness has a positive effect on attitude.
- **H2:** Organizational policies have a positive effect on subjective norms toward performing ISCCB.
- **H3:** Users' experiences and involvement have a positive effect on perceived behavioral control toward performing ISCCB.
- **H4:** Attitude toward information security has a positive effect on performing ISCCB.
- **H5:** Subjective norms have a positive effect on performing ISCCB.
- **H6:** Information security self-efficacy has a positive effect on performing ISCCB.

User Behavior and the Healthcare and Public Health Cyber Dependencies

Due to the heavily regulated nature of the Healthcare and Public Health Sector, it is important to understand and measure how poor information security behavior may contribute to increasing information security risk to confidential information systems and assets. According to the Protenus Breach Barometer Report (2018), there were approximately 4.39 million records exposed from 117 data breaches (HIPAA Journal & Protenus, 2018). Approximately 23% of data breaches were attributed to insider wrongdoing and error contributed to 15% of all records exposed in the third quarter of 2018 (HIPAA Journal & Protenus, 2018).

The Healthcare and Public Health Sector is one of the 17 U.S. critical infrastructure sectors and because this sector contributes approximately 18% to the U.S. gross national product, cyber adversaries perceive the healthcare sector as a lucrative and financially rewarding target to exploit (Appendix D). Types of adversarial targets include to the proprietary nature of medical research and development (COVID-19), ePHI, personally identifiable credit card repositories, insurance claims, and pharmaceutical information. The Healthcare and Public Health subsectors include direct healthcare systems; health information technology; health plans and payers; mass

fatality management services; medical materials; laboratories, blood, and pharmaceuticals; public health programs (federal, state, tribal, and territorial).

As the healthcare sector continues to adopt digital technology solutions to improve patient care delivery, increase worker productivity, and decrease the costs associated with patient readmission rates, user behavior compliance studies are essential to reduce the likelihood of a risk, i.e., a user, committing an error, miscalculation, or hacking to produce a political, social, economic, or religious point. Healthcare organizations are also concerned about the user, who through intentional acts of corporate espionage and sabotage, increases the likelihood of a malicious cyber actor exploiting an Internet-connected device and leading or causing a major cyber incident that would adversely affect patient care delivery or possibly contribute to harm to public health.

According to the Price Waterhouse Cooper's 2020 Global Economic Crime and Fraud Survey, approximately 43% of those who responded, attributed crimes of fraud, such as antitrust, insider trading, tax fraud, money laundering, bribery, and corruption to insiders (p.7). The calculated costs resulted in the loss of \$100 million dollars and included direct financial losses, fines, penalties, and remediation costs (2020 Global Economic Crime and Fraud Survey, 2020). There are also other non-quantifiable costs, such as brand damage, reputation, employee morale, and lost future opportunities. Human behavior compliance in healthcare settings raises important questions about cyber preparedness and strategies to prevent a catastrophic cyber incident that may also gravely impact patient care delivery, cause public harm, and inflict damage to global economic wealth and human capital. This research highlights the timeliness of continuing to pursue human behavior studies and examine employee cybersecurity education, training, and awareness programs to measure user behavior compliance that may mitigate the risk of a cyber incident.

There is a national interest in preventing a major cybersecurity event. The U.S. Cyberspace Solarium Commission, co-chaired by Senator Angus King (I-Maine) and Representative Mike Gallagher (R-Wisconsin), presented a report about a U.S. cyber deterrence strategy in cyber space (King & Gallagher, 2020). There is an effort to create a national strategy to defend the U.S. against cyber attacks. Since there is a lack of healthcare-specific human behavior studies, this is a timely pilot study to continue and plan for a larger-scale survey about human behavior compliance and learn if human behavior compliance is a root cause of poor cybersecurity hygiene practices (Kruse et al., 2017).

Healthcare and Public Health Sector Cyber Preparedness

Since human behavior studies identify users as one of the weakest links in organizations, it is increasingly apparent since the COVID-19 global pandemic that a work-from-home workforce could be another organizational risk to confidential information systems and assets (Ahmad, & Ismail, 2010; Akhunzada, Kam, 2015; Aloul, 2012; Cain, Edwards, & Still, 2018; Long, 2013; Narayana, Sookhak, & Anuar, 2015; Pike, 2011; Seidenberger, 2016). Due to the long-term consequences of the COVID-19 pandemic, it is important to consider user behavior compliance in work-from-home environments. Perhaps this concept could be explored by leadership and included as part of the large-scale survey deployment.

Users in work-from-home environments may not have the robust security controls that office parks offer. How are business entities accounting for users complying with information security controls – such as applying security updates to home Wi-Fi networks. Some workers may not have had the opportunity to collect and utilize enterprise-issued devices and laptops and are consigned to using their personally owned devices and laptops which that may not host an up-to-date anti-virus program. Confidential data may be inadvertently stored or transmitted on unsecure personally owned devices and laptops. The Healthcare and Public Health Sector, as

well as the other 16 U.S. national critical infrastructure sectors, ought to consider promulgating new compliance policies to address work-from-home information security challenges.

Since the global COVID-19 pandemic crisis, there is a new work-from-home economy that has applied additional burden on the national cyber Internet critical architecture infrastructure and may increase the likelihood of exposing public and private industry cyber weaknesses (King & Gallagher, 2020). Work-from-home users may become targets of opportunity by scam artists who conduct fraudulent COVID-19 phishing campaigns to trick users into opening an innocuous email attachment to gain unauthorized access to confidential healthcare systems and facilities.

Due to the unprecedented global COVID-19 pandemic, employees may be working from home for the foreseeable future and some researchers may be conducting vaccine research from remote locations and there may be risks to confidential information systems and assets. The U.S. Cyberspace Solarium Commission illustrates a comparison between the global response to the COVID-19 pandemic and the global response required if there were a major cyber event that caused additional delays to healthcare delivery operations. This type of cyber disaster could wreak additional burdens upon the Healthcare and Public Health Sector, as well as negatively impact the local, regional, and global economies. Within four weeks of the pandemic reaching North America, an estimated 22 million Americans filed for unemployment (HUB Staff Report, 2020). A major cyber event that could disrupt the global Internet security architecture, which could lead or cause another global disruption in critical healthcare supply chain management, such as protective equipment for healthcare workers and medicines. The U.S. critical infrastructure sectors provide a cyber independent ecosphere for private and public sector industries and any disruption could negatively impact employees providing and supporting patient care delivery, electricity, fresh water, emergency communications, data center back-up

and restore capabilities, and ancillary support services to clinics, rehabilitation centers, financial services, and the insurance industry. These types of scenarios confirm the saliency of planning for and conducting large-scale user behavior surveys in healthcare settings.

Healthcare Sector Cyber Event Preparedness

In 2019, under the National Defense Authorization Act, the U.S. Cyberspace Solarium Commission was tasked to work on a national cybersecurity strategy and cyber deterrent plan to reduce the likelihood of a major cyber event from severely impacting the nation's critical infrastructure sectors, including the Healthcare and Public Health Sector (King & Gallagher, U.S. Cyberspace Solarium Commission, 2020). The U.S. Cyberspace Solarium Commission was tasked to address the political, military, economic, and social challenges that America faces in light of increasing dependence upon the Internet and the increased cyber interdependencies that drive economic growth, social stability, and military preparedness. The Solarium Commission is composed of the Executive Branch commissioners, members from academia, and industry leaders from the finance sector, information security technology, communications, insurance, and members from the Software and Information Industry Association. Other members include the Hague Center for Strategic Studies, National Governors Association, Royal United Services Institute for Defense and Security Studies, The MITRE Corporation Center for National Security, U.S. Chamber of Commerce, Water Information Sharing and Analysis Center, PricewaterhouseCoopers, Rural Electric Cooperative Association, Institute for Critical Infrastructure Technology, Information Technology Industry Council, Financial Services Information Sharing and Analysis Center, and the Health Information Sharing and Analysis Center (King & Gallagher, 2020).

The Commission conducted over 300 interviews and recommends a tiered or layered cyber deterrent strategy. First, it is recommended that the U.S. work with domestic and other

international allies to categorize and define responsible behavior in cyberspace (King & Gallagher, 2020, p. 1). Second, it is recommended that the U.S. initiate a federal-level program, in concert with global industry sector collaboration, to deter and prevent cyber adversaries from gaining unauthorized access to critical networks and security architecture (King & Gallagher, 2020, p. 1). The Commission also recommends that the U.S. plan to offensively strike back against cyber adversaries, including nation states that are intent on instigating fear, causing social unrest, or harm to public health, the United States may need to plan, invest in a cyber resilient infrastructure, and possess the capability of launching a cyber event (King & Gallagher, 2020, p. 1).

In light of recent global events, the U.S. Healthcare and Public Health Sector must strengthen its understanding about user behavior, especially the insider threat. Through a larger-scale user behavior study, a major healthcare organization will be able to collaborate with the Seattle University Crime and Justice Research Center and local not-for-profit organizations to gain insight about a work-from-home workforce that is required to comply behavior organizational information security controls. Exploring the possibility of a collaboration with the local Cambia Health staff may offer innovative contributions from a network of over 20 companies that are driven to improve healthcare to approximately 70 million Americans (Cambia Health Solutions, 2020).

The U.S. Cyberspace Solarium Commission published a white paper (2020) and the report illustrates a connection between the global pandemic responses and the potentially dangerous outcomes if there were a major cyber event (King & Gallaher, Cybersecurity Lessons from the Pandemic: CSC White Paper #1, 2020). There is a sense of urgency about the message to illustrate that a major cyber disruption could exacerbate economic, social, political, military, and public health problems (King & Gallaher, Cybersecurity Lessons from the Pandemic: CSC

White Paper #1, 2020). The white paper urges the federal government to review 32 recommendations and address poor cyber preparedness to prevent, detect, contain, respond to, and mitigate a major cyber event against U.S. critical infrastructure sectors. The Commission recommendations include digitizing critical infrastructure services; protecting the Internet's security architecture to help the new work-from-home workforce; formulating public policies that address opportunistic cybercrime activities; creating funding for law enforcement cybersecurity training; providing higher education funding to train the next generation of cyber technology experts; increasing the utilization of artificial intelligence; collaborating with international allies to coordinate efforts to detect, report, prevent, respond to, and bring cybercriminals to justice; and determining how best to foster public and private partnerships to counter disinformation, which can instigate disinformation campaigns and cause public panic (King & Gallaher, Cybersecurity Lessons from the Pandemic: CSC White Paper #1, 2020).

There is a new era of interest in user behavior and linking a new large-scale survey to cyber preparedness in healthcare settings is an innovative approach to understanding how new compliance policies, training, education, and awareness programs can address the complex nature of a new work-from-home user. One means of determining if user behavior is influenced by new employee orientation and continuing compliance and information security training and awareness, is to launch large-scale surveys to measure how user behavior impacts and reduces the likelihood of a cyber event leading or causing the loss or compromise of confidential information systems that are dependent upon an aging security architecture. Now that the lessons learned from the pilot study are realized, it is important to seize upon the momentum and become a part of the solution, which can provide policy makers with information to assist with national preparedness efforts and reduce the likelihood of a major cyber event severely

impacting the United States Healthcare and Public Health Sector and our nation's national security.

References

- 2020 Global Economic Crime and Fraud Survey. (2020, February 26). *Fighting fraud: A never-ending battle*. Retrieved July 5, 2020, from PWC Fraud Survey:
<https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf>
- Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behavior Information Technogy*, 33(3), 236-247.
- Ahlan, A., Arshad, Y., & Lubis, M. (2011). Implication of human attitude factors toward information security awareness in Malaysia Public University. *International Conference on Innovation and Management*. Kuala Lumpur.
- Ajzen, I. (1991). Perceived behavior control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Sociology and Psychology*, 32, 1-20.
- Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50, 179-221.
- Ajzen, I. (2019, March 11). *Theory of Planned Behavior*. Retrieved 2019, from Theory of Planned Behavior: <http://people.umass.edu/aizen/tpb.html>
- Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs: Prentice-Hall.
- Akers, R. L. (1998). *Social Learning and social structure: A general theory of crime and deviance*. Boston: Northeastern University Press.
- Akers, R. L., & Sellers, C. S. (2013). *Criminological Theories: Introduction, Evaluation, and Application*. New York: Oxford University Pres.

- Akhunzada, A., Sookhak, M., & Anuar, N. (2015). Man-at-the-middle end attacks: analysis, taxonomy, human aspects, motivation, and future directions. *Journal of Network and Computer Applications, 48*, 44-57.
- Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computer Security, 26*, 276-289.
- Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation, and collective reflection: An intervention study. *Computers & Security, 29*, 423-445.
- Al-Omari, A., El-Garyar, O., & Deokar, A. (2012). Information security policy compliance: The role of information security awareness. *18th Americas Conference on Information Systems, 2*, pp. 1633-1640. Seattle: The Americas Conference on Information Systems.
- Aloul, F. A. (2012). The need for effective information security awareness. *Advance Information Technology, 3*(3), 176-183. doi:10.4304/jait.3.3
- Amayah, A. T. (2013). Determinants of knowledge sharing in a public sector organization. *Journal of Knowledge Management, 17*(2), 454-471. doi:http://dx.doi.org/10.1108/JKM-11-2012-0369
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a mulimethod empirical examination of home computer user security behavior intentions. *Management Information Systems Quarterly, 34*(3), 613-643.
- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

- Atasoy, H., & Ganju, K. (2018). The Spillover Effects of Health IT Investments on Health IT Investments on Regional Healthcare Costs. *Management Science*, 64(6), 2515-2534.
doi:<https://doi.org/10.1287/mnsc.2017.2750>
- Bachman, R., & Paternoster, R. (2009). *Statistics for criminology and criminal justice*. New York: McGraw-Hill.
- Badura, A. (1973). *Aggression: A social learning analysis*. Englewood, Cliffs: Prentiss-Hall.
- Bai, CPA, G., Jiang, PhD, J. X., & Flasher, PhD, CPA, R. (2017, June). Hospital Risk of Data Breaches. *JAMA Internal Medicine*, 177(6), 878-880.
doi:10.1001/jamainternmed.2017.0336
- Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84, 191-215.
- Bandura, A. (1998). *A social foundations of thoughts and action: A social cognitive theory*. Englewood Cliffs: Prentice Hall.
- Beas, M. I., & Salanova, M. (2006). Self-Efficacy beliefs, computer training compliance in academic medical centers. *Computers in Human Behavior*, 22, 1043-1058.
- Belanger, F., Collignon, S., Enget, K., & Negandar, E. (2017). Determinants of early conformance with information security policies. *Information Management*, 887-901.
- Box, D., & Pottas, D. (2014). A model for information security compliant behaviour in the healthcare context. *Procedia Technology*, 16, 1462-1470.
- Brown, S. A., Massey, A. P., Montoya-Weiss, M. M., & Burkman, J. R. (2002). Do I really Have to? User Acceptance of Mandated Technology. *European Journal of Information Systems*, 11, 283-295.

- Bryce, J., & Fraser, J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young people's online interactions. *Computers and Human Behavior, 30*, 299-306.
- Burgess, R. L., & Akers, R. L. (1966). A differential association-reinforcement theory of criminal behavior. *Social Problems, 14*, 128-147.
- Butler, S. (Ed.). (2019, March). *The UW Medicine Fact Book*, Number 41. Retrieved July 5, 2020, from UW Medicine Fact Book: Who we are and what we do:
<https://www.uwmedicine.org/sites/stevie/files/2019-04/Fact-Book-Interactive.pdf>
- Cain, A. A., Edwards, M. E., & Still, J. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36-45.
- Cambia Health Solutions, I. (2020, July 11). *Strategic Investing, Cambia Health Solutions*. Retrieved July 11, 2020, from Strategic Investing, Cambia Health Solutions:
<https://www.cambiahealth.com/>
- Cartwright, D. (1949). Some principles of mass persuasion: Selected findings of research on the sale of United States War Bonds. *Human Relations, 2*, 253-267.
- Cattell, R. B. (1966). The Scree Test for the Number of Factors. *Multivariate Behavioral Research, 1*(2), 245-276. Retrieved August 13, 2020, from
<https://babel.hathitrust.org/cgi/pt?id=mdp.39015003753046&view=1up&seq=282>
- Center for Health Equity, Diversity & Inclusion. (2018). *Center for Health Equity, Diversity & Inclusion*. Retrieved July 5, 2020, from Center for Health Equity, Diversity & Inclusion:
<http://cedi-web01.s.uw.edu/about-us/>
- Centers for Disease Control and Prevention. (2017, Jan 18). *Meaningful Use*. Retrieved 25 2018, from Meaningful Use: Introduction:
<https://www.cdc.gov/ehrmeaningfuluse/introduction.html>

Centers for Medicare & Medicaid Services. (2019, March 14). *Are You a Covered Entity?*

Retrieved January 11, 2020, from Are You a Covered Entity?:

<https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity>

Cerner Corporation. (2013). PubMed.gov. *Nursing Administration Quarterly*, 105-108.

doi:10.1097/NAQ.0b013e318286db0d

Chen, Y., Ramamurthy, K., & Kuang, W. W. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture. *Journal of Computer Information Systems*, 15(3), 11-19.

Cheng, L., Li, Y., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory.

Computer Security, 39, 447-459. Retrieved from

<http://dx.doi.org/10.1016/j.cose.2013.09.009>

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, 2(1), 26-38. doi:10.1080/23738871.2017.1298643

Cohen, J. K. (2019, March 25). Email now leads the pack as vector for healthcare data breaches.

Modern Healthcare, 49(12), p. 1. Retrieved January 22, 2020

Cost of a 2018 Data Breach Study: Global View. (2018, July). Benchmark research: IBM

Security and conducted by Ponemon Institute, LLC. Retrieved Dec 25 2018, 2018, from

<https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&>

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113, 48-52.

Cox, J. (2012). Information systems user security: a structured model of knowledge... *Computers in Human Behavior*, 28(5), 1849-1858.

- Creswell, J. W. (1994). *Research Design: A qualitative & quantitative approach*. Thousand Oaks: Sage Publications, Inc.
- Cullen, F. T., & Agnew, R. (2011). *Criminological Theory: Past to Present* (Fourth ed.). New York: Oxford University Press.
- Cyber and Infrastructure Analysis. (2017, Jan 24). (U) *Healthcare and Public Health Sector Cyberdependencies*. Department of Homeland Security , National Protection and Programs Directorate. Washington D.C: Department of Homeland Security . Retrieved Jan 27, 2017, from Homeland Security Information Network : <https://hsin.dhs.gov>
- D. Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information system misuse: A deterrence approach. *Information Systems*, 20, 79-98.
- Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 72-94.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems*, 20:1, 79-98.
- Department of Health and Human Services. (2000, December 28). *Standards for Privacy of Individually Identifiable Health Information. Final Privacy Rule Preamble. Health Care Clearinghouse*. Retrieved March 10, 2019, from Standards for Privacy of Individually Identifiable Health Information. Final Privacy Rule Preamble. Health Care Clearinghouse: <https://aspe.hhs.gov/report/standards-privacy-individually-identifiable-health-information-final-privacy-rule-preamble/health-care-clearinghouse>
- Department of Health and Human Services. (2013, July 26). *Health Information Privacy*. Retrieved March 10, 2019, from HHS Health Information Privacy Business Associates:

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html>

Department of Health and Human Services. (2017). *HIPAA Data Breaches Affecting 500 Individuals*. Retrieved May 2018, from HIPAA Data Breaches Affecting 500 Individuals: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Department of Health and Human Services. (2017, June 16). *HITECH Act Enforcement Interim Final Rule*. Retrieved March 3, 2020, from HITECH Act Enforcement Interim Final Rule: HITECH Act Enforcement Interim Final Rule

Department of Health and Human Services. (2019, September 19). *Omnibus HIPAA Rulemaking*. Retrieved August 11, 2020, from Omnibus HIPAA Rulemaking: <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/index.html>

Department of Health and Human Services. (2017). *HIPAA Security Rule*. Retrieved from HIPAA Security Rule: <http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>

Department of of Homeland Security, Cyber & Infrastructure Security Agency. (2018, December 4). *Healthcare and Public Health Sector*. Retrieved February 29, 2020, from Healthcare and Public Health Sector: <https://www.cisa.gov/healthcare-and-public-health-sector>

Dinev, T., & Quing, H. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of Information Systems*, 8, 386-408.

Dojkovski , S., Lichtenstein, S., & Warren, M. (2012). Fostering information security culture in small and medium size enterprises: an interpretive study in Australia. *Proceedings of the*

- 15th European conference on information systems. University of St Gallen, (pp. 1560–1571).*
- Ewell, PhD, C. (2018, Sept). Review of Master's Student Thesis Proposal. (C. T. Panattoni, Interviewer)
- Fishbein, M. (1968). An Investigation of relationships between beliefs about an object and the attitude towards that object. *Human Relationships, 16*, 233-240.
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.
- Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. New York: Psychology Press.
- Food and Drug Administration (FDA). (2016, December 22). *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. (FDA, Ed.) Retrieved July 10, 2018, from Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff.
- Food and Drug Administration (FDA). (2020, January 23). *FDA Cybersecurity-Medical Devices and Digital Health*. Retrieved February 29, 2020, from FDA Cybersecurity: <https://www.fda.gov/medical-devices/digital-health/cybersecurity>
- Fowler, Jr., F. J. (2009). *Survey Research Methods*. Thousand Oaks: Sage Publications Inc.
- Fraser, B. J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. *Computer Human Behavior, 30*, 299-306.
- Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computer Security, 983-988*. Retrieved from <http://dx.doi.org/10.1016/j.cose.2012.08.04>.

- George, J., & Emmanuel, A. (2018). Cyber Hygiene in Health Care Data Breaches. *International Journal of Privacy and Health Information Management*, 6(1), 37-48.
- Ghaznini, A., & Shukur, Z. (2016). Awareness Training Transfer and Information Security Content Developmentn for Healthcare Industry. *International Journal of Advanced Computer Science and Application*, 7(5), 361-370.
- Ghazvini, A., & Shukur, Z. (2016). Awareness Training Transfer and Information Security Content Development for Healthcare Industry. *International Journal of Advanced Computer Science and Applications*, 7(5), 361-370.
- Gist, M., Schwoerer, C., & Rosen, B. (1989). Effects of alternative training methods on self-efficacy and performance in computer software training. *Journal of Applied Psychology*, 76(4), 884-891.
- Glueck, S., & Glueck, E. (1959). *Predicting Delinquency and Crime*. Cambridge: Harvard University Press.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis*. New Jersey: Pearson Prentice Hall.
- Hassan, N. H., & Ismail, Z. (2014). Investigation of Key Resistance Factors in Knowledge Sharing Towards Information Security Culture in Healthcare Organization. *The 8th International Conference on Knowledge Management in Organizations Social and Big Data Computing for Knowledge Management* (pp. 210-601). Springer Proceedings in Complexity DOI: 10.1007/978-94-007-7287-8_48 . doi:DOI: 10.1007/978-94-007-7287-8_48
- Health and Human Services. (2009, October 30). *Health Information Privacy*. Retrieved June 19, 2019, from HITECH Act Enforcement Interim Final Rule:

<https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html>

Health Information Sharing and Analysis Center. (2020). *Health Information Sharing and Analysis Center*. Retrieved May 16, 2020, from Health Information Sharing and Analysis Center: <https://h-isac.org/>

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information System*, 18, 106-125.

HHS.gov. (2017, June 16). *HIPAA for Professionals*. Retrieved November 29, 2019, from HHS.gov Health Information Privacy: <https://www.hhs.gov/hipaa/for-professionals/index.html>

Hill, K. G., Howell, J. C., Hawkins, D., & Battin-Pearson, S. R. (1999). Children risk factors for adolescent gang membership: Results from the Seattle Social Development Project. *Journal of Research in Crime and Delinquency*, 36, 300-322.

HIPAA Journal. (2018). Q3 Healthcare Data Breach Report: 4.39 Million Records Exposed in 117 Breaches. *HIPAA Journal*, 1-3. doi:November 7, 2018

HIPAA Journal. (2020). *HIPAA Guidelines on Telemedicine*. Retrieved July 14, 2020, from HIPAA Guidelines on Telemedicine: <https://www.hipaajournal.com/hipaa-guidelines-on-telemedicine/>

Hirschi, T. (1969). *Causes of Delinquency*. University of California Press.

Hirschi, T. (1991). *Causes of Delinquency*. New Brunswick: Transaction Publishers.

Hirschi, T. (2011). Social Bond Theory. In F. F. Cullen, & R. Agnew, *Criminological Theory: Past to Present* (pp. 215-223). New York: Oxford University Press.

HITECH Act Enforcement Interim Final Rule. (2017, June 16). Retrieved Oct 27, 2018, from Health and Human Services (HHS.gov): <https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html>

Holt, T. J., Smirnova, O., & Chua, Y.-T. (2016). *Data Thieves in Action: Examining the International Market for Stolen Information*. New York: Palgrave Macmillan, Springer Nature.

Hovland, C. I., & Rosenberg, M. J. (1960). Attitude, organization, and change . In C. I. Hovland, & M. J. Rosenberg, *Attitude organization and change; an analysis of consistency among attitude components* (pp. 1-14). New Haven, CT: Yale University Press.

HSS and OCR Enforcement Highlights. (2018, June 13). *Enforcement Results as of May 31, 2018*. doi:June 13, 2018

Huang, D.-L., Pei-Luen, Rau, P., Sakvebdt, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, 870-883.

Huang, E., & Chuang, M. (2007). Extending the theory of planned behavior as a model to explain post-merger employee behaviorism of IS use. *Computers in Human Behavior*, 23, 24-257.

HUB Staff Report. (2020, April 16). *COVID19's Historic Economic Impact, in the U.S. and Abroad*. Retrieved July 11, 2020, from COVID19's Historic Economic Impact, in the U.S. and Abroad: <https://hub.jhu.edu/2020/04/16/coronavirus-impact-on-european-american-economies/>

Hulme, G. V. (2020, Jan 13). U.S. Healthcare Data Breach Cost \$4 Billion in 2019. 2020 Won't be any Better. *Security Boulevard*, p. 1. Retrieved January 21, 2020, from

<https://securityboulevard.com/2020/01/u-s-healthcare-data-breach-cost-4-billion-in-2019-2020-wont-be-any-better/>

Humaidi, N., & Balakrishnan, V. (2017). Indirect effect of management support on users' compliance behavior towards information security policies. *Health Information Management Journal*, 47(1), 17-27.

IBM Security and Ponemon Institute. (2017, June). *Cost of Data Breach Study: Global Overview*. Retrieved May 2018, from Cost of Data Breach Study: Global Overview: <https://www.ibm.com/security/data-breach>

IBM Security and Ponemon Institute. (2017, Jun). *2017 Cost of Data Breach Study: Global Overview*. Traverse City: IBM Security and Ponemon Institute. Retrieved from www.ibm.com/security/data-breach

Infinedo, P. (2014). Understanding information systems security policy compliance: An empirical study of the effects of socialisation, influence and cognition. *Information Management*, 69-79.

Institute of Translational Health Sciences. (2019, March 11). *Research Electronic Data Capture (REDCap)*. Retrieved March 11, 2019, from REDCap: <https://www.iths.org/investigators/services/bmi/redcap/>

Jayanthi, A. (2016, May 11). *First known ransomware attack in 1989 also targeted healthcare*. Retrieved May 25, 2018, from First known ransomware attack in 1989 also targeted healthcare: <http://www.beckershospitalreview.com/healthcare-information-technology-/first-known-ransomware-attacke-in1989-aslo-targeted-healthcare.html>.

Johnston, A. C., & Warkentin, M. (2008). Information privacy compliance in the healthcare industry. *Information Management and Computer Security*, 16, 5-19.

Kam, R. (2015, Dec 2015). *The human risk factor of a healthcare data breach*. Retrieved July 27, 2019, from Tech Target Community:

<https://searchhealthit.techtarget.com/healthitexchange/CommunityBlog/the-human-risk-factor-of-a-healthcare-data-breach/>

Katz, D., & Stotland, E. (1959). A preliminary statement to a theory of attitude structure and change. In S. Koch, Ed., *Psychology: A study of a science* (Vol. 3, pp. 423-475). New York: McGraw-Hill.

Kelokunnas, T., & Kuusisto, R. (2003). Information security culture in a value net. *International Education Management Conference: Managing technologically driven organizations: the human side of innovation and change*, (pp. 190-194).

King, A., & Gallagher, M. (2020, March 11). *U.S. Cyberspace Solarium Commission*. Retrieved May 17, 2020, from U.S. Cyberspace Solarium Commission:

<https://www.solarium.gov/report>

King, A., & Gallaher, M. (2020, May). *Cybersecurity Lessons from the Pandemic: CSC White Paper #1*. Retrieved July 5, 2020, from Cybersecurity Lessons from the Pandemic: CSC White Paper #1: <https://www.solarium.gov/public-communications/pandemic-white-paper>

Kirkpatrick, K. (2015). Cyber policies on the rise. *Communication of the ACM*, 58, 21-23.

Koczkodaj, W. W., Mazure, M., Strzałka, D., Wolny-Dominia, A., & Woodbury-Smith, M. (2018). Electronic Health Record Breaches as Social Indicators. *Social Indicators Research*, 141, 861-871. doi:doi.org/10.1007/s11205-018-1837-z

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, 3-11.

- Krech, D., & Crutchfield, R. S. (1948). *Theory and problems in social psychology*. New York: McGraw-Hill.
- Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology Health Care, 25*, 1-10.
- Larson, R., & Farber, B. (2006). *Elementary Statistics: Picturing the World*. Boston: Pearson Custom Publishing.
- Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information Management, 6*, 707-718.
- Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*, 177-187.
- Leonard, Lori, N., Cronan, T. P., & Kreie, J. (2004). What influences in IT ethical behavior intentions - planned behavior, reasoned action, perceived importance, or individual characteristics. *Information Management, 42*(1), 143-158. Retrieved September 16, 2018, from <https://www.sciencedirect.com/science/article/abs/pii/S0378720604000163>
- Lewis, J. (2018). *Economic Impact of Cybercrime*. Center for Strategic & International Studies (CSIS). Washington D.C. : McAfee.
- Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.
- Liao, C., Chen, J.-L., & Yen, D. (2007). Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: An integrated model. *Computers in Human Behavior, 28*, 2804-2822.

- Loeber, R., & Stouthamer-Loeber, M. (1986). Family factors as correlates and predictors of juvenile conduct problems and delinquency. In M. Tonry, & M. Norval, *Crime and Justice* (pp. 29-149). Chicago: University of Chicago Press.
- Long, R. M. (2013). *Using phishing to test social engineering awareness of financial employees*. Ellensburg: Eastern Washington University.
- Lubold, G., & Volz, D. (2020, May 14). *U.S. Says Chinese, Iranian Hackers Seek to Steal Coronavirus Research*. Retrieved May 17, 2020, from The Wall Street Journal: <https://www.wsj.com/articles/chinese-iranian-hacking-may-be-hampering-search-for-coronavirus-vaccine-officials-say-11589362205>
- Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Healthcare*, 1-9. doi:10.3233/THC-151102
- Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Psychology*, 19, 469-479.
- Maennel, K., Maeses, S., & Maennel, O. (2018). Cyber Hygiene: The Big Picture. *Lecture Notes in Computer Science*, 11252, 1-9. doi:10.1007/978-3-030-03638_18
- Martin, A. B., Hartman, M., Washington, B., Catlin, A., & The National Health Expenditure Accounts Team. (2019). National Health Care Spending in 2017: Growth Slows to Post-Great Recession Rates; Share of GDP Stabilizes. *Health Affairs*, 38(1), pp. 96-106. Retrieved May 27, 2019, from <file:///C:/Users/carla/OneDrive/Seattle%20University/Thesis%20Research/National%20Affairs,%2038,%20No.%201%202019,%20pgs%2096-106/National%20Health%20Care%20Spending%20in%202017->

- %20Growth%20Slows%20to%20Post-Great%20Recession%20Rates;%20Shar%20of%20GDP%20
- Martin, A., Hartman, M., Aaron, B., & Aaron, C. (2019, January 1). National Health Care Spending in 2017: Growth Slows to Post-Great Recession Rates; Share of Gross Domestic Product Stabilizes. *Health Affairs*, 38(1), pp. 96-106.
- McAfee , & Lewis, J. A. (2018). *Center for Strategic and International Studies, Economic Impact of Cybercrime*. Retrieved March 2, 2020, from Center for Strategic and International Studies, Economic Impact of Cybercrime: <https://www.csis.org/analysis/economic-impact-cybercrime>
- McCord, W., & McCord, J. (1959). *Origins of Crime: A new Evaluation of the Cambridge Sommerville Youth Study*. New York: Columbia University.
- McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, 108, 57-68.
- Medicaid, C. f. (2018, September). *HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules*. doi:September 2019 - 9099001
- Mehrzad, R., & Barza , M. (2015). Are physician pagers an outmoded technology? *Technology Health Care*, 23(3), 233-241.
- Miller, D. C. (1991). *Handbook of Research Design and Social Measurement*. Newberry Park: Sage Publications, Inc.
- Montgomery, M., & Morgus, R. (2020, May 12). *What the Pandemic Tells Us About the State of U.S. Cybersecurity*. Retrieved May 12, 2020, from What the Pandemic Tells Us About the State of U.S. Cybersecurity: <https://www.justsecurity.org/70132/what-the-pandemic-tells-us-about-the-state-of-u-s-cybersecurity/>

- Narayana, S. G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information Systems. *Health Information Journal*, 16, 201-209.
- Nash, K. S., & Greenwood, D. (2006, September 15). The global state of information security. *Chief Information Officer (CIO) magazine*, 22(3). Retrieved June 15, 2019
- National Initiative for Cybersecurity Careers and Studies. (2018, November 28). Glossary - Explore Terms: A Glossary of Common Cybersecurity Terminology. U.S.A: Department of Homeland Security. doi:11.28.2018
- National Institute of Standards and Technology (NIST). (2019, February 8). *Computer Security Resource Center*. Retrieved February 29, 2020, from Cyber Security NIST Glossary: <https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary>
- National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4. (2015, 1 22). Security and Privacy Controls for Federal Information Systems and Organizations,. Gaithersburg, MD, U.S. Retrieved November 11, 2019, from <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>
- National Institute of Standards and Technology. (2013). *Glossary of Key Information Security Terms*. Computer Security Division Information Technology Laboratory. Gaithersburg: U.S. Department of Commerce. Retrieved from <http://dx.doi.org/106028/NIST.IR729r2>
- National Institutes of Health (NIH), U.S. Department of Health and Human Services. (2007, February 2). *NIH HIPPA Privacy Rule*. Retrieved July 28, 2019, from NIH HIPPA Privacy Rule: https://privacyruleandresearch.nih.gov/pr_06.asp
- National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis. (2018, May 8). Cybercrime and the Darknet: Effects on Cybersecurity Practices. *Critical Infrastructure Security and Resilience Notes*, p. 4.

National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis.

(2018, May 23). Healthcare and Public Health Cybersecurity Challenge: Legacy Findings. *Critical Infrastructure Security and Resilience Note*, p. 4.

Newman, Ed., J. R. (1956). Mathematics of a Lady Tasting Tea. In J. R. Newman, *The World of Mathematics* (Vol. 3, pp. 1512-1521). New York: Simon and Schuster.

Office of Civil Rights, U.S. Department of Health & Human Services . (2013, July 23). *Breach Notification Rule*. Retrieved January 5, 2019, from HHS.gov/Health Information Privacy.

Office of Civil Rights, U.S. Department of Health & Human Services (HHS). (2017, May 12).

The Security Rule. Retrieved Jan 5, 2019, from Health Information Privacy:

<https://www.hhs.gov/hipaa/for-professionals/security/index.html>

Office of Civil Rights, U.S. Department of Health & Human Services. (2016, June 16). *Health*

Information Privacy. Retrieved January 5, 2019, from Covered Entities and Business

Associates: <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>

Office of Cyber and Infrastructure Analysis, National Protection and Program Directorate, Department of Homeland Security. (2017). *(U) Healthcare and Public Health Sector Cyberdependencies*. Washington D.S.: DHS.

Office of the Chief Information Security Officer, DHHS. (2019, April 11). *H3 Intelligence*

Briefing Update: Dark Web PHI Market Place. Retrieved July 27, 2019, from H3

Intelligence Briefing Update: Dark Web PHI Market Place:

https://content.govdelivery.com/attachments/USDHSFACIR/2019/04/25/file_attachments/1199378/Dark%20Web%20primer.pdf

Otieno, O. C., Liyayla, S., & Odongo, B. C. (2015). Theoretical and Practical Implications of Applying Theory of Reasoned Action in an Information Systems Study. *Open Access Library Journal*, 2(e2054), 1-5.

- Patel, S. L., Ranney, D., Al-Holou, S., Frost, C., Harris, M., Lewin, S., & et al. (2010). Resident workload, pager communications, and quality of care. *World Journal of Surgery*, 34(11), 2524-2529.
- Pi, S.-M., Chou, C.-H., & Liao, H.-L. (2013). A study of Facebook groups: Members knowledge sharing. *Computers in Human Behavior*, 29(5), 1971-1979.
- Pike, M. (2011). *The magazine for the IT professional*. The Chartered Institute for IT. British Computer Society.
- Porter, G., Trevors, M., & Vrtis, R. A. (2018, March 18). *A Mapping of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule to the Cyber Resilience Review (CRR)*. Retrieved January 14, 2020, from <https://www.sei.cmu.edu/news-events/news/article.cfm?assetid=517006>
- Potosky, D. (2002). A field study of computer self-efficacy beliefs as an outcome of training: The role of computer playfulness, computer knowledge, and performance during training. *Computers in Human Behavior*, 18(3), 241-245.
- Proctor, R. W., & Proctor, J. D. (2006). Sensation and Perception. In G. E. Salvendy, , *Handbook of Human Factors and Ergonomics, 3rd Edition* . New York: John Wiley.
- Protenus,. (2018). Q3 2018 Protenus Breach Barometer: Insider-wrongdoing accounts for increasing number of breached patient records over the course of 2018. *Protenus Inc., in collaboration with databreaches.net*, 1-16. doi:Nov 2018
- Public Law 111-5. (2011). *Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities*. Washington D.C.: U.S. Government. Retrieved July 13, 2020, from <https://www.google.com/search?client=firefox-b-1-d&q=13407+of+the+HITECH+Act>

- Qualtrics. (2018, October). *Qualtrics Research Core Platform*. Retrieved October 9, 2018, from Qualtrics Online Survey Software: <https://www.qualtrics.com/research-core/survey-software/>
- Rajendran, S., & Shenbagaraman, V. M. (2016). A Study on Protection Motivation Theory and Information Systems Security Policy Complianc. *International Journal of Pharmaceutical Sciences Review and Research*, 40(2), 192-197.
- Reddy, M., McDonald, D., Pratt, W., & Shabot, M. (2005). Technology, work, and information flows: Lessons from the implementation of a wireless alert pager system. *Journal of Biomedical Infomatics*, 38(3), 229-238.
- Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28, 816-826.
- Rocha, F. W., Antonsen, E., & Ekstedt, M. (2014). Information security knowldege sharing in organizations investigating the effect of behavioral information security governance and national culture. *Computer Security*, 43(0), 90-110.
- Rogers, R. (1983). *Cognitive and physiological processes in fear of appeals and attitude change: A revised theory of protection motivation*. New York: Guilford Press.
- Safa, N. S. (2018, October 7). Type of Platform to Collect Data? (C. T. Panattoni, Interviewer)
- Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers & Security*, 53, 65-78.
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 70-82.

- Sahney, R., & Sharma, M. (2018). Electronic health records: A general overview. *Current Medicine Research and Practice*, 8, 67-70.
doi:<https://doi.org/10.1016/j.cmrp.2018.03.004>
- Scarfone, K., Jansen, W., & Tracy, M. (2008). *Guide to General Server Security*. Gaithersburg: U.S. National Institute of Standards and Technology.
- Schein, E. H. (1999). *The Corporate Culture Survivor's Guide*. San Francisco: Jossey-Bass.
- Schellman, C. L. (2018, April 24). *Certificate of Registration, Information Security Management System - ISO/IEC 27001:2013*. Retrieved October 9, 2018, from Qualtrics, LLC Certificate of Registration, Information Security Management System - ISO/IEC 27001:2013: <https://cert.schellmanco.com/?action=download-certificate>
- Seattle Times EMS Staff. (2018, December 21). *Seattle EMTs suspend strike after AMR agrees to continue bargaining*. Retrieved January 6, 2019, from Seattle Times: <https://www.ems1.com/american-medical-response/articles/393107048-Seattle-EMTs-suspend-strike-after-AMR-agrees-to-continue-bargaining/>
- Seidenberger, S. (2016). *A new role for human resource managers: Social engineering defense*. Cornell HR Review.
- Setera, K. (2020, March 30). *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*. (U.S. FBI, Editor, & U.S. FBI, Producer) Retrieved July 14, 2020, from FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic: <https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic>
- Shaw, C. R., & McKay, H. D. (1942). *Jevenile delinquency in urban areas*. Chicago : University of Chicago Press.

- Shaw, C. R., & McKay, H. D. (1942). *Juvenile Delinquency and Urban Areas*. Chicago: University of Chicago Press.
- Siponen, M. (2001). On the role of human morality in information systems security. *Information Resource Management Journal*, 14(4), 15-23.
- Siponen, M., Mahmood, A. M., & Pahlila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information Management*, 51(2), 217-724.
- Smith, M. B. (1947). The personal setting of public opinions: A study of attitudes toward Russia. *Public Opinion Quarterly*, 11, 507-523.
- Stajkovic, F., & Luthans, B. (1998). Social cognitive theory and self-efficacy: Going beyond the traditional motivational and behavioral approaches. *Organizational Science*, 28(4), 62-74.
- Suhwan, J., Kim, Y.-G., & Joon, K. (2011). An integrative model for knowledge share in communities-of-practice. *Journal of Knowledge Management*, 15(2), 251-269.
- Sulleyman, A. (2017). National Health Service (NHS) cyber attack: Why stolen medical information is so much more valuable than financial data. *The Independent*.
- Tamijidyamcholo, A., Bin Baba, M. S., Shuib Nor, L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computer Science*, 43(0), 42-57.
- Technology, N. I. (2019, May 5). *Glossary*. Retrieved May 5, 2019, from Computer Security Resource Center (CSRC): <https://csrc.nist.gov/glossary/term/intranet#>
- The Office of the National Coordinator for Health Information Technology. (2015). *Guide to Privacy and Security of Electronic Health Information*. Retrieved January 1, 2018, from Guide to Privacy and Security of Electronic Health Information: <https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>

Thomson, M. E., & von Soms, R. (1998). research results supported the hypothesis that

Commitment had a positive impact on attitude towards ISSP compliance. *Information Management & Computer Security*, 6(4), 167-173.

U.S. Department of Health and Human Services (HHS). (2013, July 26). *Summary of HIPAA Privacy Rule*. Retrieved June 16, 2019, from Summary of HIPAA Privacy Rule:

<https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>

U.S. Cybersecurity & Infrastructure Security Agency. (2020, March 24). *Critical Infrastructure Sectors*. Retrieved July 14, 2020, from Critical Infrastructure Sectors:

<https://www.cisa.gov/chemical-sector>

U.S. Department of Commerce. (2008, July 25). *National Institute of Standards and Technology*. (U. D. Commerce, Producer) Retrieved June 15, 2019, from Guide to Server Security:

<https://csrc.nist.gov/publications/detail/sp/800-123/final>

U.S. Department of Commerce. (201, May 25). *National Institute of Standards and Technology, Computer Security Resource Center*. doi:2006

U.S. Department of Commerce. (2011). *Managing Information Security Risk, Organization, Mission, and Information System View*. U.S. Department of Commerce. Gaithersburg: National Institute of Standards and Technology (NIST) Special Publication 800-39.

U.S. Department of Commerce. (2016). *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworth Secure Systems*.

Gaithersburg: Computer Security Division, National Institute of Standards and Technology.

U.S. Department of Commerce. (2019). *U.S. National Institute of Standards and Technology Computer Resource Center*. Retrieved June 16, 2019, from Computer Resource Center

Glossary: <https://csrc.nist.gov/glossary/term/threat>

- U.S. Department of Commerce. (December 2018). *Risk Management Framework for Information Systems and Organizations, Revision 2*. National Institute of Standards and Technology (NIST). Gaithersburg: U.S. Department of Commerce. Retrieved from <https://doi.org/10.6028/NIST.SP.800-37r2>
- U.S. Department of Health & Human Services. (2001, July 7). *Standards for Privacy of Individually Identifiable Health Information*. Retrieved January 1, 2020, from Standards for Privacy of Individually Identifiable Health Information: <https://aspe.hhs.gov/standards-privacy-individually-identifiable-health-information>
- U.S. Department of Health & Human Services. (2018, June 18). *HHS.Gov*. Retrieved September 16, 2018, from Judge rules in favor of OCR and requires a Texas cancer center to pay \$4.3 million in penalties for HIPAA violations: <https://www.hhs.gov/about/news/2018/06/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-violations.html>
- U.S. Department of Health and Human Services . (2018, November 26). *National Health Expenditure Accounts Methodology Paper, 2017*. (U. Government, Producer) doi:November 26, 2018
- U.S. Department of Health and Human Services (HHS). (2017). *National Health Expenditure Accounts Methodology Paper*. U.S. Department of Health and Human Services (HHS), HHS. Washington D.C.: U.S. Department of Health and Human Services (HHS). doi:11-26-2018
- U.S. Department of Health and Human Services (HHS). (2017, May 12). *The HIPAA Security Rule*. Retrieved June 16, 2019, from The Security Rule: <https://www.hhs.gov/hipaa/for-professionals/security/index.html>

U.S. Department of Health and Human Services. (2013, July 26). *Breach Notification Rule*.

Retrieved June 16, 2019, from Breach Notification Rule: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

U.S. Department of Health and Human Services. (2017, June 16). *HIPPA for Professionals*.

Retrieved June 16, 2019, from Health Information Privacy:
<https://www.hhs.gov/hipaa/for-professionals/index.html>

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency.

(2020, March 24). *Critical Infrastructure Sectors*. Retrieved August 11, 2020, from
Critical Infrastructure Sectors: <https://www.dhs.gov/cisa/critical-infrastructure-sectors>

Uffen, J., & Breitner, M. H. (2013). Management of technical security measures: an empirical examination of personality traits and behavioral intentions. *43rd Hawaii International Conference on System Sciences*.

University of Washington Policy Directory. (2013, Oct 28). *Administrative Policy Statement 2.6*,

Information Security Controls and Operational Practices. Retrieved May 16, 2020, from
Administrative Policy Statement 2.6, Information Security Controls and Operational
Practices: <https://www.washington.edu/admin/rules/policies/APS/02.06.html>

UW Medicine. (2016). *UW Medicine Mission & Vision: Values, goals, and strategies to improve*

the health of the public. Retrieved May 10, 2020, from UW Medicine Mission & Vision:
Values, goals, and strategies to improve the health of the public:

<https://www.uwmedicine.org/about/the-uwmedicine-family/mission-vision>

UW Medicine. (2020). *Data Stewardship Training & PCISA*. Retrieved July 12, 2020, from Data

Stewardship Training & PCISA: <https://www.uwmedicine.org/school-of-medicine/policies-procedures-reporting/data-stewardship>

UW Medicine Compliance. (2019). *UW Medicine Compliance*. Retrieved November 30, 2019, from The Role of UW Medicine Compliance:

<http://depts.washington.edu/comply/program-overview/>

UW Medicine Compliance. (2019). *UW Medicine Compliance Information Security (COMP.107)*. Retrieved November 30, 2019, from UW Medicine Compliance

Information Security (COMP.107): http://depts.washington.edu/comply/comp_107/

UW Medicine Compliance. (2020). *UW Medicine Compliance*. Retrieved February 29, 2020, from UW Medicine Compliance: <http://depts.washington.edu/comply/>

UW Medicine Compliance Program Policies. (2019). *UW Medicine Compliance Program Policies*. Retrieved November 30, 2019, from UW Medicine Compliance Program Policies: http://depts.washington.edu/comply/compliance_program/

UW Medicine Compliance, HIPAA Privacy and Security Resources. (2020). *UW Medicine Compliance*. Retrieved February 29, 2020, from UW Medicine Compliance, HIPAA Privacy and Security Resources: <http://depts.washington.edu/comply/hipaa-privacy-and-security-resources/>

UW Medicine Information Security Standards. (2019). *UW Medicine Information Security Standards*. Retrieved November 30, 2019, from UW Medicine Approved Standards: <https://depts.washington.edu/uwmedsec/restricted/standards/>

Vanderbilt University. (2019, March 11). *REDCap*. Retrieved March 11, 2019, from About REDCap, Vanderbilt University: <https://projectredcap.org/about/>

Verizon. (2018, April 11). 2018 Data Breach Investigation Report, Executive Summary. *2018 Data Breach Investigation Reportm Executive Summary, 11*. Verizon. Retrieved December 25, 2018, from

file:///C:/Users/carla/Documents/Seattle%20University/Thesis/Verizon%20Data%20Breaches%20Report/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Washington State Legislature. (2020, March). *Personal information—Notice of security breaches*. Retrieved March 6, 2020, from Personal information—Notice of security breaches: <https://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.590>

Witherspoon, C., Bergner, J., Cockrell, C., & Stone, D. (2013). Antecedents of organizational knowledge sharing: a meta-analysis and critique. *Journal of Knowledge Management*, 17(2), 250-277.

Woon, I. M., & Kankanhalli, A. (2007). Investigation of IS professionals' intentions to practice secure development of applications. *International Journal of Man-Machine Studies*, 65(1), 29-41.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24, 2799-2816.

Wu, R., Tran, K., Lo, V., O'Leary, K., Morra, D., Quan, S., & et al. (2012). Effects of clinical communication interventions in hospitals: A Systematic review of information and communication technology adoptions for improved communications between clinicians. *International Journal of Informatics*, 81(11), 723-732.

Yuan, E. (2020, April 1). *A Message to Our Users*. Retrieved July 12, 2020, from Zoom Blog: A Message to Our Users: <https://blog.zoom.us/a-message-to-our-users/>

Zweig, D., & Webster, J. (2003). Personality as a moderator of monitoring acceptance. *Computers and Human Behavior*, 479-493.

Zweig, D., & Webster, J. (2003). Personality as a moderator of monitoring acceptance. *Computer and Human Behavior*, 497-493.

Appendix A

Original Safa et al., (2015) and UW Medicine Survey Items Statements (Modified)

Human Behavior Categories	No.	Original Survey Item Statements	Modified Survey Item Statements
Information Security Awareness (ISA)	1	I am aware of potential security threats.	UW Medicine promotes information security awareness
	2	I have sufficient knowledge about the cost of information security breaches.	Information security awareness helps me to understand that a risk may lead or contribute to an incident, which could cause the loss or compromise of Confidential information.
	3	I understand the risk of information security incidents.	UW Medicine promotes information security awareness.
	4	I keep myself updated in terms of information security awareness.	Information security awareness improves my information security compliance behavior
	5	I share information security knowledge to increase my awareness.	Sharing knowledge improves my information security compliance behavior.
Information Security Organization Policy (ISOP)	1	Information security policies and procedures are important in my organization.	Organizational compliance policies and information security standards are important to me.
	2	Information security policies and procedures affect by behavior.	Compliance policies and information security standards affect my behavior towards compliance.
	3	Information security policies and procedures have attracted my attention.	Compliance policies and information security standards attract my attention.
	4	Behavior in line with organizational policies and procedures is of value in my organization.	Compliance policies and information security standards teach me how to apply best practices.

Information Security Experience and Involvement (ISEI)	1	My experience increases my ability to have safe behavior in terms of information security.	My experience ensures my behavior complies with policies and information security best practices.
	2	I am involved with information security and I care about my behavior in my job.	My experience helps me to care about protecting UW Medicine Confidential information.
	3	My experience helps me to recognize and assess information security threats.	My experience helps me to recognize and information security threat.
	4	I can sense the level of information security threat due to my experience in this domain.	Due to my information security-compliance experience, knowledge sharing with co-workers benefits UW Medicine.
	5	My experience helps me to perform information security conscious care behavior.	Intentionally left blank
	6	I have suitable capability in order to manage information security risk due to my experience.	Intentionally left blank
Attitude (ATT)	1	Information security conscious care behavior is necessary.	My attitude towards information security compliance is positive.
	2	Information security conscious care behavior is beneficial.	My attitude about information security compliance is beneficial to UW Medicine.
	3	Practicing information security conscious care behavior is useful.	My attitude towards information security compliance affects my behavior.
	4	I have a positive view about changing users' information security behavior to conscious care.	My attitude towards information security compliance may influence others to comply their behavior.
	5	I believe that information security conscious care behavior is valuable in an organization.	My attitude towards information security compliance is valued by UW Medicine.
Subjective Norms (SN)	1	Information security policies in my organization are important for my colleagues.	It is important to role-model information security compliance behavior for co-workers.
	2	My colleagues' information security behavior influences my behavior.	My coworkers' information security compliance behavior influences my behavior.
	3	Information security culture in my organization influences my behavior.	An information security culture influences my behavior.
	4	My boss's information security behavior influences my behavior.	When leader's role model information security compliance behavior, it affects my information security compliance behavior.

Information Security Self-Efficacy (ISSE)	1	I have the skills to protect my business and private data.	I possess the training and skills to safeguard Confidential information.
	2	I have the expertise to protect my business and private data.	I am confident about safeguarding Confidential information.
	3	I think the protection of my data is in my control in terms of information security violations.	Protecting Confidential information is within my control.
	4	I have the ability to prevent information security violations.	I have the ability to prevent information security violations.
Information Security Conscious Care Behavior (ISCCB)	1	I consider information security experts recommendation in my information security manner.	I think about how my information security behavior can reduce organizational risk.
	2	Before taking any action that affects information security, I think about its consequences.	I can contact compliance or information security experts before I make a decision.
	3	I talk with security experts before I do something that relates to information security.	I consider recommendations made by compliance and information security subject matter experts.
	4	I consider my previous experience in information security to avoid repeating prior mistakes.	My information security compliance behavior helps me to avoid making mistakes.
	5	I always try to change my habits in information security behavior.	Intentionally left blank.

Appendix B

UWM REDCap Survey Statements

Theoretical Category	Survey Statements	Strongly Agree	Agree	Disagree	Strongly Disagree
Information Security Awareness (ISA)	1 UW Medicine promotes information security awareness.				
	2 Information security awareness helps me to understand that a risk may lead or contribute to an incident, which could cause the loss or compromise of Confidential information.				
	3 UW Medicine promotes information security awareness.				
	4 Information security awareness improves my information security compliance behavior				
	5 Sharing knowledge improves my information security compliance behavior.				
Accessibility-Compliance Policies and Information Security Standards (CPISS)	1 Organizational compliance policies and information security standards are important to me.				
	2 Compliance policies and information security standards affect my behavior towards compliance.				
	3 Compliance policies and information security standards attract my attention.				
	4 Compliance policies and information security standards teach me how to apply best practices.				
Information Security Experience and Involvement (ISEI)	1 My experience ensures my behavior complies with policies and information security best practices.				
	2 My experience helps me to care about protecting UW Medicine Confidential information.				
	3 My experience helps me to recognize an information security threat.				
	4 Due to my information security-compliance experience, knowledge sharing with co-workers. benefits UW Medicine.				
	5 My experience ensures my behavior complies with policies and information security best practices.				

Theoretical Category	Survey Statements	Strongly Agree	Agree	Disagree	Strongly Disagree
Attitude (ATT)	1 My attitude towards information security compliance is positive.				
	2 My attitude about information security compliance is beneficial to UW Medicine.				
	3 My attitude towards information security compliance affects my behavior.				
	4 My attitude towards information security compliance may influence others to comply their behavior.				
	5 My attitude towards information security compliance is valued by UW Medicine.				
Subjective Norms (SN)	1 It is important to role-model information security compliance behavior for co-workers.				
	2 My coworkers' information security compliance behavior influences my behavior.				
	3 An information security culture influences my behavior.				
	4 When leader's role model information security compliance behavior, it affects my information security compliance behavior.				
Information Security Self-Efficacy (ISSE)	1 I possess the training and skills to safeguard Confidential information.				
	2 I am confident about safeguarding Confidential information.				
	3 Protecting Confidential information is within my control.				
	4 I have the ability to prevent information security violations.				
Information Security Conscious Care Behavior (ISCCB)	1 I think about how my information security behavior can reduce organizational risk.				
	2 I can contact compliance or information security experts before I make a decision.				
	3 I consider recommendations made by compliance and information security subject matter experts.				
	4 My information security compliance behavior helps me to avoid making mistakes.				

Appendix C*HIPAA Protected Health Information Identifiers*

1. Names
2. Address (other than a town or city, state, and zip code)
3. Telephone numbers
4. All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
5. Fax numbers
6. Electronic mail (email) addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images, any other unique identifying number, characteristic, or a code
18. Any characteristic that could identify an individual

Appendix D*U.S. Cybersecurity & Infrastructure Security Agency*

1. Chemical Sector
2. Commercial Facilities Sector
3. Communication Sector
4. Critical Manufacture Sector
5. Dams Sector
6. Defense Industrial Base Sector
7. Emergency Services Sector
8. Energy Sector
9. Financial Services Sector
10. Food and Agriculture Sector
11. Government Facilities Sector
12. Healthcare and Public Health Sector
13. Information Technology Sector
14. Nuclear Reactors, Materials, and Waste Sector
15. Sector-Specifics Agencies
16. Transportation Systems Sector
17. Water and Wastewater Systems Sector