Behavioural Information Security Practices of Healthcare Professionals: A Five-Year Systematic Literature Review.

by

Olivia Uhrle

A dissertation submitted to Auckland University of Technology in partial fulfilment of the requirements for the degree of Master of Business (MBus)

2024

Business Information Systems,
Faculty of Business, Economics and Law

ABSTRACT

Information security is critical to fortifying organisations in a technologically evolving world where cyber criminals, threats and challenges remain prominent, particularly for healthcare organisations. The healthcare industry has been known as a patient-centric sector focusing and investing in increasing patient care, services, and medical devices to ensure services operate efficiently and effectively; however, health organisations still need to be equipped and remain under-trained against cyber threats and attacks. This study focused on the behavioural interactions of health professionals through a systematic literature review between 2017 and 2023. The study found seventeen behavioural interactions, including but not limited to shared workstations, shared passwords and credential log-in, utilising shared USB sticks and sticky notes to record patient information. The behavioural interactions were sorted against a factor, which included information security knowledge and awareness, workload management, information security culture, access and authentication, and data backup and encryption. The behavioural interactions against the factors were found to have implications on the overall cybersecurity dimensions of people, processes, and technology. The study recommended using the CIS benchmark, and HIPAA controls to address the identified behaviours, in addition to a proposed information security knowledge and awareness implementation framework that highlights the training contents that could be used to address the behavioural interactions of health professionals.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ATTESTATION OF AUTHORSHIP

"I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor used artificial intelligence tools or generative artificial intelligence tools (unless it is clearly stated, and referenced, along with the purpose of use), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning."

Signature: [Jennifer Olivia Uhrle]

Date: 19/03/2024

ACKNOWLEDGEMENTS

I thank my Heavenly Father for this journey. Without Him, nothing would be possible. To those who were here before me, my ancestors including my Ma, Kaiva and Pa, William Uhrle. I have carried our last name in the hopes I have carried it well. May you rest in eternal love.

Firstly, to an incredibly patient and caring supervisor, who not only remained flexible with his schedule but made the time of day (or night) to dedicate his wisdom, advice, and efforts to pushing this study over the line. Despite my many hurdles, you maintained a potent force for me to keep going. Thank you, Dr. Ranjan Vidya. It has been an honour to have been taught by you.

To my soul sister, who shared "study" dates, tears, but most importantly, academic, career and life goals with me, you have made every journey, memorable and so much fun. Life is so much more beautiful with you in it. I cannot thank you enough. Ofa atu, Ilaisaane Falevai.

To my support system, I write this with my heart so full. 4.5 years of full-time undergrad and postgrad study while working full-time simultaneously meant that a lot of doubts and opinions were thrown my way, but you guys believed in me when no one else did. The encouragement has given me so much courage. Thank you, Christine and Jamil, Ursula, Danielle and Eddie, Myra and Ethan, Herman, and aunties' little angels – Aaleya, Naz and Aminah.

To my dearest mama, Sigalu Cordtz-Unasa. Fa'afetai mo le tatalo mo a'u. E le mafai ona ou faia lenei mea without you. Fa'afetai mo lou alofa ma lou agalelei. Ou te tatalo ina ia tele nisi aso tou te fa'atasi ma a'u so we can travel together. Alofa tele atu mo oe.

> *Translation for Samoan only – ("Thank you for praying for me. I could not have done this without you. Thank you for your love and goodness. I pray you have many more days with me").*

Now to my dearest fiancé. The man who stood by me and wiped my tears, held my hand, and loved me through it all. You are the epitome of patience. You made everything that seemed impossible, possible. You give me something I struggle to find in life's trials, that is hope. Thank you for your devotion, love, and efforts into making my life easier and so much more beautiful. Thank you, Tyler Oversluizen. I would love to acknowledge my mother and grandmother-in-law – Leeanne and Apaira Nicholas. Meitaki maata for opening your home and hearts to me.

Most importantly, to the very people who inspired me. My parents, Virgil and Aiga Uhrle. Fa'afetai mo mea uma. I am so proud to be your daughter. I am honoured to be the product of hardworking, loving, and giving people. Ua ou fa'alogo i tatalo na faia mo a'u ma ou te tatalo ina ia ou fa'ataunu'uina. Aua lava nei galo lo'u alofa tele ia te o lua uma. May all the sacrifices you have made for the aiga, never go in vain. I have and always will do everything for you both.

> *Translation for Samoan only –* ("*Thank you. For everything. I have listened to your prayers made for me, and I pray I have fulfilled them. Never forget how much I love you two").*

And finally, to Unasa Leo Unasa. The man who made me promise him, three months before he passed, that I would strive to do better in school for the family and take my education as far as possible. No matter the bag or event, I carry your funeral badge to remind me of our promise when I was 13. Papa, I hope I have now fulfilled this promise to you. I hope you are smiling down from the heavens, knowing I gave it my all. Eleven years later, we finally made it to Masters. However, now, it is time for me to take an academic break.

DEDICATION

I dedicate this research to my dearest tama, Virgil Uhrle. Who unknowingly paved my career pathway in primary school and ultimately inspired my first research focusing on healthcare. Thank you for everything.

1 INTRODUCTION

In the dynamic surge of an unceasingly transforming world and decades of relentless technological innovation across all industries, Information Technology (IT)[1] and Information Systems (IS[2]) have facilitated the foundation of seamless communication, broader but deeper connectivity and networking amongst organisations and customers (Coventry et al., 2018). The healthcare industry, in particular, has ushered transformative technological benefits such as enhancing patient care, streamlining administrative processes, and nurturing technical contributions to help improve and develop healthcare outcomes (Coventry et al., 2018). There are several data storage systems used by healthcare professionals, such as Electronic Health Records (EHR), Electronic Medical Records (EMR), and Personal Health Records (PHR), which provide repositories of patient data in the overall Health Information System (HIS).

The rapid growth of HIS has made the security of patients' Personally Identifiable Information (PII) and Patient Health Information (PHI) secure, thus creating privacy security protection frameworks within the healthcare industry. However, despite the advances, the overall structure of the healthcare industry has made it extremely difficult to implement suitable and proper security measures effectively (Wager et al., 2009). While it is essential to understand the technical aspect of information security[3] or cybersecurity[4], past studies have indicated that it is critical to understand the behavioural aspect of overall employee behaviour when interacting with information security measures. This is due to the notation that humans are regarded as a "major threat to an organisation's security system" (Chen et al., 2012). Safeguarding patient privacy and maintaining security over HIS necessitated understanding how health professionals interact with information security practices. Recognising and addressing the biggest threat to an organisation's security system, the human element, is fundamental to ensuring healthcare data's Confidentiality, Integrity, and Availability (CIA)[5]. Examples of information security best practices include reporting malicious emails or content, locking devices when left unattended, password management, ensuring no sensitive information is left visible on a solitary desk, and updating device systems to install the latest patching.

Past research has reviewed the behavioural connection to information security interactions by touching on the importance of motivation, education, social and cultural influence, management support, and information security awareness (Lebek et al., 2014; Sonmez et al., 2022; Moustafa et al., 2021; Ifinedo, 2012; Kadena & Gupi, 2021). Similarly, Ifinedo (2012) concluded that self-efficacy, attitude, subjective norms, response efficacy, and perceived vulnerability positively contributed to an individual's information security behaviour. In addition, a further study conducted a decade later by Yeng et al. (2021) through the systemic mapping analysis of healthcare IS professionals proved that individual characteristics such as psychological, social, and cultural traits contributed to information security compliance behaviour. Structural factors also contribute to the information security behaviour of healthcare professionals. For example, concerns about privacy and information security relating to patient information had Keshta et al. (2021) conclude that several factors, specifically funding of technology, cultural norms, and attitude towards information security, hinder proper protection of EHR and increase vulnerability to cyber-attacks. Bada et al. (2019) discussed how cultural differences could impact the effectiveness of information security awareness campaigns. To understand the working

[1] Interconnected equipment used in the automatic acquisition, storage, manipulation, management, interchange, transmission, or reception of data or information (Johnson et al., 2011).

[2] Systems, people, and processes utilised for creating, storing, manipulating, and distributing information (Brien & Marakas, 2006).

[3] Protecting an organisation's information from unauthorised access, disclosure, and modification (IBM, 2023b).

[4] Information security and cybersecurity are often used interchangeably. This will be reflected throughout this study to ensure thorough context.

[5] The CIA triad is a 'benchmark' model for information security. Its purpose is to govern organisations in handling sensitive data, whether it is stored, transmitted, or processed. (CIS, n.d).

effects of HIS security policy compliance behaviour, Humaidi et al. (2015) found that healthcare professionals who are highly experienced and more aware of HIS are more likely to have positive behaviour towards complying with information security policies (ISP)[6], whereas, in previous research conducted by Humaidi et al. (2014) again, they examined information security awareness factors that impacted compliance behaviour through the use of a Health Belief Model (HBM)[7]. Furthermore, Koloseni et al. (2019) expanded Humaidi et al. (2014) use of the HBM and conducted a study surrounding habitual or automatic security behaviours and conscious security behaviour toward information security practices. Yasin et al. (2019) believed that organisations should use game-based learning to equip employees better for handling cyberattacks. Similarly, Dong et al. (2021) conducted a social bonding experiment involving 241 nurses to understand information security awareness and comply with information security practices.

While we understand that human error is a substantial contributing factor to a failure in cybersecurity practices, it is essential to understand what is currently being done by healthcare professionals when interacting with cybersecurity measures and how we can close the learning gap to comply better with ISPs and increase information security practices. Due to the working culture of healthcare organisations, they are vulnerable to many challenges, as can be found in **Table 1**.

Table 1 - Information Security Challenges vs Best Practices

Challenge	Best Practice
Struggling to prevent unsafe user behaviour.	Information security training and education – this can be done through regular phishing simulation and refreshment activities.
	Outline the importance of information security policy compliance and practices.
Ineffective employee engagement and alignment methods.	Reward and recognition for good information security behaviour.
	Precise specification of information security policies and practices.
	Regular refreshment security activities.
	Align security training and awareness with organisational norms, culture, and practices.
	Provide training in an interactive measure, such as a classroom session.
Enlisting and providing support for the detection of cyber incidents.	Provide a convenient measure for users to report suspicious activity.
Identifying and responding to information security incidents.	Ensure that the Business Continuity Plan(s) and Disaster Recovery Plan(s) are concise and practised.
	Organisations should develop checklist(s) for routine incidents, ensuring all employees are assigned to a specific team and understand their roles and responsibilities during an incident.
Access and authentication management.	Password management – ensuring passwords are not displayed or disclosed in an insecure environment or to unauthorised users.

[6] Examples of information security policies can include a 'Clean Desk Policy' ensuring that no sensitive information is visible on desks. Another example is an 'Access Control Policy', which ensures only authorised individuals have access to specific systems and applications, and a 'Password Management Policy' ensures that individuals apply complexity (upper case, lower case, numbers, and symbols) controls to password creations whilst also ensuring that passwords are not reused and changed after a specific time frame (e.g., 90 days). Policies vary on company size and needs.

[7] One of the first models that adapted theory from behavioural sciences to health issues. It attempts to predict health-related behaviour in terms of specific belief patterns (Hochbaum et al.,1952).

	Lock devices when left unattended.
	Implementing multi-factor authentication across all devices.
	Ensure a secure password manager application is used to store sensitive access information.

Note. Table adapted from McLaughlin & Gogan (2018) Challenges and Best Practices in Information Security Management. MIS Quarterly Executive.

1.1 PURPOSE OF THE RESEARCH

Various factors shape the information security behaviour of healthcare professionals. Psychological, organisational, social, and structural factors have been known to contribute to information security behaviour (Yeng et al., 2021). This study focuses on the human element of information security. It aims to explore the relationship between behavioural interactions of health professionals while practising information security. In addition, it relies on past research to understand why specific information security interactions, such as password sharing, are commonly used among health practitioners.

Various studies have sought to understand health professionals' behavioural interactions by understanding their compliance behaviours towards set ISPs. Extant literature has relied on multiple theories to explain information security compliance behaviour. Some of the widely used theories include – The Theory of Planned Behaviour (TPB), the Technology Acceptance Model (TAM), the Protection Motivation Theory (PMT), and the Social Cognitive Theory (SCT). Past research has widely used the theories of TPB, TAM, PMT and SCT to understand behavioural intention towards information security compliance (Ajzen, 1991; Al-Omari et al.,2012; Anderson & Arharwal, 2010; Ifinedo, 2012; Widianto et al., 2021; Chen et al., 2012). The theory of TPB highlights the individual attitudes, subjective norms, and perceived behavioural control that can impact an individual's or the organisation's security culture (Ajzen, 1991). The TAM model proposes technology's perceived ease of use and usefulness (Davis, 1989). PMT considers fear appeals and uses self-efficacy (SE), response efficacy (RE), and past behaviour factors that may have influenced security behaviour. In addition, PMT considers an individual's perceived probability of a threat or event occurrence and the impact of a recommended action (Yeng et al., 2022a). Lastly, SCT highlights that personal, behavioural, and environmental influences influence an individual's belief to control actions or events (Bandura, 1986).

Ifinedo (2012) explored ISP compliance by drawing on general theories such as TPB and PMT to analyse data collected through the survey given to 124 business managers and information systems professionals. In comparison, Lebek et al. (2014) conducted a literature review comprising 113 publications. They identified 54 theories primarily using the following theories: TPB, TAM, PMT, SCT, and TAM and argued that there are specific difficulties in observing compliance behaviour; however, it was evident that TPB strongly influenced behavioural intention and recommended that models and campaigns should be more developed to increase security awareness. Siponen (2000) discussed employees' information security awareness due to behavioural impact within the last decade and found that TPB and TAM influence information security compliance behavioural intention and Chen et al. (2006) found that reward and punishment influence information security compliance in organisations through a survey involving over 500 IS professionals in medical institutions.

Reliance on particular theories is a characteristic of the information security literature on healthcare. This research proposes an information security and awareness framework to help health leaders better prepare themselves to increase their knowledge and awareness to ensure a robust information security culture (ISC)[8]. The research question that it seeks to answer is:

[8] Set of values shared within an organisation, which consists of the manner in which employees perceive and interact (behave) with the security controls implemented (Veiga et al., 2020).

"How do healthcare professionals behave while interacting with information security practices?".

The study applies a Systematic Literature Review (SLR) method (Okolio et al., 2010) to answer the research question and develop the security awareness framework to help health leadership take a more practical approach to organise and improve their ISC. In addition, the SLR is a crucial factor in enhancing the depth and broadness of the study, which will provide a robust outcome and control recommendation to improve healthcare information security further.

1.2 SIGNIFICANCE OF THE RESEARCH

This qualitative SLR-based study is significant for conceptualising and designing organisational ISPs and frameworks. In its practicality, the research seeks to provide healthcare executives and researchers with a framework to ensure that information security practices are designed to match the behavioural patterns of healthcare professionals through increasing information security knowledge and awareness. This framework will help ensure compliance with information security standards and policies and raise awareness regarding the potential information security vulnerabilities of the healthcare industry. The study will also encourage healthcare executives to develop realistic procedures, policies, and practices to promote better information security practices by helping them understand the most common staff behavioural interactions with information security practices that could pose a risk to the overall ISC and compromise the protection of PHI and PII.

The remaining dissertation has been organised into five chapters following this introductory chapter. Chapter 2 provides an overview of health information security and discusses the threats and challenges posed to the healthcare industry. Chapter 3 describes the systematic literature review methodology, which consists of data analysis's inclusion and exclusion criteria. Chapter 4 expands the selected pieces of literature into themes and sub-themes. This is followed by Chapter 5, which will discuss the proposed recommendations and framework that can be utilised to address the identified behaviours. Finally, Chapter 6 discusses the findings and conclusions of the research, followed by the study's conclusion.

2 AN OVERVIEW: HEALTH INFORMATION SECURITY

2.1 CHAPTER OVERVIEW

Health information security is guided by several standards, regulations, laws, and procedures to ensure that PHI and PII are secure and protected. Chapter 2 will provide an overview of health information security, highlighting the common threats and challenges health professionals face. In addition, the chapter will discuss the Waikato District Health Board (WDHB) attack that occurred during the peak of COVID-19 in 2020 and the lessons learned.

2.2 HEALTH INFORMATION SECURITY – THE THREATS AND CHALLENGES

Information security is designed to fortify critical systems and information from cyber-attacks, whether they originate internally or externally (IBM, 2023a). Adequately managing information security is fundamental to optimising information security within organisations and is essential to protecting PHI and PII (Fischer, 2014). To ensure adequate management of information security, there are guidelines, standards, regulations, and documents which often provide a foundation for what needs to be done by an organisation to protect information. An ISP is an example of documentation commonly used by organisations to understand best practices. It is pivotal to an organisation as it guides the implementation of information security and sets out to help an organisation understand their responsibility to protect assets (Hone & Eloff, 2022). Regulations are another great way to help organisations set up an ISP. For example, the Health Insurance Portability and Accountability Act (HIPAA)[9] outlines the rules and regulations for healthcare professionals. Usually, ISPs, guided by the HIPAA, train health professionals with information security practices in a stressful environment (Hedstrom et al., 2011). However, research has demonstrated that personnel often do not comply with the ISPs, increasing organisations' vulnerabilities to information security threats (Vance et al., 2012).

Information security issues vary and are different for every organisation. The value of practising and understanding information security could ensure the proper protection of an organisation; however, many industries, particularly healthcare, do not see the value of information security and, as a result, have fallen victim to various attacks such as phishing. The healthcare industry has also proven unequipped to face cyber-attacks as attackers systematically exploit them (Kioskli et al., 2021). This is understandably due to the immense pressure to tend to the needs of patients first. Faster and more convenient approaches are often taken to ease workload and time pressure. Consequently, ISPs are often considered irrelevant and inconvenient to health professionals and challenging to comply with (D'Arcy & Teh, 2019). Employees are expected to know about information security and the threats imposed. This is because the expectations of having basic information security knowledge are often reflected in an employee's work and in dealing with and complying with ISPs (Box & Pottas, 2014). Compliance with ISPs is usually unconsciously disrupted due to a lack of security awareness (Alqahtani, 2017).

The use of HIS has introduced a variety of threats. HIS threats are no different from threats faced by other industries. They are divided into two sources, internal and external, and each source is caused by human and non-human factors (Box & Pottas, 2014). Natural disasters such as flooding and cyclones can impact the data centre infrastructures and expose them to security vulnerabilities—for example, the unprecedented humanitarian crisis, COVID-19, crippled human life and rapidly transformed business operations. The pandemic caused a significant threat to all walks of life, technological developments, and use, and combined all three threats – natural, human, and environmental. Within a month, beginning in March 2020, companies shifted to virtual connections, causing immense pressure on technology professionals to meet demands to fit the 'new norm' of remote working (Baz et al., 2020). The increased

[9] Developed in 1996, the act was established to ensure an individual's health information is securely stored and protected while allowing the flow of information needed to enhance healthcare services (Institute of Medicine, 2009).

digital traffic and footprints exposed numerous vulnerabilities in information systems (Baz et al., 2020), particularly in the healthcare and banking industries (Alawida et al., 2022).

Generically, an internal threat can occur because of the following factors (Box & Pottas, 2014):

- A lack of understanding and knowledge of information security;
- Forgetting to apply security procedures or policies in day-to-day tasks;
- Deliberate acts of negligence towards information security, such as leaving computers logged in for convenience;
- Weak organisational ISC due to lack of investment and security advocation; and
- Highly intensive workload.

Past studies have identified organisations' significant information security threats (Baker, 2023)[10]. **Table 2** lists the commonly known security threats.

Table 2 - Most Common Cyberattacks in 2023

Attack	Description
Identity-Based Attack	An attacker compromising a user's credentials.
Malware	A program or code used to harm a computer, network, or server.
Denial-of-Service (DoS)	An attack that is used to flood a network with false requests impacting business operations.
Phishing	This attack uses various forms of social communication such as Short-Message-Services (SMS), phone, social media, or social engineering techniques to lure a victim into sharing sensitive information that will blindly have the victim install viruses onto devices.
Spoofing	An attacker disguises themselves as a known or authorised user to steal sensitive information or install malware onto devices.
Code Injection Attacks	A malicious code is injected into a vulnerable device or network to change or disrupt its course of action.
Insider Threats	This relates to current and former personnel with direct access to the company network, sensitive data, and intellectual property (IP) to help carry out an attack.
Domain Name System (DNS) Tunnelling	An attack that leverages a DNS attack to bypass traditional security measures, data in transit, and code within a network.

Aotearoa recorded 350 incidents in 2021/2022[11]. Of the 350 incidents, 34% indicated links to suspected state-sponsored actors, 23% indicated links to suspected criminal or financially motivated activity, and the remaining 43% of incidents recorded had insufficient information to judge attribution (NCSC, 2022).

While recovering from the COVID pandemic in 2021, the WDHB[12] sent shockwaves nationwide after falling victim to a large-scale ransomware attack. The WDHB's initial response was to seek physical

[10] Microsoft's STRIDE threat model identifies six major categories of cyber threats namely Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Services, and Elevation of Privileges (Baldwin et al., 2022).
[11] Refer to the National Cybersecurity Centre – Cyber Threat Report, 2021/2022 via https://www.ncsc.govt.nz/assets/NCSC-Documents/2021-2022-Cyber-Threat-Report.pdf. *Accessed September 2023.*
[12] Refer to the InPhySec WDHB Incident Response Analysis, v0.5, 2 September 2022 via https://www.tewhatuora.govt.nz/assets/Publications/Proactive-releases/WDHB-Final-Report-2.0-redacted.pdf. *Accessed September 2023.*

measures to disconnect all connections to the Internet, including corporate IT systems, laptops, printers, phone lines, medical devices, and any additional cloud service connectivity to ensure protection and security from further compromises. However, this approach severely impacted healthcare services and facilities, including other external hospitals, District Health Boards (DHBs), and primary and community providers who shared services and clinical services. As a result of the attack and initial approach, patient surgeries were postponed, critical patients were urgently transferred to other hospitals within other DHBs, and over 4,000 PII were accessed and disclosed across the dark web and mainstream media (NZ Herald, 2021). InPhySec[13] performed an incident response analysis and provided the following recommendations for the WDHB (InPhySec, 2022):

1. "Architected for security", in which data encryption, implementing access controls, and identifying high-risk and critical assets should be considered to ensure that systems are usable at a "clinical level", reflecting urgency at the point of delivery.
2. Systems should be kept updated by installing the latest patches. This recommendation involves investing in people through IT skills training and providing clear frameworks.
3. Implementing active detective and response mechanisms, including logging, monitoring, responding, and planning. InPhySec recommended that this step be accompanied by "behavioural discipline".
4. Ensuring that cyber threat responses are tested through a simulation.

Te Whatu Ora[14] revised and accepted the above recommendations, launching the National Cyber Security Uplift Programme with $75 million in funding from the Cabinet to develop a unified health system by doing the following activities (Te Whatu Ora, 2022):

1. Building a national security operations team;
2. Plan a series of incident response simulation exercises, including phishing simulations to support personnel in identifying suspicious cyber activity;
3. Hiring additional security colleagues to join the uplift program; and
4. Implementing new security technologies to help shield legacy systems.

However, on the other side of the world, 4-days before the ransomware attack in Aotearoa, the Health Service Executive of Ireland[15] (HSE) suffered a similar ransomware attack on May 14, causing a blockade of data and systems, compromising encrypted files and documents (Asghar, 2021). As a result, systems were forced to shut down nationwide, impacting patient treatment, and healthcare professionals reverted to a paper system to keep up with records, and appointments dropped by 80% (McNamee, 2021). Similarly, 2-days after the Aotearoa WDHB attack, the US healthcare industry faced a similar ransomware attack where the Federal Bureau of Investigation (FBI) identified at least 16 successful ransomware attacks targeting the US healthcare[16], first responder networks, law enforcement agencies, emergency medical services, 911 dispatch centres, and municipalities (CISA, 2021).

[13] InPhySec Security, a Fujitsu company, provide many services, including managed security, consulting, and technical services.
[14] A centralised DHB system to monitor and lead the day-to-day running of the healthcare system for Aotearoa (Te Whatu Ora, 2022).
[15] Refer to the Lessons Learned from the HSE Cyberattack Report, 02/03/2022 via https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf (US Department of Health and Human Services, 2022b). *Accessed December 2023.*
[16] Refer to the FBI Flash – Cyber Division, 20/05/2021 via https://www.cisa.gov/sites/default/files/Conti%20Ransomware%20Heathcare%20networks.pdf for further details. (CISA, 2021). *Accessed December 2023.*

2.3 HIS AND HUMAN BEHAVIOUR

Given the increasing cybersecurity threats, HIS security has become a significant security consideration for health organisations. This research focuses on the behavioural aspects of health professionals through interactions with information security.

HIS is the integrated effort encompassing the storage, processing, reporting, and application of collected health data (Ngafeeson, 2015). The overarching objective of HIS is to support decision-making processes that impact individual and public outcomes. In addition, the World Health Organization ("WHO") outlined that the HIS helps identify needs and evidence-based decisions to distribute resources optimally (WHO, 2023). HIS can consist of three types of records, each referring to patient-specific and identifiable healthcare information for healthcare professionals to understand the records used (NAHIT, 2008). The records include IR, EMR, and PHR[17].

Humans, in this case, healthcare professionals, are characterised as the weakest link in cybersecurity for HIS (Russell et al., 2017). Considering behavioural intention when looking closely at health professionals' interactions is essential because it is a measurable component of understanding what practices need to be implemented for more secure practices and interactions. Cert NZ published a report regarding behavioural insights and proposed a model for behavioural change known as "COM-B", referring to the three main factors of "Capability, Opportunity and Motivation", which stated that behavioural intention with change behavioural outcomes of more secure information security practices. Given the rapid increase in malicious attacks, particularly during and post-COVID-19, information security controls and mechanisms are extremely critical yet challenging to implement due to the overwhelming conditions.

Global security standards such as the International Organisation for Standardisation (ISO), National Institute of Standards and Technology (NIST) and Control Objectives for Information Technologies (COBIT) provide all organisations (regardless of industry) with a set of guidelines, controls, and implementations on what, how, who and when to secure information and assets. The most common and highly referenced health standard is HIPAA, published in the United States. In Aotearoa, the Health Information Security Framework (HISF)[18] and Health Privacy Code (HPC)[19] are often used to guide our health organisations and can be assessed against global standards. Such standards are critical to guiding human behaviour when handling information and practising security. Health leadership is expected to align its organisation against a framework or standard to ensure it guides its staff correctly through the publication of an ISP. However, an ISP's information security controls can only work by providing healthcare professionals with knowledge of how to apply those security mechanisms. Health professionals serve as a critical gateway for external actors to access HIS; therefore, financial investment in training health professionals to become aware of their role in protecting HIS is important (Konieczny et al., 2015). Due to the lack of investment in information security training, healthcare professionals need help to comply, implement, and apply simple best practices into their daily routines, such as password protection, locking unattended computers/ devices, and not writing sensitive information on sticky notes or boards. The absence of training and awareness also feeds into the negative behaviour and attitude toward cybersecurity measures (Hu et al., 2006).

[17] The three types of records are based on the Health Insurance Portability and Accountability Act (HIPAA).
[18] The HISF is designed to support the health sector and practitioners in Aotearoa. Refer to the official Health New Zealand website https://www.tewhatuora.govt.nz/publications/health-information-security-framework/ for further details.
[19] The HPO outlines specific rules for health agencies in Aotearoa that are collected, used, held, and disclosed by health agencies. Refer to the official Privacy Commissioner website https://www.privacy.org.nz/privacy-act-2020/codes-of-practice/hipc2020/ for further details.

3 RESEARCH METHOD

3.1 CHAPTER OVERVIEW

To establish a well-defined research, the study adopted SLR to mitigate bias and draw insightful outcomes to the proposed framework. SLR will serve as the backbone of the research process and identify major themes. Chapter 3 will provide an understanding of SLR, followed by a description of the steps and the inclusion and exclusion criteria for selecting the research studies, and finally, discuss the thematic analysis used to determine themes relating to behavioural interactions.

3.2 UNDERSTANDING SLR

SLR provides an explicit, comprehensive, and reproducible "method for identifying, evaluating and synthesising the existing body of completed and recorded work produced by researchers, scholars, and practitioners" (Fink, 2005). Researchers have used SLR as a cornerstone in healthcare research to contribute and provide a comprehensive review of healthcare topics. SLR aims to help researchers expand knowledge surrounding a specific topic. Tandon et al. (2020) provided an SLR review of blockchain in healthcare to assist in explaining existing knowledge gaps and identifying avenues for future contributions. Similarly, Khanra et al. (2020) used SLR to review big data analytics (BDA)[20] in healthcare to recognise relevant studies using appropriate keywords referring to BDA and eventually present gaps and future research opportunities.

SLR is applied to review relevant literature to understand the breadth and depth of the existing body of work and identify what needs to be done next (Xiao & Watson, 2019). The planning and selection stages of an SLR are critical to identifying and evaluating the validity and quality of existing work against the criteria to identify weaknesses, inconsistencies, and contradictions and help develop a new way of working or expand the current knowledge of work. Okoli et al. (2010) defined a systematic literature review as an explicitly comprehensive and reproducible methodology for identifying, evaluating, and synthesising an existing body of completed and recorded research produced by researchers, scholars, and practitioners.

The SLR process for this research will be based on Okoli et al. (2010).

The procedural steps are presented below, including their respective chapters:

Table 3 - The SLR Process

Procedural Step	Procedural Description	Chapter
Planning	The planning step involves outlining the purpose of the research and practising notetaking for large amounts of literature to ensure thorough preparation of writing out a research paper.	Chapter 1 - Introduction Chapter 2 – An Overview: Health Information Security

[20] Methods, tools, and applications used to gather process and produce insights from varied, high-volume, and high-velocity data sets that originate from a variety of sources including the web, devices, and emails (Microsoft Azure, n.d).

Selection	The searching step involves the searching and practical screening of past literature. It presents specific selection criteria for searching the studies/literature that will be included in the research. This research will focus on healthcare professionals' behavioural information security practices in the last five years. In addition, past literature that does not contain details or data surrounding behaviours of healthcare professionals toward information security will also not be considered. To ensure that the literature selection criteria are relevant to the research, the example points of consideration include content, publication language, and publication date. This study's inclusion and exclusion criteria are described in a separate sub-section below.	Chapter 3 - Research
Extraction	The extraction step involves extracting the relevant knowledge by applying grounded theory, thematic analysis, action research, etc. This study uses the thematic analysis method to extract the themes and knowledge from the literature. Data extraction is a crucial phase of a systematic literature review process. This action should mean that practical screening and quality appraisal have been completed, leaving the researcher with a complete list of articles comprising the material for the final systematic review. During this stage, information from the studies will be systematically taken from each article to serve as the raw material for the execution stage.	Chapter 4 – Literature Review
Execution	This step involves the analysis of findings and writing the final review. Once the articles have been screened, selected, recorded, and scored, combining them is required to make a comprehensive sense of the large number of studies chosen. A discussion, organisation and comparison between studies will be conducted. Once this has been completed, writing a final review should be made accessible as all articles, data collected and contained, and information should be completed.	Chapter 6 – Discussion and Findings

Note. Table adapted from Okoli et al. (2010) A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts: Working Papers on Information Systems.*

An SLR holds several advantages for this research. SLR reduces the literature bias and removes irrelevant literature that will compromise the study's outcome. SLR will only consider specific literature reviews identified in steps two and three (Okoli et al., 2010). SLR can allow researchers to quickly analyse and convey vast information from previous literature reviews within my research field. Furthermore, due to the specific nature of the selection and extraction process of SLR, where comparisons and contract actions are taken to reduce bias, the reliability of the research conclusions will increase (Okoli et al., 2010).

3.3 INCLUSION AND EXCLUSION CRITERIA

Through the SLR method, the study applied inclusion/exclusion criteria in the filtering process to ensure that only the selected literature was utterly relevant to the research. The study followed a five-year systematic review from 2017 to 2023 to prove the chosen literature was relevant.

The following inclusion criteria were used to screen for relevant literature:

- Articles that report on information security practices or interactions in a healthcare setting.
- Articles that identify behavioural intention and compliance of healthcare professionals.
- Articles reflecting and providing insights into a cyberattack simulation, training, or similar awareness activities within a healthcare setting.
- Articles that report on managerial support for healthcare information security.
- Studies relevant to a healthcare professional's organisational and work environment when interacting with information security.
- Articles that thoroughly reviewed information security policy and its relation to information security practices within a healthcare setting.

The following exclusion criteria were used to screen irrelevant literature:

- Articles based on healthcare information security or behavioural interactions published before 2017.
- Articles that were not written or published in English.
- Studies that did not have applicability to the research question.
- Duplicate articles.
- Articles demonstrating patient safety and patient impact from the use of medical devices.
- Articles not set in healthcare (though discussing information security behaviour).
- Articles that spoke of information security but not of information security practices in healthcare.
- Articles that were inaccessible to review.

The following table reflects the total quantity of the type of publications used for the study:

Table 4 - Publication Types

Type of Publications	Total Collected:
Journal Article	22
Conference Proceedings	7
Case Study	4
Systematic Review	4
Research Article	3
Review	3
Original Research Article	1
Proceeding Paper	1
Total	45

The following terms were searched to encapsulate the finalised relevant pieces of literature to the study:

Table 5 - Search Terms

Search Terms:	Total Collected:
Healthcare + Technology Adoption Challenges	6
Healthcare + Workload + Behavioural Intention + Information Security	6
Healthcare + Information Security Practices	5
Healthcare + Information Security Behaviour	4
Healthcare + Information Security Challenges	4
Healthcare + Information Security Behaviour + HER	3
Healthcare Behaviour + Cybersecurity	3
Healthcare Behaviour + Information Security Awareness	3
Healthcare Behaviour + Information Security Culture	3
Healthcare + Information Security Policy Compliance	2
Healthcare Behaviour + Applications and BYOD Usage	2
Healthcare Behaviour + Information Security + HIS	2
Healthcare Leaders + Information Security	2
Total	45

The study selected 56 publications for review from 2017-2023. All literature was related to behavioural intention and how healthcare professionals interact with information security. However, 11 publications were removed from the 56, as 4 were not published in English despite being accessible, and the remaining seven were inaccessible for review.

The study finalised and reviewed 45 publications. A final collection of literature reviewed can be found in **Appendix A**.

3.4 INFORMATION SOURCES

The search criteria were applied to SpringerLink, Google Scholar, IEEE Explore, ScienceDirect, Business Source Complete (EBSCO), Emerald Insights, JMIR, IGI Global Database, JSTOR and Scopus. However, the following databases covered the most comprehensive body of research on healthcare information security practices but not limited to leadership engagement, security advocacy, and information security compliance behaviour in a healthcare setting:

Table 6 - Database Collection Total

Database:	Total Collected:
ScienceDirect	8
SpringerLink	7
MDPI	6
JMIR Publications	5
National Library of Medicine	3
Sage Journals	3
Association for Computing Machinery (ACM)	2
Google Books	2
ResearchGate	2
Association for the Advancement of Medical Instrumentation (AAMI)	1
British Medical Journal Publications	1
Emerald Insight	1
IGI Global	1
IOS Press	1
LJMU Research Online	1
The Lancet	1
Total	45

ScienceDirect, SpringerLink, and MDPI captured the most articles on behavioural intention, information security compliance, and healthcare information security.

The above databases were preferred over other options (such as IEEE Xplore, EBSCO, Scopus, Google Books, and Wiley Online Library), as the articles had little access. The search period covered articles and conference proceedings from January 2017 to December 2023 to ensure this only captures the most recent research.

3.5 THEMATIC ANALYSIS

The study used a thematic analysis to develop common themes and sub-themes (Braun & Clarke, 2006). As part of the overall SLR method, thematic analysis identifies, analyses and reports patterns across the selected publications. Thematic analysis is advantageous to this study due to its flexibility and theoretical freedom to search through rich and detailed data accounts (Braun & Clarke, 2006). This contributed to highlighting the five factors (sub-themes)– *Information Security Knowledge and Awareness, Workload Management, ISC, Encryption, Data Backup and Access and Authentication* and understand where each factor would fall and what implications it would have for each cybersecurity dimension (themes) – *people, process, and technology.*

The study identified and reviewed 45 publications. Of the 45 publications, 19 publications had implications on the *people* dimensions (11 *Information Security Knowledge and Awareness* and 8 *Workload Management),* 13 publications had implications on the *process* dimension (13 *ISC*), and 13 publications had implications on the *technology* dimension (2 *encryption,* 2 *data backup,* 9 *access and authentication).*

4 LITERATURE REVIEW

4.1 CHAPTER OVERVIEW

Traditionally, and understandably, healthcare has been focused on patient care. Due to this tradition, healthcare information security complications and vulnerabilities have increased (Coventry et al., 2018). Healthcare facilities have become increasingly overwhelmed with high workloads, stress, fast-paced environments, high staff turnover, and complex interconnected systems. In addition, legacy systems have contributed to information security risks and introduced new threats to the healthcare industry (Lehto et al., 2022). This chapter presents the themes related to the information security behaviours identified using the guidelines by Braun and Clarke (2006).

The literature review from the last five years has identified 17 common behaviours, as shown in Table 6. The identified behaviours are connected to and dependent on a broader spectrum of factors, often tied to one of the three cybersecurity dimensions – *people, process, and technology*. Extant literature discusses these factors through theories such as TPB, PMT, TAM and SCT. The following sections will describe and group the seventeen behaviours into one of the dimensions (Yeng et al.,2022b; Coventry & Branley, 2018; Coventry et al., 2020; Kruse et al., 2017a; Anderson, 2022; Jalali et al.; 2020). The following sections have been split into three parts: Behavioural Interactions in Healthcare, the Factors, and the dimensions – *people, process, and technology*.

4.2 BEHAVIOURAL INTERACTIONS IN HEALTHCARE

Health information holds rich PII; a cybercriminal can instantly identify an individual once sensitive information is accessible. Being one of the most highly sought-after industries to attack, it is critical to ensure that health professionals are aware of their part in protecting HIS and compliance with HIPAA. Multiple studies in the selected time frame (2017-2023) have indicated a relationship between information security compliance behaviour and healthcare practices (Yeng et al., 2022; Yeng et al., 2021; Martin et al., 2017; D'Arcy & Teh, 2019; Dong et al., 2021; Ali et al., 2021; Humaidi & Balakrishnan, 2018; Alanzai et al., 2020; Grasseggar & Nedbal, 2021) while other studies delved deeper into this behaviour through security practices (He et al., 2021; Kaiser & Jalali, 2018; Coventry et al., 2020; Wei & Courtney, 2018; Christiansen et al., 2017; Kruse et al., 2017a; Tazkarji, 2020). Behaviour through information security practices describes how an individual behaves while using or interacting with information or assets of an organisation, such as PHI and PII (Tanriverdi & Metin, 2021). Other studies focused on the most significant attack faced by healthcare – phishing – and conducted simulations across different countries to see whether health professionals were able to detect and report phishing emails; these countries included but were not limited to the United States, Greece, Portugal, Italy, United Kingdom and many more (Jalali et al., 2020; Gioulekas et al., 2022; Yeng et al., 2022; Gordon et al., 2019; Rizzoni et al., 2022).

Healthcare is behind other industries in understanding information security and digital literacy (Sari et al., 2022). Despite the growing opportunities and awareness to develop more informed and interactive security awareness training and programs, information security continues to burden healthcare professionals. It is understood that health professionals' priority is patients. To ease such burdens of information security practices, Coventry et al. (2020) and Tazkarji (2020) noted that sharing passwords and credentials with colleagues was done to reduce additional tasks such as facilitating logging back into a device, and Martin et al. (2017) noted the widespread use of sharing passwords amongst health professionals was a practice that 'makes sense'. In addition, shared workstations and spaces allowed nurses to access the same information (Wei & Courtney, 2018), and Coventry et al. (2020) also highlighted that along with shared workstations, computers were left logged in while they stepped away to tend to patients. Another form of sharing was through shared USB sticks, which stored patient

information and were handed over to colleagues when needed. Wei & Courtney (2018) noted that while looking after patients, health professionals also used 'sticky notes' during a procedure or an assessment of a patient to help track their tasks (Kellogg et al., 2017).

Table 7 - How do Healthcare Professionals Interact with Information Security?

ID	Behavioural Interactions	Reference
B01	Health leaders need help to adapt to changing technologies and implementing HIT.	(Laukka et al., 2020); (Garcia-Perez et al., 2023).
B02	Staff share passwords and credentials for convenience when accessing devices between patients.	(Tazkarji, 2020); (Martin et al., 2017)
B03	Due to a lack of care and stress, staff unknowingly click on embedded email links (phishing, scams).	(Jalali et al., 2020); (Priestman et al., 2019); (Rachmayani et al., 2021)
B04	The use of USB sticks is common for sharing information with patients.	(Javaid et al., 2023)
B05	Sticky notes are used to record patient information, passwords and other tasks for convenience during shifts.	(Kellogg et al., 2017); (Coventry et al., 2020)
B06	Staff are leaving computers logged in and unattended when tending to patients.	(Farah et al., 2022) (Nunes et al., (2021)
B07	Security incidents are not reported as they occur.	(Argaw et al., 2020).
B08	Patient information is not encrypted, whether stored or transmitted in personal or work devices.	(Anmulwar et al., 2020); (Pollini et al., 2021)
B09	Lack of cybersecurity teams to protect assets.	(Gioulekas et al., 2022);
B10	Unauthorised access to patient information (e.g., celebrity patient)	(Kim, 2022); (Thapa & Camtepe, 2021)
B11	Improper use of ISPs.	(Alanazi et al., 2020)
B12	Staff bypass authenticated communication channels by sharing patient medical information with large groups involving other staff.	(Coventry et al., 2020); (Liu et al., 2019)
B13	Little to no budget was dedicated to information security practices as it was not a priority.	(Kaiser & Jalali, 2018)
B14	Staff have shared workstations where resources and information are open and available for use.	(Wei & Courtney, 2018);
B15	Lack of access controls to connected medical devices or EHR systems.	(Coventry & Branley, 2018) (Nifakos et al., 2021)
B16	Lack of patient data backup.	(Erceg, 2019)
B17	Staff wrote passwords in insecure and accessible locations when dealing with work.	(Farah et al., 2022)

Looking closely into behaviours, it is essential to understand that an organisation's *ISC* plays a pivotal role in how it views its practices and complies with ISPs. ISPs are set out and enforced by leadership. The success of technological implementation is driven by *ISC* (Chen & Decary, 2020), but a lack of investments in security teams have made it challenging to navigate *ISC* (Gioulekas et al., 2022). Coventry et al. (2020) found that a lack of ISPs or reinforcement of existing policies makes it difficult to identify what 'best practice' is when practising information security. Further, Coventry et al. (2020) mentioned the importance of ensuring health professionals understood why they were expected to perform security practices. They also highlighted difficulties adapting to changing technologies due to a lack of security awareness and ISP enforcement. However, Laukka et al. (2020) noted that some leaders also felt insecure with their understanding of technology and struggled to adapt to changing technologies.

Separate case studies and surveys demonstrated that security awareness was minimal. Due to a lack of knowledge and understanding and the absence of reinforcements of ISPs, many threats are protected. Jalali et al. (2020) conducted a case study of a phishing simulation across three hospitals in the United States. They found that out of the final sample of 397 health professionals, about 231 (58.19%) of participants clicked on a simulated phishing link, and about two years later, Yeng et al. (2022) had a similar result in a phishing simulation conducted in a Ghanian hospital found that out of 167 participants, 102 (61.1%) clicked on the simulated link. Moreover, in the same year, Gioulekas et al. (2022) had a finalised sample of 736 participants, where only 161 (21.9%) knew how to detect a suspicious email. Coventry et al. (2020) explained that phishing emails and failure to see scams in emails were due to health professionals failing to recognise safe email addresses and often relying on identifying a patient's name in the subject box instead. While failing to detect threats, others were unable to understand the consequences of their actions, including one noted by Boddy et al. (2018) in which some health professionals abused their access privileges to seek and access patient information, particularly celebrities, to understand where they were held and for what reason. Further, a lack of access controls makes legacy systems and new technologies vulnerable. This was noted by Christiansen et al. (2017), who touched on integrated EHR and networks and found access controls needed when Integrating EHR in a hospital facility in Norway. To ensure practices of the CIA triad, *data backup* (related to the Integrity and Availability of the triad) is crucial to ensuring patient information is up to date; however, Erceg (2019) found that personal data and document data needed to be stronger. In other cases, data was shared in large groups by bypassing secure communication channels, which was more convenient (Coventry et al., 2020; Newaz et al., 2021; Liu et al., 2019). Despite this, records of unprotected data were also found when in transmission or storage (Coventry et al., 2020; Anmulwar et al., 2020).

4.3 THE FACTORS

The identified behaviours are connected to and dependent on a broader spectrum known as factors. These factors are often discussed and understood through behavioural agents such as TPB, PMT, TAM and SCT. Each behaviour was tied to one of the five factors demonstrated in **Figure 1**. This sub-section will define why each behaviour was organised into their respective factors.

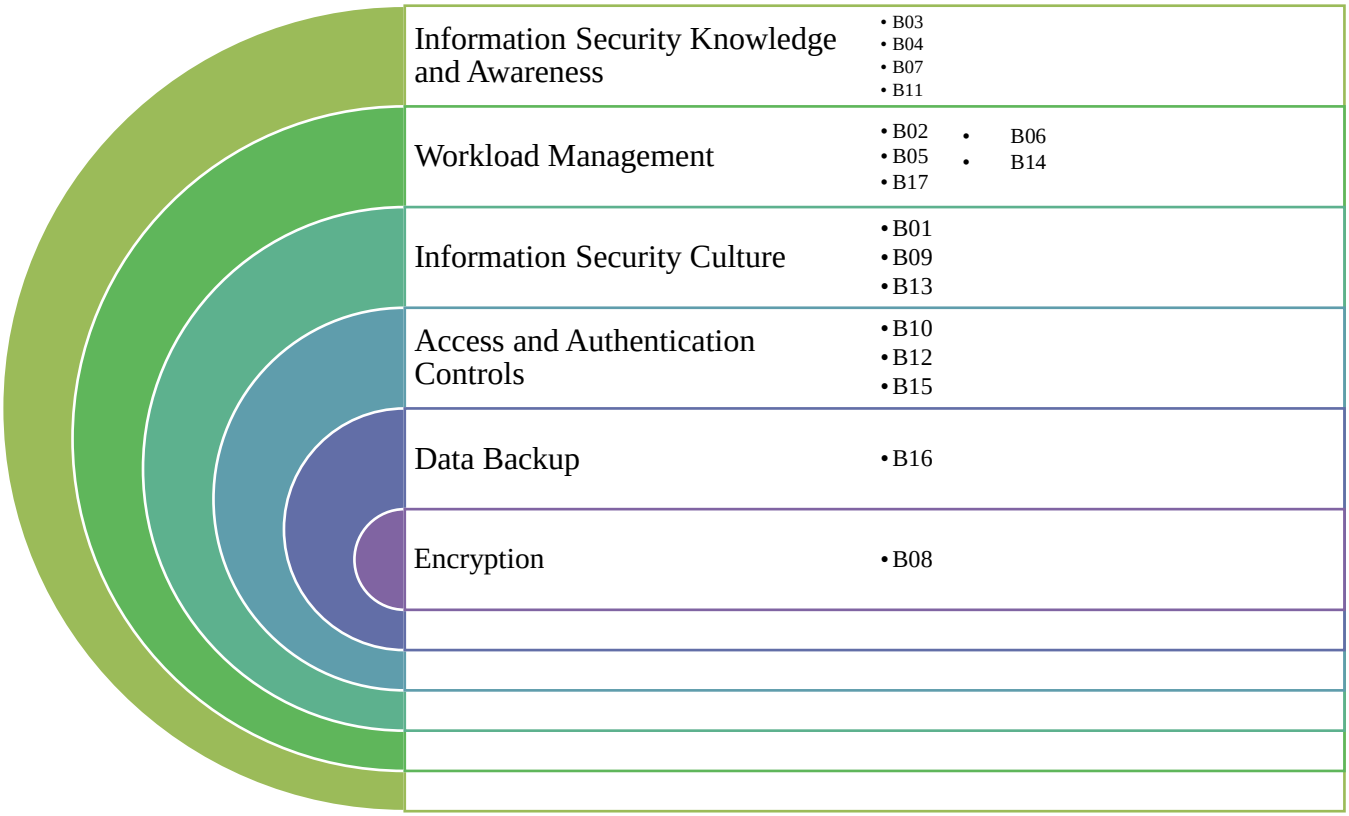

Figure 1 - The Factors

Information Security Knowledge and Awareness focuses on individuals' ability to interact with information security practices based on their awareness and knowledge. Behaviours are often determined by the individual's perceived severity and attitude towards completing a task. In this instance, behaviours **B03, BO4, B07** and **B11** have been recognised as behaviour driven by this factor. Chen et al. (2006) studied the lack of security awareness in organisations and detailed numerous security risks such as viruses, stolen passwords, social engineering, authorisation, and authentication violations due to a lack of security knowledge and awareness. **B03** was found by Jalali et al. (2020), who recognised that due to an increase in stress and a lack of care, staff were unknowingly clicking on embedded emails to make sure they were not missing any important announcements or updates on patients therefore making PII and PHI are susceptible to confidentiality, integrity, and availability issues. Failing to detect and report a phishing email or scam is a result of a lack of security knowledge and awareness (Jalali et al., 2020) and often leads to behaviours like **B07**, where failure to detect phishing emails often leads to incidents are left unreported in real-time (Argaw et al., 2020). He et al. (2021) found that incident reporting of phishing scams and malware was found to be the most commonly missed incidents to be reported as health professionals failed to detect scams embedded in emails. Lack of security training prioritisation has led many organisations to human error. Emails are known as a 'formal medium of communication'; however, the use of email does not provide the use of a dedicated service or application (Wani et al., 2022). Priestman et al. (2019) discussed that health professionals may have limited awareness of such threats due to training prioritisation, where security

training was focused on the ‘functional’ features of the software and 01 In addition, his one-month assessment of an organisation in 2018 found that 18,871 threat messages were detected out of 486 individual employee email addresses identifiable from publicly scraped data. A separate study conducted a year later by Coventry et al. (2020) found that there are warnings for staff not to click or open attachments; however, many staff members perceived this advice as unfeasible as they needed to open attachments to complete their jobs. Failing to detect malicious attachments has led to failing to prevent phishing attacks. **B11** was an expected behaviour amongst many health professionals who did not understand the implications of an ISP due to a lack of training and awareness of its criticality. Alanazi et al. (2020) concluded that there is a moderating impact of ISP and technology awareness on an employee’s information security compliance behaviour towards practising information security. As a result, behaviours like B04 become common as staff are unaware of policies and find no perceived danger of using and sharing USB sticks due to a lack of transparent policy enforcement and security training (Javaid et al., 2023)**.** Lack of *information security knowledge and awareness* often makes handling workload careless.

Workload Management focuses on a health professional's ability to manage their workload whilst practising information security to protect PHI and PII. In this instance, the behaviours **B02, B05, B06, B14,** and **B17** have been recognised as driven by this factor. This factor was tied to many behaviours because health professionals prioritised convenience over security to ensure that workload was not an issue. Patient care culture guides how health professionals handle workloads, emergency cases, ease of stress environments and their intention to practice information security. *Workload management* is one of the factors in dealing with and influencing how health professionals behave when interacting with information security, and having convenience means resources and information need to be easily accessible. As a result, staff are more induced to share passwords and credentials (B02) and use sticky notes (B05) to have a more convenient use of time, especially during high emergency cases in which the hospital is liable to short staff (Tazkarji, 2020; Kellogg et al., 2017). Further, some staff would utilise both behaviours of **B02** and **B05** together, as discovered by Coventry et al. (2020), who noted that sticky notes were attached to monitors for convenience when logging into their devices to “save time and [remember] forgotten passwords” and in addition to this, staff often left computers logged in and unattended when tending to patients **(B06)** (Farah et al., 2022) and Coventry et al. (2020) also noted that passwords were written and stored in insecure and easily accessible locations **(B17)** so that staff were able to see it during times of high workload intensity. Health professionals often have shared workstations where resources and information are open and shared for all staff usage **(B14)** to ensure no difficulty accessing information when searching amongst patient files (Wei & Courtney, 2018). Struggles in dealing with the workload while practising information security are due to the lack of *ISC*, in which leadership is not invested in the *ISC* to help staff understand their responsibilities and expectations.

ISC ties all the factors together and is often consistent with how staff behave or perceive the set controls put in place to protect information. *ISC* is captured and guided through the enforcement of ISPs. Although the enforcement of ISPs guides all behaviours, this instance will focus solely on the health organisations' overall preparation, investment, and enforcement of ISPs in which B01, B09 and B13 behaviours were recognised to be behaviours driven by this factor. Establishing cybersecurity departments to monitor and protect assets, as *ISC* denotes the understanding of attitudes, behaviours, knowledge, and awareness (Yeng et al., 2019a) and is often a great way to ensure that incidents and technological updates are sent to a centralised team to manage this and protect and establish a more secure security culture however Gioulekas et al. (2022) found that many health organisations in Europe did not have established cybersecurity teams due to a lack of understanding on its importance. In addition, some health organisations acknowledged the budget prioritisation of security training. A study by Kaiser & Jalali (2018) study, conducted in the form of an interview, acknowledged the existence of **B13** where some hospitals did not have control or sufficient resources to prioritise a cybersecurity

budget as it was a lack of priority, with many viewing *ISC* as a barrier to patient data portability resulting in increased workloads and high rates of error with one interviewee stating the following:

> "*Doctors, that is a different story…The nature of their work – they have to get patients in and out. They are probably the least understanding."* (Kaiser & Jalali, 2018).

This indicates that an *ISC* is unlikely to be seen as a priority due to the nature of their work. Coventry and Branley (2018) spoke of the importance of cybersecurity as a critical part of patient care culture. Grass et al. (2019) noted that health organisations would take substantially longer than other industries to contain data breaches due to a lack of resourcing, trained staff, and inefficient infrastructure. Maintaining strong and consistent security training can contribute to a stronger *ISC*. **B01** demonstrates the struggles of health professionals to adapt to changing technologies and other interconnected medical devices; this is an example of a weak *ISC* where such processes are not supported. Laukka et al. (2020) discussed that while significant investments in technological advancements in health organisations to drive better work efficiency, the lack of training, role delegation, and support provided to health leaders have caused adaptation challenges to newly implemented HIT. *ISC* can have a ripple effect on critical controls such as *access and authentication*, which protects unauthorised access to PHI and PII stored on HIS.

Access and authentication focus on the authorisation of access to HIS. In this instance, the behaviours B10, B12 and B15 have been recognised as behaviours influenced by the factor. Due to open workstations, shared passwords and credentials, *access and authentication* controls needed to be enforced better to protect HIS and physical workstations. Boddy et al. (2018) noted that users who access sensitive patient data may abuse their privileges for personal reasons, such as accessing and viewing celebrity information **(B10)**. Kim (2022) found that accessing patient records, such as celebrity records, often leads to identity theft and fraud, which is against HIPAA regulations to ensure patient data are protected from authorised access in other cases, like the study conducted by Kaiser & Jalali (2018), the study found that there was a need for authentication before accessing patient information. However, due to the complexity of the healthcare culture, understanding the hospital's primary mission often leads to a conflict of choice over information security practices (Kaiser & Jalali, 2018). Authorised personnel should only access medical devices and keep information through an access log (Newaz et al., 2021). A study by Coventry et al. (2020) found that staff bypassed official communication channels **(B12)** and emailed patient information to large groups involving other staff who required the same information; however, authentication to access that shared information was optional. However, in an earlier study conducted by Coventry & Branley (2018), it was found that there was a lack of access controls to connected medical devices or EHR systems **(B15)** as there were easily accessible points in HIS, and the use of legacy systems was in place. More emphasis needs to be placed on cybersecurity surrounding *access and authentication* controls. If compromised, patient data could be exposed to several threats, especially if the shared data is not securely backed up. All behaviours demonstrated a common danger of lack of *access and authentication* controls needed to protect patient information. However, if it has been unauthorised, patient data must be backed up to avoid confidentiality and availability issues.

Data backup focuses on ensuring that patient information is stored securely and kept for a specific period recommended by the organisation-aligned standard. In this instance, behaviour **B16** was the only behaviour influenced by this factor. Erceg (2019) conducted a survey highlighting information security practices of health professionals when storing patient information and found that staff failed to back up patient data.

Lastly, *encryption* is a technical practice that ensures patient information is kept secure by locking or encrypting the data from unauthorised access. In this instance, much like the previous factor, only one behaviour, **B08**, was recognised to be influenced by this factor. Farah et al. (2022) conducted a study demonstrating compliant and non-compliant behaviour among medical students. They found that

students practice one or more insecure behaviours, such as sharing patient data with other staff through unencrypted work and personal devices.

4.4 THE DIMENSIONS

Information security or cybersecurity, often used interchangeably, comprises three dimensions – *People, Process and Technology*, as demonstrated in **Figure 2**. Each dimension focuses on a different aspect of information security and contributes to an organisation's overall security health and posture. The dimensions align with the three pillars of information security, the CIA triad.

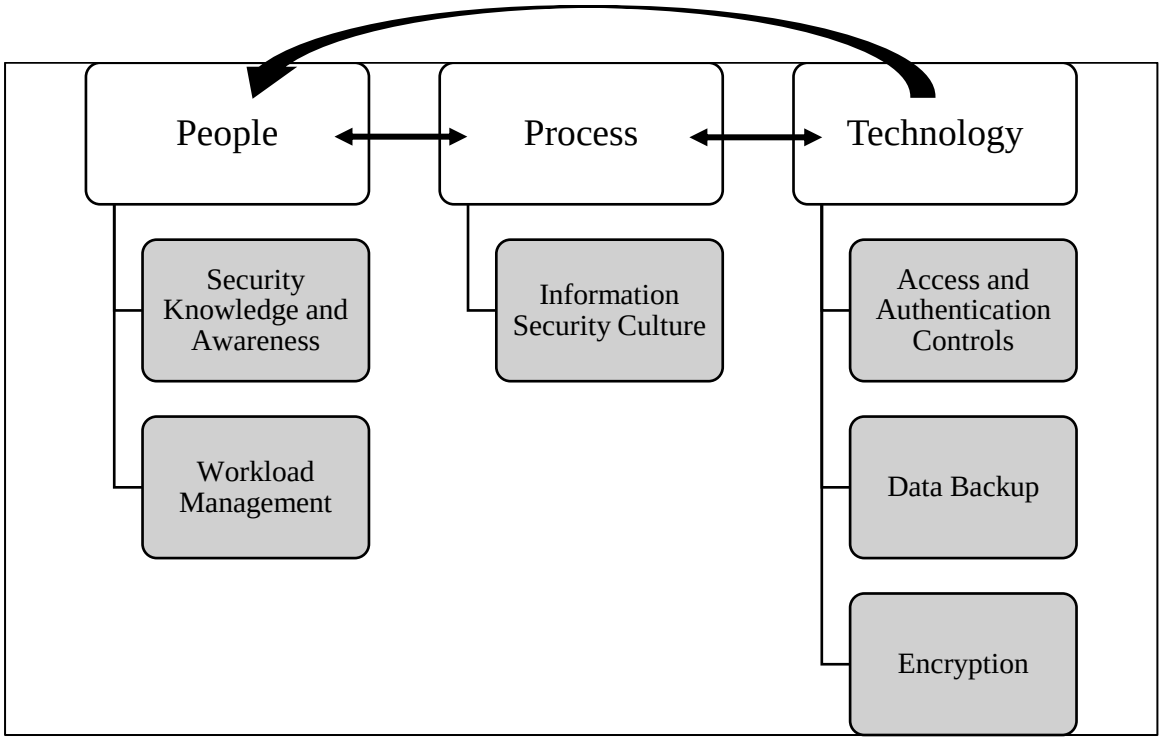

Figure 2 – Relationship between Factors and Dimensions

4.4.1 People Dimension

The *people* dimension focuses on employees and stakeholders responsible for maintaining and carrying out information security. People are the biggest threat to information but are also the first line of defence (Harper, 2023). Therefore, the people dimension of cybersecurity must be addressed efficiently. It can be done through understanding and increasing *security knowledge and awareness,* understanding the employee's *workload management* and behavioural intention to follow set ISPs. Information security compliance behaviour is a matter of human behaviour (Ali et al., 2021). Health professionals are the first line of defence against any posed threats or cyber challenges; however, as much as technological advancements go, its defences will not matter if the *people* dimension is not addressed as the priority as they are often considered the weakest link in the security chain (Dalal et al., 2022). To ensure that the *people* dimension is addressed, the factors of *'Security Knowledge and Awareness' and 'Workload Management'* have been considered under this dimension.

Security breaches in healthcare are common and are widely due to human error, mishandling, and misuse of IT (Yeng et al., 2021a). This dimension is essential to addressing and focusing on the needs of health professionals. Healthcare professionals often face high workloads, intense emergency cases, and various psychological, social, and cultural factors influencing their behaviour and attitude towards information security practices. The urgency to tend to patient care before technology gives cybercriminals an advantage (Yang et al., 2022). In dire situations, healthcare professionals dealing with intense emergencies rely on coworkers to access HIS by sharing passwords (Handayani et al., 2023). Lee & Seonum (2021) found that healthcare professionals' perceived severity of such insecure practices is influenced by security awareness and the understanding of potential security issues and consequences; however, they concluded that extrinsic and intrinsic rewards did not impact HIS intentions and behaviour, which contradicts Yeng et al. (2022b) findings which later found that financial rewards did have a positive relation with intention and behaviour.

Coventry et al. (2020) mentioned the importance of ensuring health professionals understood why they were expected to perform security practices. It would encourage more secure actions and provide urgency for health leaders to drive adequate training for better security awareness when dealing with behaviours highlighted in **B03, B04, B07** and **B11**. Separate case studies and surveys demonstrated that security awareness was minimal. Behaviours such as unknowingly clicking on embedded links or insecure attachments (Jalali et al., 2020; Priestman et al., 2019) are outcomes that health professionals would take when there is a lack of security knowledge and awareness. However, this also plays into the *workload management* of their job because attachments are often sent to the staff to access patient information and client files. However, there is a need to increase security knowledge and awareness within health organisations (Nunes et al., 2021) to help staff differentiate what is authentic and what is not (Coventry et al., 2020). Nunes et al. (2021) also described standard practices in healthcare, including sharing computers and passwords to handle workloads and a factor of their overall behavioural intention to practice information security.

Argaw et al. (2019) acknowledged the healthcare sector's vulnerability to attacks as the work makes it extremely sensitive and vulnerable to any service disruption. Workload stress and emergency cases often led to behaviours highlighted in **B02, B05, B06,** and **B14**. These behaviours could lead to social engineering attacks due to the lack of awareness when sharing information. Argaw et al. (2019) recommended specialised training programming for social engineering as its practicality and relationship would be beneficial in dealing with such behaviours. The risk of cybercrime and increased threats increases as the healthcare industry continues to evolve technologically, making it more difficult for healthcare professionals to keep up with basic information security practices while ensuring they are fulfilling their day-to-day obligations. Healthcare professionals must adapt to the security procedures and information systems developed to securely manage and maintain patient information (Williams et al., 2021). A healthcare professional's core responsibility should be to deliver quality healthcare; therefore, changing clinical practices to meet the demands of IT and practice information

security is not a priority. Understanding why these certain security practices are essential would encourage them to act cautiously (Coventry et al., 2020). Many staff expressed the importance. It is essential to be 'kept in the loop' when practising information security and for healthcare executives to provide adequate training to encourage better cyberattack awareness (Coventry et al., 2020).

Investing in and providing adequate security awareness training will ensure that proper practical implementations of secure behaviour would play a role in ethical norms such as privacy-preserving behaviour when sharing and using PII (Mikuletic et al., 2023). Awareness interventions are one way to ensure an understanding of social influence and ethical practices and implications on healthcare (Mikuletic et al., 2023). In addition, unawareness of ISPs and the practices within would cause information handling (Alanazi et al., 2020). However, the investment in security awareness to motivate healthcare professionals may need to be the second priority as successful training is mainly dependent on "user buy-in", indicating that the busy nature of a healthcare professional may impact how much of the training will be useful (Wani et al., 2022). A study by Grasseggar and Nedbal (2021) found that from a managerial perspective, information security awareness should be the central development of information security measures. Another study completed by Yadav et al. (2017) concluded that cybersecurity knowledge for healthcare organisations is essential for staff and urged the importance of staff training to ensure a secure and safe environment for patients.

Stress often leads healthcare professionals to rush through emails. Rachmayani et al. (2021) discovered a significant association between stress and risky cybersecurity behaviour. As a result, health professionals are more vulnerable to phishing emails as they rush through their day-to-day tasks. In addition, health professionals who may not have experience detecting phishing emails or do not have the time to consider the insecure embedded link will open the link, which was particularly common during the outbreak of COVID-19 (Chaturvedi et al., 2020). It is understood that there is a positive correlation between stress and insecure information security practices (Rachmayani et al., 2021). The workload of healthcare professionals often results in the staff becoming exhausted, burnt out, and having limited attention and cognitive resources, making them more likely to click on insecure embedded links without proper review or share sensitive information with others to avoid any further social activity, to allow themselves a moment to breathe (Rachmayani et al., 2021). Due to the common practice of credential sharing and USB passing, most phishing emails would likely be able to use social engineering to retrieve passwords and access data (Javaid et al., 2023). Higher assessments of peers' security interaction relating to behavioural intention impact an employee's evaluation of the organisation and cues to action when dealing with information security or cyber threats (Li et al., 2019).

4.4.2 Process Dimension

The *process* dimension addresses the procedures and policies set out by an organisation. It also considers laws and regulations, such as HIPAA, to help guide the other two dimensions. ISPs are set in stone for this reason, and information security behaviour is often defined or influenced by the ISPs, which is set out by the leadership team. To drive positive behaviour towards information security, ISPs are enforced through a strong *ISC* (Chen & Decary, 2020).

Driving a positive *ISC* would be pivotal to promoting information security behaviours when utilising medical technologies daily (Sari et al., 2021). However, adopting new technologies requires time to enforce ISPs and implementation processes (Kruse et al., 2017a). Health leaders noted the struggle to adapt to changing technologies and other interconnected medical devices as a result of a lack of security culture where such adaptation was not prioritised to be looked into (Laukka et al., 2020). Health leaders have a role in directing and supporting transformational changes for all staff (Garcia-Perez et al., 2023). Wiig et al. (2020) considered resilience in healthcare as "the diverse capacities of a healthcare system that allow[s] it to maintain the delivery of high-quality care" is grounded in the processes of system adaption, individuals and teams which represent processes underpinning growth, development, and recovery from challenges. Failing to understand and implement methods to enforce ISPs and build a

strong *ISC* would impact the technological adaptation processes. Securing the endorsement of upper management to champion ISPs for a better *ISC* is crucial to ensuring that medical technologies are up-to-date and used effectively and efficiently for increased patient care. Building a strong 'human firewall' requires enhancing a security resilience culture (Yeng et al., 2021).

Leeuw et al. (2019) identified several barriers that have been noted to contribute to the difficulty in adapting to changing technologies. These barriers include 'an organisation's structure and security culture, the incentives given, and the development and organisation of technology developments. Humaidi and Balakrishnan (2017) discussed the importance and influence of information security processes in the healthcare industry. Notably, the study stressed the importance of using TPB and self-efficacy to promote and understand compliance behaviour when implementing ISPs. The study concluded that leadership support and reinforcements of ISPs influence health professionals' trust in the organisation of ISPs. Amankwa et al. (2022) found that staff expectations of evaluation greatly impacted the attitudes to comply with ISPs. This insinuated that if staff were made aware and believed that their security activities were being evaluated and tracked, they would demonstrate secure behaviour more.

Kruse et al. (2017b) noted that healthcare organisations prepare for data breaches by including security techniques such as implementing a data breach plan and training employees to become more aware of security threats – all of which are extensions of ISPs and a practical step into a better *ISC*. As an extension of B07, currently aligned to the people dimension, highlights the behaviour of lack of incident reports as they occur due to lack of security knowledge and awareness; the process dimension focuses on processes such as an Incident Response Plan (IRP) to help health professionals prepare for incidents. These plans must be regularly tested and exercised, and a precise alignment of the organisation's security culture and posture should be considered (Argaw et al., 2020). In the case of an attack, an organisation should have an internal plan to deal with and adapt to the needs and requirements revealed through the incident (Argaw et al., 2020). Zakaria et al. (2019) developed an Internet of Things (IoT) Security Risk Management Model for Healthcare Practice[21] by aligning with COBIT 5 to better align healthcare IoT with the Hospital Performance Indicator for Accountability (HPIA). The model touches on the importance of risk management and its alignment with factors that highlight HIPA, including internal business processes, customer focus, employee satisfaction, learning and growth, financial and office management, and environmental support. However, due to the complexity of the proposed model, health leaders may require more than ISPs to address the alignment fully and utilise the model at its total capacity. Healthcare information security culture has been described as counterproductive and time-consuming (Coventry et al., 2020). The culture has been a predictor of low risk to cues to action, response efficacy and punishment severity (Yeng et al., 2022), resulting in behaviours **B09 and B13** (Gioulekas et al., 2022; Kaiser & Jalali, 2018; Farah et al., 2022). Lin & Kujabi (2022) recommended that leadership evaluate the IT skills of the hospitals and clinics to effectively partner with policymakers to fund HIS projects and train hospitals and health professionals on their maintenance. In addition, they indicated a need to upgrade health professionals' computer literacy levels.

4.4.3 Technology Dimension

The final dimension, often mistakenly prioritised over the *people and process* dimension, is the *technology* dimension. It is often prioritised in the healthcare industry due to its efficiency in developing and providing patient health services. The *technology* dimension refers to the tools and solutions used to protect an organisation's information assets (Harper, 2023). This dimension combines the efforts of the *people* dimension and the *process* dimension to provide a more secure technological experience.

[21] Formulation of the IoT security risk management model for healthcare practice consists of three parts consisting of Healthcare IoT Risk Management, HPIA alignment and COBIT5 implementation phases to help reduce information security risks and threats whilst also aiming to reduce cost, time, and operational tasks in healthcare.

The factors of '*access and authentication*', *'data backup' and 'encryption'* are related to the technical protection of information assets as they are required to ensure CIA is in practice when using HIS.

Access and authentication controls are fundamental requirements of HIPAA. These requirements are set forth to ensure that only authorised users, under specific roles and responsibilities, are provided access to certain sensitive information or systems (Zhang et al., 2018). It is essential to ensure that devices storing and transmitting PHI are secure (Thapa & Camtepe, 2021). Accessing sensitive health data requires consent, including if this data is only for short-term collection, analysis, and long-term storage. Access controls protect individual privacy, confidentiality, and autonomy (Thapa & Camtepe, 2021). Health professionals utilise and change between personal and work devices to access PHI. Pollini et al. (2021) observed that health professionals who needed more security knowledge and awareness fully acknowledged personal devices used for work-related activities. As a result, protective measures were not in place, potentially exposing the company equipment and their devices to vulnerabilities. Wani et al. (2022) found the use of SMS and WhatsApp to transmit and store patient data, such as photos and videos, especially among doctors. Wani et al. (2022) concluded that the lack of a dedicated and secure communication service, including its convenience, may be one of the reasons for the high usage of SMS and WhatsApp. Moreover, another study by Yadav et al. (2017) also recommended using a low-interaction honeypot intrusion detection system to help health professionals who will only provide limited access to patient information. Intrusion Prevention Systems and Intrusion Detection Systems (IPS and IDS)[22] are essential security tools to protect sensitive information (Thapa & Camtepe, 2021). These tools would help any device detect any malware or virus that may have been installed anonymously, as health professionals can become unaware of information security threats (Nifakos et al., 2021).

An average hospital room could contain as many as 15-20 medical devices; however, this is multiplied depending on the number of rooms within a single ward (O'Dowd, 2017). As medical technologies[23] evolve, so does interconnectivity (Kruse et al., 2017a). New technologies have been implemented to provide a more seamless integration and connection between healthcare professionals and patients. A study by Christiansen et al. (2017) noted that integrated EHR and networks lacked access controls when combining EHR in a hospital facility in Norway. Argaw et al. (2019) recommended that access controls and security testing would need to be conducted beyond its integration. However, due to such failures in implementing access controls, staff can retrieve patients' data conveniently for personal reasons (Boddy et al., 2018). It can share such information by bypassing authenticated communication channels (Coventry et al., 2020). Ahmed et al. (2019) recommended that health organisations invest in automatic online backup systems or cloud storage to avoid any data loss, as it was found that when leaving the responsibility of ensuring *data backup*, staff are doubtful to do so. Data breaches are common in healthcare; therefore, *data backup and encryption* are necessary to protect the disclosure of PHI and PII. Access to neither backed-up nor encrypted data could indirectly lead health organisations to monetary vulnerability (Gordon et al., 2017).

[22] IPS and IDS watch, protect and identify possible incidents within an organisation. It can log, stop, and report incidents to security administrators (Juniper, 2024).

[23] Medical technologies vary from remote monitoring, telemedicine, neurotechnology, digital therapeutics and more. Its purpose is to feed the HIS and contribute to reporting for better healthcare service.

5 PROPOSED RECOMMENDATIONS AND FRAMEWORK

5.1 CHAPTER OVERVIEW

This chapter will align the identified behavioural aspects with two internationally accepted security standards: HIPAA and the Centre for Internet Security (CIS). This mapping will guide a proposed security awareness framework to help health organisations understand what is essential to drive and foster a better *ISC*. **Table 8** has taken CIS controls and HIPAA safeguards to help health organisations address health professionals' behavioural interactions identified within this study.

One of the most respected regulations set about for healthcare information security is the HIPAA security rule. Enacted in 2005, it regulated electronic health information to protect the PHI and PII of individuals, particularly for information which healthcare organisations have created, received, used, shared and maintained (US Department of Health and Human Services, 2022a). HIPAA requires adopting administrative, physical, and technical standards alongside other standards to ensure the CIA of PHI and PII. Therefore, using HIPAA safeguards alone is not enough to ensure protection; it is a guide. Therefore, this study has adopted the CIS[24] benchmark controls to align with the HIPAA safeguards. In order to address information security-related issues or behaviours of employees, *people, processes, and technology* are needed (Yeng et al., 2019a). CIS released their controls' latest version (V8) in January 2023 to ensure accuracy in alignment with HIPAA controls for PHI[25]. Health organisations must ensure that access to PHI is restricted, integrated, and highlighted during security training (Argaw et al., 2020).

The study's findings have stated that *information security knowledge and awareness* impact other factors. The alignment of the CIS benchmark controls, and the HIPAA noted that several recommended controls emphasised the importance of implementing and reinforcing security awareness and increasing security knowledge. The most common security control to address many of the behaviours was **C14 – Security Awareness and Skills Training *(HIPAA 164.308(a)(5)(i))*.** C14 is overarching control, focusing on establishing and maintaining a security program to help, encourage, and increase security awareness amongst employees, allowing them to be security conscious and adequately skilled to reduce the likelihood of cyberattacks and risks to the organisation.

The C14 control was also supported through other CIS sub-controls that focused on increasing security knowledge and awareness through training, including:

- C14.1 - Establish and Maintain a Security Awareness Program;
- C14.2 - Train Workforce Members to Recognise Social Engineering Attacks;
- C14.4 - Train Workforce Members on Data Handling Best Practices;
- C14.5 - Train Workforce Members on Causes of Unintentional Data Exposure;
- C14.6 - Train Workforce Members on Recognising and Reporting Security Incidents and
- C16.9 - Train Developers in Application Security Concepts and Secure Code.

The above CIS sub-controls were applicable across nine of the seventeen identified behaviours (<50% of the behaviours. Health organisations are recommended to implement these security controls to protect the sensitivity of PHI and control access to information on connected medical devices (Argaw et al., 2019). It is critical to understand that while it emphasises the importance of hosting a security

[24] The CIS benchmark controls are a set of controls used to highlight best security practices to strengthen an organisation's security posture. It is often mapped to other global information security standards, such as the International Organisation for Standardisation, NIST and the COBIT Framework (CIS, n.d).

[25] Full controls list of CIS Controls and HIPAA safeguards can be found here: *https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-hipaa*. *Accessed January 2024.*

training program, it does not necessarily mean it should be a one-time establishment. However, it should be a recurring effort to ensure that skills and knowledge regarding cyber threats, risks and challenges are addressed continuously. Therefore, HIPAA safeguards like **164.308(a)(5)(ii)(A) - Security Reminders** focus on the effort to have health organisations organise a 'refresher' training to equip staff better. The behavioural contribution to information security interactions is one of the most critical issues to be addressed. This can be done by implementing security controls, such as CIS controls and security guidelines, such as HIPAA safeguards (Zwilling et al., 2020).

Other sub-controls can come quickly once health professionals have the knowledge and awareness to understand the implications of failing to interact securely with information security. Adequate controls, such as configuring *access and authentication* controls to ensure the protection of information, will come naturally as teams are more aware of the importance of implementing such controls because perceived severity and behavioural intention to implement controls will only come if a user is aware of how and why it would need to be operated (Martins & Elofe, 2002). This is also applicable to *data backup and encryption*. Driving this implementation and increasing *information security knowledge and awareness* will fall onto the health leaders to ensure effective control management even after implementing training and technical controls (Martins & Elofe, 2002).

5.2 OTHER CONTROLS

Upon assignment of the security controls against each identified behavioural interaction, it was noted that behaviours **B09, B11** and **B13** did not require direct security controls against the interaction as these behaviours would require the health organisations to prioritise and discuss internally and align their security posture, culture, and budget accordingly to impact and influence these behaviours positively. Health organisations would need to evaluate the IT skills of the hospital to ensure tasks are carried out securely, effectively, and efficiently (Lin & Kujabi, 2022). These behaviours can be understood and positively influenced indirectly through some of the CIS and HIPAA security controls. For example, *C1.1 – Establish and Maintain Detailed Asset Inventory (HIPAA 164.310(d)(2)(iii))* can be applicable indirectly to the behaviours. Establishing a detailed asset inventory will outline the critical assets of the health organisation. In turn, health leaders should then allocate a budget towards protecting the assets (addressing **B13**), including establishing teams (addressing **B09**) and ensuring ISPs are in place to help guide the security teams in safeguarding the assets (addressing **B11**). A risk analysis or assessment can be the first step organisations take to understand the organisation's risk position (Argaw et al., 2020). This will indicate how much data can be lost before severely impacting the organisation.

Table 8 - Behaviour Interactions Alignment with CIS and HIPAA Controls

ID	Behaviour	Factor	CIS Control v8 (C)	HIPAA Control
B01	Health leaders are struggling to adapt to changing technologies and implementing HIT.	Information Security Culture	C16.9 - Train Developers in Application Security Concepts and Secure Code	
			C14.1 - Establish and Maintain a Security Awareness Program	164.308(a)(5)(i) - Security Awareness and Training
				164.308(a)(5)(ii)(A) - Security Reminders
B02	Staff share passwords and credentials for convenience when accessing devices between patients.	Workload Management	C5.1 - Establish and Maintain an Inventory of Accounts	164.312(a)(2)(i) - Unique User Identification
			C6 - Access Control Management	164.312(a)(2)(i) - Unique User Identification
				164.308(a)(4)(i) - Information Access Management
				164.308(a)(4)(ii)(c) - Access Establishment and Modification
			C14.2 - Train Workforce Members to Recognise Social Engineering Attacks	
			C14.4 - Train Workforce Members on Data Handling Best Practices	164.310(d)(2)(i) - Disposal
			C14.5 - Train Workforce Members on Causes of Unintentional Data Exposure	
B03	Due to a lack of care and stress, staff unknowingly	Information Security Knowledge and Awareness	C14 - Security Awareness and Skills Training	164.308(a)(5)(i) - Security Awareness and Training

	click on embedded email links (phishing, scams).			164.308(a)(5)(ii)(A) - Security Reminders
			C9 - Email and Web Browsers Protection	
B04	The use of USB sticks is common for sharing information with patients.	Information Security Knowledge and Awareness	C14 - Security Awareness and Skills Training	164.308(a)(5)(i) - Security Awareness and Training
				164.308(a)(5)(ii)(A) - Security Reminders
			C1.1 - Establish and Maintain Detailed Enterprise Asset Inventory	164.310(d)(2)(iii) - Accountability
			C10.1 - Deploy and Maintain Anti-Malware Software	164.308(a)(5)(ii)(B) - Protection from Malicious Software
			C10.3 - Disable Autorun and Autoplay for Removable Media	164.310(d)(1) - Device and Media Controls
			C10.4 - Configure Automatic Anti-Malware Scanning of Removable Media	
			C10.7 - User Behaviour-Based Anti-Malware Software	
			C14.4 - Train Workforce Members on Data Handling Best Practices	164.310(d)(2)(i) - Disposal
			C14.5 - Train Workforce Members on Causes of Unintentional Data Exposure	
B05	Sticky notes record patient information, passwords, and other tasks for convenience during shifts.	Workload Management	C14 - Security Awareness and Skills Training	164.308(a)(5)(i) - Security Awareness and Training
				164.308(a)(5)(ii)(A) - Security Reminders

			C14.4 - Train Workforce Members on Data Handling Best Practices	164.310(d)(2)(i) - Disposal
			C14.5 - Train Workforce Members on Causes of Unintentional Data Exposure	
B06	Staff are leaving computers logged in and unattended when tending to patients.	Workload Management	C4.3 - Configure Automatic Session Locking on Enterprise Assets	164.312(a)(2)(iii) - Automatic Logoff
B07	Security incidents are not reported as they occur.	Information Security Knowledge and Awareness	C14.6 - Train Workforce Members on Recognising and Reporting Security Incidents	164.308(a)(6)(ii) - Response and Reporting
			C17 - Incident Response Management	164.308(a)(2) – Assigned Security Responsibility
				164.308(a)(6)(ii) – Response and Reporting
				164.308(a)(1)(i) – Security Management Process
				164.308(a)(6)(i) – Security Incident Procedures
				164.308(a)(7)(i) – Contingency Plan
				163.310(a)(2)(i) – Contingency Operations
				164.308(a)(7)(ii)(D) – Testing and Revision Procedures
				164.308(a)(8) - Evaluation
B08	Patient information is not encrypted, whether stored or transmitted in personal or work devices.	Encryption	C3.6 - Encrypt Data on End-User Devices	
			C3.9 - Encrypt Data on Removable Media	164.310(d)(1) - Device and Media Controls
			C3.10 - Encrypt Sensitive Data in Transit	164.312(a)(2)(iv) - Encryption and Decryption

				164.312(e)(1) - Transmission Security
				164.312(e)(2)(i) - Integrity Controls
				164.312(e)(2)(ii) - Encryption
			C3.11 - Encrypt Sensitive Data at Rest	164.312(a)(2)(iv) - Encryption and Decryption
				164.312(e)(2)(ii) - Encryption
			C3.12 - Segment Data Processing and Storage Based on Severity	
			C3.13 - Deploy a Data Loss Prevention Solution	164.312(e)(2)(i) - Integrity Controls
				164.312(e)(2)(ii) - Encryption
			C3.14 - Log Sensitive Data Access	164.312(c)(1) - Integrity
				164.312(c)(2) - Mechanism to Authenticate Electronic Protected Health Information
				164.312(b) - Audit Controls
B09	*Lack of cybersecurity teams to protect assets.*	*Information Security Culture*	*N/A*	*N/A*
B10	Unauthorised access to patient information (e.g., celebrity patient)	Access and Authentication Controls	C3.3 - Configure Data Access Control Lists	164.308(a)(3)(i) - Workforce Security
				164.308(a)(3)(ii)(A) - Authorisation and/or Supervision
				164.312(a)(1) - Access Control
			C6 - Access Control Management	164.312(a)(2)(i) - Unique User Identification

				164.308(a)(3)(ii)(c) - Termination Procedures
				164.308(a)(3)(ii)(B) - Workforce Clearance Procedure
				164.308(a)(4)(i) - Information Access Management
				164.308(a)(4)(ii)(C) - Access Establish and Modification
B11	*Improper use of ISPs.*	*Information Security Knowledge and Awareness*	*N/A*	*N/A*
B12	Staff bypass authenticated communication channels by sharing patient medical information with large groups involving other staff.	Access and Authentication Controls	C3.3 - Configure Data Access Control Lists	164.308(a)(3)(i) - Workforce Security
				164.308(a)(3)(ii)(A) - Authorisation and/or Supervision
				164.312(a)(1) - Access Control
			C3.10 - Encrypt Sensitive Data in Transit	164.312(a)(2)(iv) - Encryption and Decryption
				164.312(e)(1) - Transmission Security
				164.312(e)(2)(i) - Integrity Controls
				164.312(e)(2)(ii) - Encryption
			C3.11 - Encrypt Sensitive Data at Rest	164.312(a)(2)(iv) - Encryption and Decryption
				164.312(e)(2)(ii) - Encryption
			C6 - Access Control Management	164.312(a)(2)(i) - Unique User Identification

				164.308(a)(3)(ii)(C) - Termination Procedures
				164.308(a)(3)(ii)(B) - Workforce Clearance Procedure
				164.308(a)(4)(i) - Information Access Management
				164.308(a)(4)(ii)(C) - Access Establish and Modification
			C14.4 - Train Workforce Members on Data Handling Best Practices	164.310(d)(2)(i) - Disposal
B13	*Little to no budget was dedicated to information security practices as it was not a priority.*	*Information Security Culture*	*N/A*	*N/A*
B14	Staff have shared workstations where resources and information are open and available for use.	Workload Management	C14 - Security Awareness and Skills Training	164.308(a)(5)(i) - Security Awareness and Training
				164.308(a)(5)(ii)(A) - Security Reminders
			C14.4 - Train Workforce Members on Data Handling Best Practices	164.310(d)(2)(i) - Disposal
			C14.5 - Train Workforce Members on Causes of Unintentional Data Exposure	
B15	Lack of access controls to connected medical devices or EHR systems.	Access and Authentication Controls	C3.3 - Configure Data Access Control Lists	164.308(a)(3)(i) - Workforce Security
				164.308(a)(3)(ii)(A) - Authorisation and/or Supervision

				164.312(a)(1) - Access Control
			C6 - Access Control Management	164.312(a)(2)(i) - Unique User Identification
				164.308(a)(3)(ii)(C) - Termination Procedures
				164.308(a)(3)(ii)(B) - Workforce Clearance Procedure
				164.308(a)(4)(i) - Information Access Management
				164.308(a)(4)(ii)(C) - Access Establish and Modification
B16	Lack of patient data backup.	Data Backup	C11 - Data Recovery	164.308(a)(7)(ii)(A) - Data Backup Plan
				164.308(a)(7)(ii)(B) - Disaster Recovery Plan
				164.310(d)(2)(iv) - Data Backup and Storage
B17	Staff wrote passwords in insecure and accessible locations when dealing with work.	Workload Management	C14 - Security Awareness and Skills Training	164.308(a)(5)(i) - Security Awareness and Training
				164.308(a)(5)(ii)(A) - Security Reminders
			C14.4 - Train Workforce Members on Data Handling Best Practices	164.310(d)(2)(i) - Disposal
			C14.5 - Train Workforce Members on Causes of Unintentional Data Exposure	

5.3 PROPOSED FRAMEWORK

Health professionals are often expected to comply with and follow information security practices to ensure the privacy and protection of PHI and PII within HIS (Yeng et al., 2019a). However, the study noted several factors tying back to information security knowledge and awareness, and much of the recommendations proposed within this study focus on this factor. One essential step was user education and awareness, which involved producing ISPs to correspond with staff training. While much research emphasises the *lack of security knowledge and awareness* causing poor behavioural interactions with information security, the study did not find many frameworks focusing on the types or contents of security training that could apply to healthcare organisations.

Past research has proposed a couple of ways to protect healthcare information. Hsu et al. (2013) proposed a privacy-enhanced HIS framework to investigate the role of privacy protection in HIS adoption by expanding the unified theory of acceptance and use of technology by considering perceived security and information security literacy. It concluded that security literacy indirectly affects the user adoption of HIT and HIS perceived security awareness. Yeng et al. (2019a) developed a control experiment framework for assessing nurses' motivations in security practices. The framework focused on the influence of knowledge, attitude, and behavioural intention of the nurses on security practices such as password management, incident reporting and email use. In another study, Martin et al. (2017) highlighted critical steps to improving cybersecurity.

This study proposes an Information Security Knowledge and Awareness Program (ISKAP) implementation framework, as demonstrated in **Figure 3**; despite healthcare organisations deeming information security culture time-consuming (Coventry et al., 2020), it is critical to outline what methods could be incorporated when considering how to increase security knowledge and awareness in a highly intensive workplace. This framework focuses on the core factor of information security knowledge and awareness to drive more secure behavioural interactions. The framework has four main components: *people, processes, and technology*. These four main components are Training Program Content, Reinforcement and use of ISPs, Technology Updates and Leadership Advocacy and Engagement.

1. The Training Program Content – *People* Dimension

This is often the first step to identifying an organisation's security culture and understanding staff security knowledge and awareness gaps. Clear awareness of information protection should be prioritised to increase healthcare information protection intention when using HIS (Yang et al., 2016). By first conducting and highlighting the most common and recent cyber-attacks occurring within the healthcare industry, the health executives will understand what types of threats their staff need to become aware of. Once establishing this, the health executives should send out a five-minute survey to receive insight from staff regarding their behavioural intention to interact with information security whilst juggling workload and also understand what other internal threats the organisation may face. This establishes the content necessary for the organisation to focus on. However, it is critical to keep in mind the high-intensity environment of a healthcare organisation and therefore, the suggested training methodology should be simulation-based, with security posters and a bi-annual security refresher through assessment or video-based training. Although classroom–based training, virtual training or a team presentation on security awareness are a great way to connect with staff on the importance of information security, the study found that health professionals find information security counterproductive and time-consuming (Coventry et al., 2020) and therefore such training would not be efficient to host in a healthcare organisation as they are patient-centric.

2. Reinforcement and Use of Internal ISPs and Leadership Advocacy and Engagement – *Process* Dimension

These components often go hand-in-hand as reinforcements, and ISPS could not be used without leadership advocacy and engagement. These components focus on establishing and reinforcing ISPs to support employee training. These components often involve auditing the organisation's security posture to analyse its risk appetite[26]. Processes must be enforced to align with security practices, as these are often used to guide best practices amongst employees. Leadership advocacy and engagement are critical to ensuring that alignment to international standards like ISO, NIST and COBIT are carefully aligned to the organisation's security objectives. This will also impact the budget allocation of the organisation, which is often aligned with international standards and requires a frequent audit review. Therefore, it must be carefully and explicitly considered when pulling health professionals away from their day-to-day tasks to training. Providing clear awareness of the consequences of security threats is a prerequisite to increasing a user's awareness of protecting PHI and PII (Yang et al., 2016).

3. Technology Updates – *Technology* Dimension

This dimension requires technical knowledge and is often addressed by internal information security teams dedicated to ensuring this component is operating effectively and efficiently, as much of the HIS relies on this component to store and transmit all patient information from one facility to another and from one colleague to another. Reviewing and upgrading legacy systems will also help protect PHI and PII; however, non-technical staff are often unaware of such systems and, therefore, would need to be made aware of them to ensure secure behavioural interactions. This component does not necessarily focus on ensuring 'all' health professionals become technical; it focuses on developing training methods to ensure non-technical staff are aware of the threats, risks and implications that come from carelessly using a legacy system or failing to practice and follow other controls such as backing up patient information before transmission or encrypted devices before usage (Gordon et al., 2017). Healthcare information is highly likely to continue being vulnerable despite the advances in HIT. The carelessness of HIT use increases the risk of exposure. Therefore, continuous investment in updating, upgrading, or replacing legacy systems for a more user-friendly security system is necessary to ensure that non-technical users of HIS can use HIT and HIS more easily (Yang et al., 2016). Increasing the CIA of PHI and PII is directly impacted by the users' feeling of the necessity of the system and their confidence to use the system with ease (Yang et al.,2016).

The framework has also incorporated an evaluation step focusing on rewarding and recognising staff compliant with information security practices. This evaluation is an excellent way of helping health executives understand what is still missing and what can be done next to improve security knowledge and awareness amongst staff. Rewards were highlighted by Ifinedo (2012) as an extrinsic motivator for an individual to facilitate a recommended behaviour. Rewards and recognition often boost behavioural intention to comply with information security practices.

[26] A risk appetite is the amount and type of risk an organisation is willing to take (Institute of Risk Management, n.d).

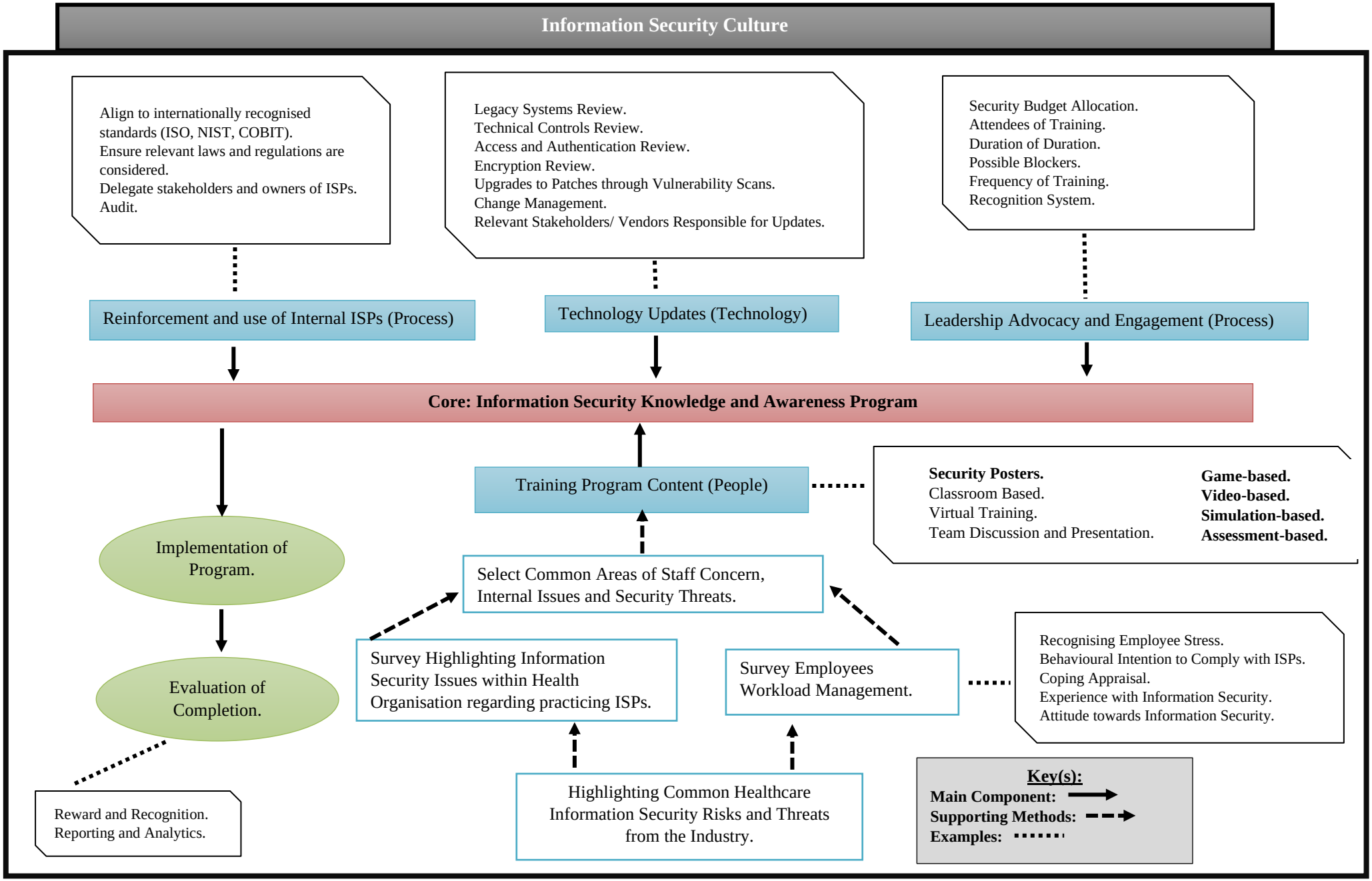

Figure 3 - Information Security Knowledge and Awareness Program Implementation Framework

6 DISCUSSION AND FINDINGS

6.1 CHAPTER OVERVIEW

This study is one of many seeking to understand health professionals' behavioural intentions and interactions when dealing or interacting with information security practices. It explored what interactions took place, highlighted their behaviours, and sought to find and understand the circumstances health professionals faced to influence such behaviours. As per the terminology used by Braun and Clarke (2006), the 45 research studies reviewed formed the data corpus subjected to thematic analysis.

The study reviewed 45 pieces of literature from 2017 to 2023 to ensure relevancy and highlight health professionals' most recent information security interactions. The five-year literature review period was also the period of the COVID-19 pandemic. The following chapter will present the findings alongside the three cybersecurity dimensions of *People, Process and Technology*.

Past research has focused on the behavioural aspect of information security and their compliance towards ISPs. The findings from this literature review are also consistent with past studies as it has identified the types of behaviour such as perceived severity, self-efficacy, and behavioural intention to comply with ISPs and interact with information security practices accordingly (Yeng et al., 2019a; Yeng et al., 2021b; Coventry et al., 2020; Ali et al., 2021). The current study suggests that the *People* and *Process* dimensions of *information security knowledge and awareness, workload management and ISC* are most relevant to health professionals' interactions with information security. As demonstrated in Appendix B, 19 publications out of 45 publications were related to the *People* dimension, and 13 publications out of 45 publications were related to the Process dimension, making it a total of 32 publications identifying impacts of *information security knowledge and awareness, workload management and ISC.*

Overall, the literature review demonstrated a common conclusion: The healthcare industry needs to be prepared, as staff are continuously overworked, understaffed, and undervalued (reference will be helpful). Health organisations are patient-centric and, therefore, prioritise the services given to patients; therefore, investments are made to increase patient satisfaction; however, in doing so, health leaders have failed to recognise the importance of investments in security training and inadequately allocate budgets impacting the staff's ability to detect and respond to cyber threats and attacks.

His study also identified that while behavioural intention may have caused specific information security practices, social cues and environmental factors also played a role. The overall nature of the health industry makes it patient-centric, which has implications for information security. For example, this study has found that while attending to and switching between patients, it was common amongst health practitioners to share passwords and credentials and exchange and share information via unencrypted devices, USB sticks and unencrypted communication applications. Other concerning behaviours highlighted in this study included:

- Writing down passwords in insecure and accessible locations.
- Unknowingly clicking on embedded email links (e.g., phishing attachments);
- Utilising sticky notes for recording of patient information, passwords and tasks;
- Leaving computers logged in and unattended when tending to patients;
- Failing to report security incidents as they occur;
- Patient information is not encrypted, whether stored or transmitted in personal or work devices;
- Unauthorised access to patient information (e.g., celebrity patient);
- Improper use of ISPs;

- Utilising shared workstations;
- Lack of access controls to connected medical devices or EHR systems;

Each behaviour was grouped into one of the following factors, which served as the overarching sub-theme to understanding where each behaviour fell into, and this was noted to be the overall findings of the study:

- Lack of Information Security Knowledge and Awareness;
- Struggles with Workload Management;
- Weak Information Security Culture;
- Lack of Access and Authentication Controls;
- Lack of Data Backup; and
- Lack of Encryption Controls.

Past studies have also made similar observations. For example, Tarkarji (2020) noted the sharing of passwords and credentials for convenience, and other studies have also found this to be very common (Martin et al., 2017; Coventry et al., 2020; Yeng et al., 2021a; Wei & Courtney, 2018). Martin et al. (2017) noted the same security behaviour amongst health professionals, in which such behaviour was seen as a practice that 'made sense' under the conditions of the healthcare environment. This demonstrated a lack of password management, and if unauthorised personnel were to retrieve a password that was unintentionally shared with them, the PHI and PII of a patient could be modified and disclosed to unauthorised external parties.

6.2 PEOPLE AND PROCESS FINDINGS

The healthcare industry was the only industry in which insider threats were most common, reporting that 56% of its cyber threats were due to human error and abuse of access to HIS[27] in 2018 (Verizon, 2018). Healthcare professionals must understand the consequences of unauthorised access, modification, or use of sensitive medical information. Without the proper guidance of healthcare executives, many healthcare professionals unknowingly become a threat to patient's privacy.

The *Process* dimension focuses on growing the *ISC* and reinforcing the ISPs'. It calls for more leadership engagement and security advocacy to drive the *People* dimension forward. Leadership engagement is critical in the health industry. This is because leadership reinforces the importance of security issues and should set a clear expectation for staff to follow. Strengthening security awareness through the guidelines and the use of ISPs should be brought about first at the leadership level and only secondly at the staff level (Karaz & Kollar, 2020). Healthcare leadership and advocacy for information security highly influence healthcare information security behaviour. This, in turn, has impacted how healthcare professionals choose to interact with information security practices. Li et al. (2019) study indicated that an individual's awareness depends on the leadership's ability to inform them accordingly regarding ISPs; however, the stress to implement better information security awareness training and programs in the healthcare industry is more complex than suggested. Budget allocation was the most significant influence on why information security was not considered a priority (provide a reference).

While *workload management* was another notable factor, it was the 'excuse' for health professionals to ignore information security guidelines. The utilisation of unencrypted USB sticks, sticky notes pasted to a secure and easily accessible location, and leaving computers logged for the convenience of coming back to patient information 'faster' all fell under the *People* dimension and was a result of a lack of

[27] Verizon's Data Breach Investigation Report (DBIR) details authoritative and comprehensive information regarding data breaches and cyber incidents worldwide. The assessment analyses over 16,000 security incidents and over 5,000 confirmed data breaches across six continents and 20 industries. *Please refer to Verizon for further details regarding the DBIR reports: https://www.verizon.com/business/resources/reports/. Accessed October 2023.*

security knowledge and awareness (Coventry et al., 2020; Wei & Courtney, 2018; Kellog et al., 2017; Jalali et al., 2020; Priestman et al., 2019; Farah et al., 2022).

Health professionals performed such behaviours without perceiving the severity of the implications that could come about if patient information was disclosed to unauthorised personnel. Healthcare professionals often share credentials and USBs containing PII and other sensitive information to avoid piles of workload and unnecessary stress. It was found to be a common practice due to the convenience of the activity; however, it contradicts ISP procedures and policies when handling information. Many healthcare professionals need a more fundamental understanding when practising information security, thus making it less of a priority in their day-to-day tasks. A few case studies pinpointed that there may be a correlation between workload stress and the interaction with information security practices. There are also contradictory conclusions regarding workload stress. In some cases, workload was not a perceived barrier to implementing and complying with information security practices (Yeng et al., 2022), indicating that workload may not contribute to the interactions with information security. Therefore, the relationship between healthcare information security practices and workplace stress needs more research.

6.3 TECHNOLOGY FINDINGS

Technology was deemed the healthcare industry's most 'important' dimension. This is because technology is needed to keep up with demand. HIT offers numerous opportunities for improving and transforming healthcare and helps health practitioners provide more seamless decisions and support for patients (Alotaibi & Federico, 2017). Implementing the latest HIT and upgrading interconnected medical devices is also necessary to keep up with services and demands. However, this also proved to have its shortcomings as lack of access and authentication controls and data backup demonstrated to be concerning factors to the dimension (Boddy et al., 2018; Coventry & Branley, 2018; Coventry et al., 2020; Nifakos et al., 2021; Erceg, 2019). According to HIPAA, two of the most critical controls, *access, and authentication,* focus on protecting the CIA of PHI and PII. Such controls must be carefully considered to protect patient records and HIS. The lack thereof could cause PHI to be compromised, modified incorrectly, and otherwise disclosed to unauthorised parties. The study found that while integrated and interconnected medical devices were continuously looked into and upgraded for better patient service efficiency, access and authentication controls remained a failure as staff were able to bypass authenticated communication channels and utilised insecure communication platforms such as SMS and WhatsApp to share unencrypted patient information and photos (Christiansen et al., 2017; Boddy et al., 2018; Wani et al., 2022). Lack of technical controls results from weak *ISC* and lack of reinforcement of ISPs to better equip health information teams with the knowledge, skills, and guidance to implement and frequently review *access and authentication* controls to ensure unauthorised access was continuously looked at to avoid malicious activities. Moreover, patient records become more easily accessible and unprotected during transmission and storage in which patient information is disclosed through unencrypted personal and work devices, which could impact PHI's confidentiality and availability (Anmulwar et al., 2020). This demonstrated the relationship across all three dimensions in which health professionals need to be trained (*People* dimension) and reinforcements of ISPs for technological advancements need to be more invested in (*Process* dimension) for the improvement and maintenance of technical upgrades (*Technology* dimension). As a result, the incentive to have leadership engage, financially advocate, and train healthcare professionals, even if effective, may need to be more motivational to drive and change how healthcare professionals interact with information security.

Overall, the study found that information security knowledge and awareness sit at the core of *ISC* and influence *workload management, access and authentication, data backup and encryption,* as demonstrated in **Figure 4**. The study found that a lack of security knowledge and awareness influenced four behavioural interactions (B03, B04, B07 and B11). *Information security knowledge and awareness* are core to the factor of *ISC* because this is what information security knowledge and awareness fosters

an organisation's preparation to detect and respond to internal and external threats such as social engineering (Yasar & Pratt, 2021). In addition, *ISC* emerges in how health professionals behave towards information security (Martins & Elofe, 2002). *ISC* is driven through the reinforcement of ISPs when training and increasing security awareness amongst employees. The core aspects of *ISC* also include *workload management*, which seeks to understand how health professionals manage workload while trying to practice information security safely. The next is access and authentication management, which aims to understand how health professionals protect PHI and PII from being disclosed to unauthorised users of HIS. The final two of data backup and encryption often go hand-in-hand as you would need to encrypt data before and after backup. This ensures no modification to the patient information being stored, transmitted, or used. Each aspect falls under *ISC* and is fostered through information security knowledge and awareness.

Employees must understand the implications of failing to interact securely with information. Carelessness demonstrated within the findings, such as sharing passwords, unencrypted USB sticks, accessing patient information, failing to back up critical information, and failing to understand the implication of sharing information over unencrypted platforms, are all interactions influenced by the lack of security knowledge and awareness. Behavioural intentions to carry information security practices in a high-intensity environment, much like a healthcare facility, often becomes second nature to ensure the primary goal of tending to patients comes first; however, it is found that health professionals need to understand that information security focuses on a much broader aspect than protecting PHI and PII of patients within HIS but is fundamental to patient safety, privacy and protecting the trust built between a health professional and patient (Martin et al., 2017).

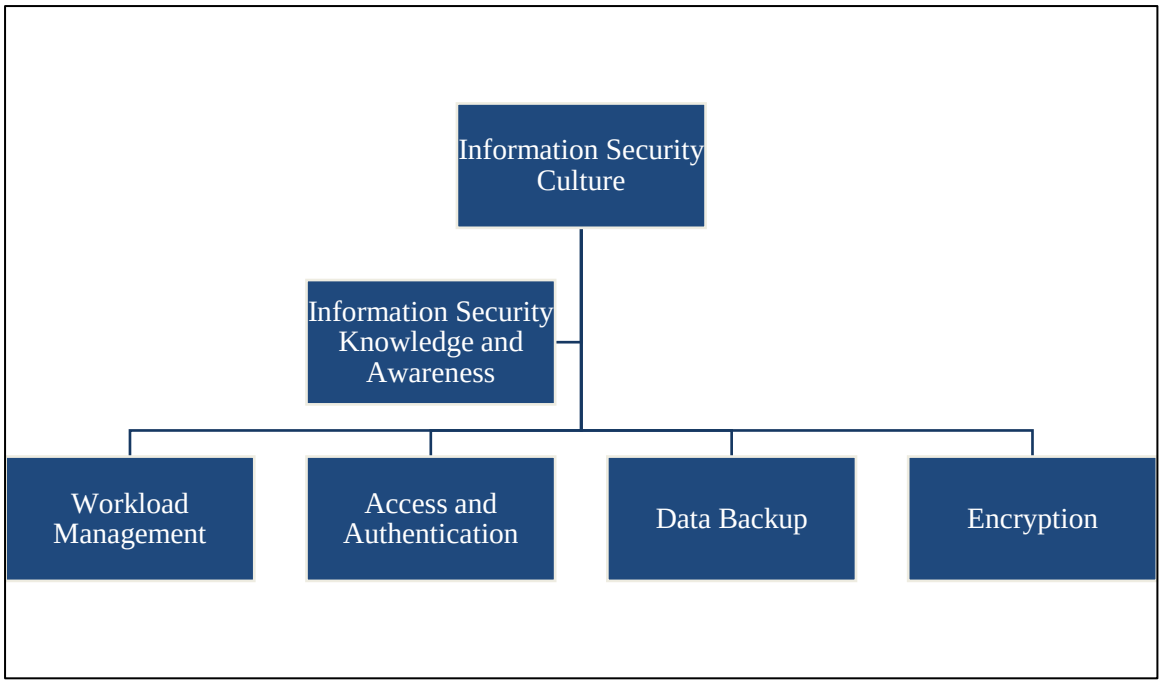

Figure 4 - The Influence of Information Security Knowledge and Awareness

To conclude, this research considered several notable limitations when interpreting conclusions drawn from the selected pieces of literature from the years 2017 to 2023.

Firstly, the focus on information security practices within a highly intensive and stressful environment, much like healthcare organisations, creates a bias that insinuates that healthcare professionals do not care for information security practices due to the nature of the environment in which workload management and information security practices need to be done simultaneously. Much past research, including this one, did not assess information security practices in a live environment and relied heavily

on conclusions made in past research and surveys that concluded the opinions of professionals who already knew information security practices. This limits the opportunity to seek and observe first-hand what information security behaviour in the healthcare industry looks like. Undertaking such approaches in which surveys are provided or a literature review is conducted to expand an existing body of work further limits the potential to fully comprehend and understand two critical themes identified within this research: workplace dynamics and individual drive and commitment.

Understanding that the factor *ISC* is a critical component of the process dimension and has often driven the course of an organisation's security awareness and posture, the study did not assess the *ISC* of health organisations, and it can be pretty difficult to assess what is a 'good *ISC'* in an organisation as every organisation, healthcare based or not, is different depending on their security posture and prioritisation of information security. Although the study did highlight indications of *ISC*, they were made applicable through the review of past research. *ISC* is purely process-influenced, which needs the guidance and support of organisational leadership. The cases of executive interactions highlighted within the study relating to information security practices and their teams were limited. Therefore, it is hard to tell whether leadership directly impacts employee interactions with information security practices despite previous research indicating that it does. It is important to note that while it does not clearly outline interactions, fostering and advocating an information security culture creates awareness to increase better practices, which was notably the most important outcome of all the literature.

This study has proposed a combination of the CIS controls and HIPAA controls that could be utilised to address the behaviours found in the study; however, future research in a live environment would need to be completed to ensure such security controls are, in fact, relevant and applicable to addressing the behaviours. An updated live environment assessment of security interactions of health organisations is required to ensure the study captures the interactions accurately. In addition, it has opened a newfound interest in understanding workload management more. Lastly, the study proposed an information security knowledge and awareness program implementation framework that could support health executives in aligning their culture with a more robust security training culture to drive the protection and privacy of patients whilst also recognising healing professionals' perceived threats and behavioural intentions. A study to further assess the framework would be required to ensure its applicability and relevance to the healthcare industry.

7 APPENDICES

Appendix A -Final Collection of Literature with Behavioural Themes

No.	Literature Title	Author(s)	Year	Database
1.	Identifying the Roles of Healthcare Leaders in HIT Implementation: A Scoping Review of the Quantitative and Qualitative Evidence.	Laukka, E; Huhtakangas, M; Heponiemi, T; Kanste, O	2020	MDPI
2.	A Comprehensive Assessment of Human Factors in Relation to Cybersecurity Compliance of Healthcare Staff in a Paperless Hospital	Yang, B; Fauzi, M; Yeng, P;	2022	MDPI
3.	Framework for Healthcare Security Practice Analysis, Modeling, and Incentivization	Yeng, P; Yang, B; Snekkenes, E	2019	ResearchGate
4.	The Determinants of an Information Security Policy Compliance Culture in Organisations: The Combined Effects of Organisational and Behavioural Factors	Amankwa, E; Loock, M; Kritzinger, E;	2022	Emerald Insight
5.	Information Security Behaviour in Health Information Systems: A Review of Research Trends and Antecedent Factors	Sari, P; Hundayani, P; Hidayanto, A; Yazid, S; Aji, R;	2022	MDPI
6.	Indirect Effect of Management Support Users' Compliance Behaviour Towards Information Security Policies	Humaidi, N; Balakrishnan, V;	2019	Sage Journals
7.	Mapping the Psychosocial Cultural Aspects of Healthcare Professionals' Information Security Practices: Systematic Mapping Study	Yeng, P; Szekeres, A; Yang, B; Snekkenes, E	2019	JMIR Publications
8.	Healthcare Staff's Information Security Practices Towards Mitigating Data Breaches	Yeng, P; Yang, B; Snekkenes, E	2019	Google Books
9.	Examining the Link Between Stress Levels and Cybersecurity Practices of Hospital Staff in Indonesia	Rachmayani, D; Fauzi, M; Yeng, P; Yang, B;	2021	Association for Computing Machinery (ACM)
10.	Influence of Human Factors on Cybersecurity within Healthcare Organisations: A Systematic Review	Nifakos, S; Changdramouli, K; Nikolaou, C; Papachristou, P; Koch, S; Panaousis, E; Bonacina, S;	2021	MDPI
11.	Cyber-Risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour	Coventry, L; Branley, D; Sillence, E; Magalini, S; Mari,	2020	SpringerLink

		P; Magkanaraki, A; Anastaopoulou, K;		
12.	Information Security: Threat from Employees	Erceg, A;	2019	IGI Global
13.	Evaluating Cybersecurity Attitudes and Behaviours in Portuguese Healthcare Institutions	Nunes, P; Antunes, M; Silva, C;	2021	ScienceDirect
14.	Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks	Argaw, S; Troncoso, J; Lacey, D; Florin, M; Calcavecchia, F; Anderson, D; Burleson, W; Vogel, J; O'Leary, C; Eshaya-Chauvin, B; Flahault, A;	2020	SpringerLink
15.	Healthcare Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review	He, Y; Aliyu, A; Evans, M; Luo, C;	2021	JMIR Publications
16.	Resilience in Healthcare Systems: Cybersecurity and Digital Transformation	Garcia-Perez, A; Cegarra-Navarro, J; Sallos, M; Martinez-Caro, E; Chinnaswamy, A	2023	ScienceDirect
17.	Defining the Boundaries and Operational Concepts of Resilience in the Resilience in Healthcare Research Program	Wiig, S; Billett, S; Canfield, C; Roise, Ol Nja, O; Guise, V; Haraldseid-Driftland, C; Ree, E; Anderson, J; Macrae, C	2020	SpringerLink
18.	The Effect of Patient-Centeredness on Nures' Security Policy Compliance	Tazkarji, M;	2020	ResearchGate
19.	Cybersecurity in Hospitals: A Systematic, Organisational Perspective	Kaiser, J; Jalali, M;	2018	JMIR Publications
20.	Why Employees (Still) Click on Phishing Links: Investigation in Hospitals	Jalali, M; Bruches, M; Westmattelman, D; Schewe, G;	2020	JMIR Publications
21.	Precision Health Data: Requirements, Challenges and Existing Techniques	Thapa, C; Camtepe, S;	2021	ScienceDirect
22.	Cybersecurity: Ensuring Confidentiality, Integrity, and Availability of Information	Kim, L;	2022	SpringerLink
23.	Cybersecurity and Healthcare	Martin, G; Martin, P; Hankin, C; Darzi, A; Kinross, J	2017	British Medical Journal Publications
24.	Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward	Coventry, L; Branley, D;	2018	ScienceDirect

25.	Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends	Javaid, M; Haleem, A; Singh, R; Suman, R;	2023	ScienceDirect
26.	Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach	Pollini, A; Callari, T; Tedeschi, A; Ruscio, D; Save, L; Chiarugi, F; Guerri, D;	2021	SpringerLink
27.	Phishing in Healthcare Organisations: Threats, Mitigation and Approaches	Priestman, W; Anstis, T; Sebire, I; Sridharan, S; Sebire, N	2019	National Library of Medicine
28.	EHR Usability: Get it Right from the Start	Kellogg, K; Fairbanks, R; Ratwani, R	2017	Association for the Advancement of Medical Instrumentation (AAMI)
29.	Data Protection in Healthcare Research: Medical Students' Knowledge and Behaviour	Farah, M; Helou, S; Tufenkji, P; Helou, E	2022	Google Books
30.	Challenges of IoT in Healthcare	Anmulwar, S; Gupta, A; Derawi, M	2020	SpringerLink
31.	A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures	Gioulekas, F. Stamatiadis, E.; Tzikas, A.; Gounaris, K.; Georgiadou, A.; Michalitsi-Psarrou, A.; Doukas, G.; Kontoulis, M.; Nikoloudakis, Y; Marin, S.	2022	MDPI
32.	Establishing Situational Awareness for Securing Healthcare Patient Records	Boddy, A; Hurst, W; Mackay, M; Rhalibi, A	2018	LJMU Research Online
33.	Theory-Based and Prediction Analysis of Information Security Compliance Behaviour in the Saudi Healthcare Sector	Alanazi, S; Anbar, M; Ebad, S; Karuppayah, S; Al-Ani, H;	2020	MDPI
34.	Nursing Information Flow in Long-Term Care Facilities	Wei, Q; Courtney, K;	2018	National Library of Medicine
35.	Artificial Intelligence in Healthcare: An Essential for Health Leaders	Chen, M; Decary, M;	2020	Sage Journals
36.	Shared Electronic Health Record Systems: Key Legal and Security Challenges	Christiansen, E; Skipenes, E; Iversen, M;	2017	Sage Journals
37.	A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defences	Newaz, A; Sikder, A; Rahman, M; Ulugac, A;	2021	Association for Computing Machinery (ACM)

38.	Evaluation of Secure Messaging Applications for a Healthcare System: A Case Study	Liu, X; Sutton, P; McKenna, R; Sinanan, M; Fellner, B; Leu, M; Ewell, C	2019	National Library of Medicine
39.	The Challenges of Cybersecurity in Healthcare: The UK National Health Service as a Case Study	Grass, E; Ghafur, S; Jennings, N; Darzi, A;	2019	The Lancet
40.	Information Security Cultural Differences Among Healthcare Facilities in Indonesia	Sari, P; Prasetio, A; Candiwan; Handayani, P; Hidayanto, A; Syauqina, S; Astuti, E; Talleli, F;	2021	ScienceDirect
41.	Identification of Factors Influencing the Adoption of Health Information Technology by Nurses Who Are Digitally Lagging: In-Depth Interview Study	Leeuw, J; Woltjer, H; Kool, R;	2019	JMIR Publications
42.	Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends	Kruse, C; Frederick, B; Jacobson, T; Monticone, D	2017	IOS Press
43.	Security Techniques for Electronic Health Records	Kruse, C; Smith, B; Vanderlinden, H; Nealand, A;	2017	SpringerLink
44.	Addressing Challenges in the Development of Health Information Systems in The Gambia	Lin, R; Kujabi, B;	2022	ScienceDirect
45.	BYOD Usage and Security Behaviour of Hospital Clinical Staff: An Australian Survey	Wani, T; Mendoza, A; Gray, K; Smolenaers, F;	2022	ScienceDirect

Appendix B – Thematic Analysis of Behavioural Interactions

No.	Literature Title	Author(s)	Key Idea of Literature	Applicable Behavioural ID	Factor Impacted	Dimension Impacted	Notable Mentions
1.	Identifying the Roles of Healthcare Leaders in HIT Implementation: A Scoping Review of the Quantitative and Qualitative Evidence.	Laukka, E; Huhtakangas, M; Heponiemi, T; Kanste, O	HIT, Implementation, Healthcare, Leader	B01	ISC	Process.	N/A.
2.	A Comprehensive Assessment of Human Factors in Relation to Cybersecurity Compliance of Healthcare Staff in a Paperless Hospital	Yang, B; Fauzi, M; Yeng, P;	Security Practice, Healthcare, Information Security Attitude, Security Knowledge, Security Behaviour, Security Compliance, Work Factors.	B02	Workload Management.	People.	Information Security Knowledge and Awareness.
3.	Framework for Healthcare Security Practice Analysis, Modeling, and Incentivization	Yeng, P; Yang, B; Snekkenes, E	Healthcare Staff, Information Security, Psycho-social-cultural, ISP, Information Security Awareness.	B11	Information Security Knowledge and Awareness.	People.	ISC.
4.	The Determinants of an Information Security Policy Compliance Culture in	Amankwa, E; Loock, M; Kritzinger, E;	ISP, Compliance Culture,	B13	ISC	Process	N/A

	Organisations: The Combined Effects of Organisational and Behavioural Factors		Organisational factors, Behavioural Factors.				
5.	Information Security Behaviour in Health Information Systems: A Review of Research Trends and Antecedent Factors	Sari, P; Hundayani, P; Hidayanto, A; Yazid, S; Aji, R;	Information Security Behaviour, Antecedent Factor, HIS, ISP.	B11	Information Security Knowledge and Awareness.	People.	ISC.
6.	Indirect Effect of Management Support Users' Compliance Behaviour Towards Information Security Policies	Humaidi, N; Balakrishnan, V;	Information Management, Information Security, Organisation, Motivation, Organisational Management, Health Information Management, Data Security, Information Protection, ISP.	B13	ISC	Process	Information Security Knowledge and Awareness.
7.	Mapping the Psychosocial Cultural Aspects of Healthcare Professionals' Information Security Practices: Systematic Mapping Study	Yeng, P; Szekeres, A; Yang, B; Snekkenes, E	Psycho-social-cultural, Healthcare Professionals, Data Breaches, PMT, TPB, SCT, Health Belief Model.	B16	Data Backup	Technology	Information Security Knowledge and Awareness. ISC.
8.	Healthcare Staff's Information Security Practices Towards Mitigating Data Breaches	Yeng, P; Yang, B; Snekkenes, E	Data Breaches, Social-Cultural,	B15	Access and Authentication Controls	Technology	N/A.

			Access Control Management, Access Control Systems, Information Privacy, Information Security.				
9.	Examining the Link Between Stress Levels and Cybersecurity Practices of Hospital Staff in Indonesia	Rachmayani, D; Fauzi, M; Yeng, P; Yang, B;	Cybersecurity Practices, Behaviour, Stress Management, Workload Management, Phishing, Hospital Staff.	B03	Information Security Knowledge and Awareness.	People	Workload Management.
10.	Influence of Human Factors on Cybersecurity within Healthcare Organisations: A Systematic Review	Nifakos, S; Changdramouli, K; Nikolaou, C; Papachristou, P; Koch, S; Panaousis, E; Bonacina, S;	Information Security Training, Cyber Risk Assessment, and Cybersecurity Awareness.	B15	Information Security Knowledge and Awareness.	People	Access and Authentication Controls
11.	Cyber-Risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour	Coventry, L; Branley, D; Sillence, E; Magalini, S; Mari, P; Magkanaraki, A; Anastaopoulou, K;	Cybersecurity Behaviour, Healthcare, Behavioural Change, Lack of Awareness, Workload Management, Security Attitude.	B05	Workload Management	People	Information Security Knowledge and Awareness.

12.	Information Security: Threat from Employees	Erceg, A;	Business Data, Information Security, Passwords, Data Backup, Security Risk.	B16	Data Backup	Technology	Information Security Knowledge and Awareness.
13.	Evaluating Cybersecurity Attitudes and Behaviours in Portuguese Healthcare Institutions	Nunes, P; Antunes, M; Silva, C;	Information Security Practices, Security Awareness, Security Behaviour.	B06	Workload Management	People	Information Security Knowledge and Awareness.
14.	Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks	Argaw, S; Troncoso, J; Lacey, D; Florin, M; Calcavecchia, F; Anderson, D; Burleson, W; Vogel, J; O'Leary, C; Eshaya-Chauvin, B; Flahault, A;	Security Incidents, Reporting Incidents, Incident Response, and Business Continuity Plans.	B07	Information Security Knowledge and Awareness.	People	N/A
15.	Healthcare Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review	He, Y; Aliyu, A; Evans, M; Luo, C;	Security Incidents, Cybersecurity Challenges, Phishing, Ransomware, Distributed Denial of Service Attacks, Malware.	B07	Information Security Knowledge and Awareness.	People	N/A

16.	Resilience in Healthcare Systems: Cybersecurity and Digital Transformation	Garcia-Perez, A; Cegarra-Navarro, J; Sallos, M; Martinez-Caro, E; Chinnaswamy, A	Technology Adoption, Digital Transformation.	B01	ISC	Process	Information Security Knowledge and Awareness.
17.	Defining the Boundaries and Operational Concepts of Resilience in the Resilience in Healthcare Research Program	Wiig, S; Billett, S; Canfield, C; Roise, Ol Nja, O; Guise, V; Haraldseid-Driftland, C; Ree, E; Anderson, J; Macrae, C	Digital Resilience, Digital Transformation, Technology Adoption.	B01	ISC	Process	Information Security Knowledge and Awareness.
18.	The Effect of Patient-Centeredness on Nures' Security Policy Compliance	Tazkarji, M;	Password Management, ISP, Password Sharing, EMR.	B02	Workload Management	People	N/A
19.	Cybersecurity in Hospitals: A Systematic, Organisational Perspective	Kaiser, J; Jalali, M;	Organisational Models, Cybersecurity, Computer Simulation, Cybersecurity Capabilities, Health Organisations.	B13	ISC	Process	N/A
20.	Why Employees (Still) Click on Phishing Links: Investigation in Hospitals	Jalali, M; Bruches, M; Westmattelman, D; Schewe, G;	Information Security Management, Phishing Emails,	B03	Information Security Knowledge and Awareness	People	N/A

			Compliance, TPB.				
21.	Precision Health Data: Requirements, Challenges and Existing Techniques	Thapa, C; Camtepe, S;	Access and Authentication, Security, Privacy, Precision Health.	B10	Access And Authentication Controls	Technology	N/A
22.	Cybersecurity: Ensuring Confidentiality, Integrity, and Availability of Information	Kim, L;	CIA Triad, HIPAA, NIST, Cybersecurity Hygiene, Frameworks, Exploits, Security Awareness.	B10	Access And Authentication Controls	Technology	Information Security Knowledge and Awareness.
23.	Cybersecurity and Healthcare: How Safe Are We?	Martin, G; Martin, P; Hankin, C; Darzi, A; Kinross, J	ISP, Password Management, Password Sharing, Credential Sharing.	B02	Workload Management	People	ISC
24.	Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward	Coventry, L; Branley, D;	Access Controls, EHR, Medical Devices, Organisational Processes.	B15	Access and Authentication Controls	Technology	ISC
25.	Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends	Javaid, M; Haleem, A; Singh, R; Suman, R;	Credential Sharing, USB Sharing, Phishing Scams, Email Use.	B04	Information Security Knowledge and Awareness	People	Access and Authentication Controls.

26.	Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach	Pollini, A; Callari, T; Tedeschi, A; Ruscio, D; Save, L; Chiarugi, F; Guerri, D;	Technology Adoption, Encryption, CIS, Cybersecurity Culture, Security Awareness, Human Factors.	B08	Encryption	Technology	Information Security Knowledge and Awareness. ISC.
27.	Phishing in Healthcare Organisations: Threats, Mitigation and Approaches	Priestman, W; Anstis, T; Sebire, I; Sridharan, S; Sebire, N	Phishing, Scams, Embedded Emails, Malicious Links, Attachments, IT Policies, ISP, Information Security Awareness, Threat Awareness.	B03	Information Security Knowledge and Awareness	People	ISC.
28.	EHR Usability: Get it Right from the Start	Kellogg, K; Fairbanks, R; Ratwani, R	Human Factors, EHR Usability, Sticky Notes, Posted Notes, Information Sharing.	B05	Workload Management	People	Information Security Knowledge and Awareness.
29.	Data Protection in Healthcare Research: Medical Students' Knowledge and Behaviour	Farah, M; Helou, S; Tufenkji, P; Helou, E	Data Protection, PHI, ISP, Password Management.	B17	Workload Management	People	Information Security Knowledge and Awareness.
30.	Challenges of IoT in Healthcare	Anmulwar, S; Gupta, A; Derawi, M	Encryption, Data Security, Data Protection,	B08	Encryption	Technology	N/A

			Data Flow, Data Privacy.				
31.	A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures	Gioulekas, F. Stamatiadis, E.; Tzikas, A.; Gounaris, K.; Georgiadou, A.; Michalitsi-Psarrou, A.; Doukas, G.; Kontoulis, M.; Nikoloudakis, Y; Marin, S.	Cybersecurity Culture, Security Assessment, Security Awareness.	B09	ISC	Process	N/A
32.	Establishing Situational Awareness for Securing Healthcare Patient Records	Boddy, A; Hurst, W; Mackay, M; Rhalibi, A	Security Awareness, Access Management, CIA Triad, Data Access.	B11	Information Security Knowledge and Awareness	People	ISC
33.	Theory-Based Model and Prediction Analysis of Information Security Compliance Behaviour in the Saudi Healthcare Sector	Alanazi, S; Anbar, M; Ebad, S; Karuppayah, S; Al-Ani, H;	Behavioural Theory, HIS, Information Security, Compliance Behaviour, ISP.	B11	Information Security Knowledge and Awareness	People	ISC
34.	Nursing Information Flow in Long-Term Care Facilities	Wei, Q; Courtney, K;	EHR, Workstations, Shared Resources, Workload Management.	B14	Workload Management	People	N/A
35.	Artificial Intelligence in Healthcare: An Essential for Health Leaders	Chen, M; Decary, M;	Artificial Intelligence, Digital Transformation.	B01	ISC	Process	N/A

36.	Shared Electronic Health Record Systems: Key Legal and Security Challenges	Christiansen, E; Skipenes, E; Iversen, M;	Access Management, EHR Protection, Security Challenges.	B15	Access and Authentication Controls.	Technology	N/A
37.	A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defences	Newaz, A; Sikder, A; Rahman, M; Ulugac, A;	Access Management, Authentication, Access Logs.	B15	Access and Authentication Controls.	Technology	N/A
38.	Evaluation of Secure Messaging Applications for a Healthcare System: A Case Study	Liu, X; Sutton, P; McKenna, R; Sinanan, M; Fellner, B; Leu, M; Ewell, C	HIPAA, PHI, PII, Security Privacy, Information Security, Messaging Applications,	B12	Access and Authentication Controls.	Technology	N/A
39.	The Challenges of Cybersecurity in Healthcare: The UK National Health Service as a Case Study	Grass, E; Ghafur, S; Jennings, N; Darzi, A;	Budget Allocation, Healthcare Organisations.	B13	ISC	Process	N/A
40.	Information Security Cultural Differences Among Healthcare Facilities in Indonesia	Sari, P; Prasetio, A; Candiwan; Handayani, P; Hidayanto, A; Syauqina, S; Astuti, E; Talleli, F;	Health Information Management, HIS, ISC, Healthcare Facilities, Healthcare.	B13	ISC	Process	N/A
41.	Identification of Factors Influencing the Adoption of Health Information Technology by Nurses Who Are Digitally Lagging: In-Depth Interview Study	Leeuw, J; Woltjer, H; Kool, R;	Technology Adoption, Digital Adoption, HIS, Professional Competence.	B01	ISC	Process	N/A

42.	Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends	Kruse, C; Frederick, B; Jacobson, T; Monticone, D	Technology Adoption and implementation Support.	B01	ISC	Process	N/A
43.	Security Techniques for the Electronic Health Records	Kruse, C; Smith, B; Vanderlinden, H; Nealand, A;	Access Management, Technology Adoption, EHR.	B12	Access and Authentication Controls.	Technology	N/A
44.	Addressing Challenges in the Development of Health Information Systems in The Gambia	Lin, R; Kujabi, B;	Information Management, Orgnaisational Security Culture.	B13	ISC	Process	N/A
45.	BYOD Usage and Security Behaviour of Hospital Clinical Staff: An Australian Survey	Wani, T; Mendoza, A; Gray, K; Smolenaers, F;	BYOD, Security Behaviour, Security Awareness, Privacy, Data Privacy, Patient Information.	B12	Access and Authentication Controls.	Technology	Information Security Knowledge and Awareness.

Appendix C - Databases

AAMI
ACM
British Medical Journal Publications
Emerald Insight
IOS Press
JMIR Publications
MDPI
National Library of Medicine
ResearchGate
ScienceDirect
SpringerLink
The Lancet

8 REFERENCES

Agarwal, R., & Anderson, C. (2010). Practising Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behaviour Intentions. *Management Information Systems Quarterly, 34*(3), 613-643. doi:https://doi.org/10.2307/25750694

Ahmed, Z., Ong, T., Liew, T., & Norhashim, M. (2019). Security Monitoring and Information Security Assurance Behaviour Among Employees. *Information & Computer Security, 27*(2), 165-188. doi:http://dx.doi.org/10.1108/ICS-10-2017-0073

Ajzen, I. (1991). The Theory of Planned Behaviour. *Organisational Behaviour and Human Decisions Processes, 50*(2), 179-211. doi:https://doi.org/10.1016/0749-5978(91)90020-T

Alanazi, S., Anbar, M., Ebad, S., Karuppayah, S., & Al-Ani, H. (2020). Theory-Based Model and Prediction Analysis of Information Security Compliance Behaviour in the Saudi Healthcare Sector. *Symmetry, 12*. doi:http://dx.doi.org/10.3390/sym12091544

Alawida, M., Omolara, A., Abiodun, O., & Al-Rajab, M. (2022). A Deeper Look into Cybersecurity Issues in the Wake of COVID-19: A Survey. *Journal of King Saud University - Computer and Information Sciences, 32*(10), 8176-8206. doi:https://doi.org/10.1016%2Fj.jksuci.2022.08.003

Ali, R., Dominic, P., Ali, S., Rehman, M., & Sohail, A. (2021). Information Security Behaviour and Information Security Policy Compliance: A Systematic Literature Review of Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences, 11*(8). doi:https://doi.org/10.3390/app11083383

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Information Security Policy Compliance: The Role of Information Security Awareness. *AMCIS 2012 Proceedings.* Retrieved from https://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/16

Alotaibi, Y., & Federico, F. (2017). The Impact of Health Information Technology on Patient Safety. *Saudi Medical Journal, 38*(12), 1173-1180. doi:https://doi.org/10.15537%2Fsmj.2017.12.20631

Alqahtani, F. (2017). Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science, 124*, 691-697. doi:https://doi.org/10.1016/j.procs.2017.12.206

Amankwa, E., Loock, M., & Kritzinger, E. (2022). The Determinants of an Information Security Policy Compliance Culture in Organisations: The Combined Effects of Organisational and Behavioural Factors. *Information and Computer Security, 30*(4), 683-614. doi:https://doi.org/10.1108/ICS-10-2021-0169

Anderson, V. (2022). *Top Management and Organisation Support for Information Security as Perceived by US Healthcare Employees: A Quantitative Study.* Capella University.

Anmulwar, S., Gupta, A., & Derawi, M. (2020). Challenges of IoT in Healthcare. *IoT and ICT for Healthcare Applications*, 11-20. doi:https://doi.org/10.1007/978-3-030-42934-8_2

Argaw, S., Bempong, N., Eshaya-Chauvin, B., & Flahault, A. (2019). The State of Research on Cyberattacks Against Hospitals and Available Best Practice Recommendations: A Scoping Review. *BMC Medical Informatics and Decision Making*, 1-11. doi:https://doi.org/10.1186/s12911-018-0724-5

Argaw, S., Troncoso, J., Lacey, D., Florin, M., Calcavecchia, F., Anderson, D., . . . Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the Challenges and Working Towards Mitigating the Risks. *BMC Medical Information and Decision Making, 20*(146). doi:https://link.springer.com/article/10.1186/s12911-020-01161-7

Asghar, R. (2021, June 2). *A Cyberattack Lesson from Waikato DHB*. Retrieved from NewsRoom: https://newsroom.co.nz/2021/06/20/a-cyberattack-lesson-from-waikato-dhb/

Baker, K. (2023, February 13). *10 Most Common Types of Cyber-Attacks*. Retrieved from CrowdStrike: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

Baldwin, M., Geib, J., Santos, B., Berry, D., & Kess, B. (2022, August 25). *Microsoft Threat Modeling Tool Threats - STRIDE Model*. Retrieved from Microsoft: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

Bandura, A. (1986). Differential Engagement of Self-Reactive Influences in Cognitive Motivation. *Organisational Behaviour and Human Decision Processes, 38*, 92-113.

Baz, M., Alhakami, H., Agrawal, A., Baz, A., & Khan, R. (2020). Impact of COVID-19 Pandemic: A Cybersecurity Perspective. *Intelligent Automation & Soft Computing, 27*(3), 641-652. doi:http://dx.doi.org/10.32604/iasc.2021.015845

Boddy, A., Hurst, W., Mackay, M., & Rhalibi, A. (2018). Establishing Situational Awareness for Securing Healthcare Patient Records. *The Tenth International Conference on eHealth, Telemedicine, and Social Medicine eTELEMED 2018.* Rome, Itlay. Retrieved from https://researchonline.ljmu.ac.uk/id/eprint/10038

Box, D., & Pottas, D. (2014). A Model for Information Security Compliant Behaviour in the Healthcare Context. *Procedia Technology, 16*, 1472-1470. doi:https://doi.org/10.1016/j.protcy.2014.10.166

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 77-101.

Brien, J., & Marakas, G. (2006). Management Information Systems. *6*, 102-117. Retrieved from https://dias.ac.in/wp-content/uploads/2020/06/102-112-Pages-of-DTR-8th-issue.pdf

CertNZ. (2022). *Cyber Change - Behavioural Insights for Being Secure Online.* Retrieved from Cert NZ: https://www.cert.govt.nz/assets/resources/cert-nz-cyber-change-behavioural-insights-2022-online-version.pdf

Chaturvedi, R., Chahravarthy, K., & Williams, C. (2020). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research*. doi:http://dx.doi.org/10.2196/23692

Chen, C., Shaw, R., & Yang, S. (2006). Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. *Information Technology, Learning, and Performance Journal, 24*.

Chen, M., & Decary, M. (2020). Artificial Intelligence in Healthcare: An Essential Guide for Health Leaders. *Healthcare Management Forum, 33*(1), 10-18. doi:https://doi.org/10.1177/0840470419873123

Chen, Y., Ramanurthy, K., & Wen, K.-W. (2012). Organisations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, 157-188.

Christiansen, E., Skipenes, E., & Iversen, M. (2017). Shared Electronic Health Record Systems: Key Legal and Security Challenges. *Journal of Diabetes Science and Technology, 11*(6). doi:https://doi.org/10.1177/1932296817709797

CIS. (n.d). *Election Security Spotlight - CIA Triad*. Retrieved from Centre for Internet Security: https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-cia-triad

CISA. (2021, May 20). *FBI Flash - Conti Ransomware Healthcare Networks.* Retrieved from Federal Bureau of Investigation, Cyber Division: https://www.cisa.gov/sites/default/files/Conti%20Ransomware%20Heathcare%20networks.pdf

Coventry, L., & Branley, D. (2018, July). Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward. (Elsevier, Ed.) *Maturitas, 113*, 48-52. doi:https://doi.org/10.1016/j.maturitas.2018.04.008

Coventry, L., Branley, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020). Cyber-Risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour. *HCI for Cybersecurity, Privacy, and Trust, 12210*, 105-122. doi:https://doi.org/10.1007/978-3-030-50309-3_8

Dalal, R., Howard, D., Bennett, R., Posey, C., Zaccaro, S., & Brummel, B. (2022). Organisational Science and Cybersecurity: Abundant Opportunities for Research at the Interface. *Journal of Business Psychology, 37*, 1-29. doi:https://doi.org/10.1007/s10869-021-09732-9

D'Arcy, J., & Teh, P.-L. (2019). Predicting Employee Information Security Policy Compliance on a Daily Basis: The Interplay of Security-Related Stress, Emotions, and Neutralisation. *Information & Management, 56*(7). doi:https://doi.org/10.1016/j.im.2019.02.006

Davis, F. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science, 35*(8), 982-1002.

Dong, K., Ali, R., Dominic, P., & Ali, S. (2021). The Effect of Organisation Information Security Climate on Information Security Policy Compliance: The Mediating Effect of Social Bonding towards Healthcare Nurses. *Sustainable Information Systems, 13*(5). doi:https://doi.org/10.3390/su13052800

Erceg, A. (2019). *Information Security: Threat from Employees* (Vol. 13). doi:https://doi.org/10.31803/tg-20180717222848

Farah, M., Helou, S., Tufenkji, P., & Helou, E. (2022). Data Protection in Healthcare Research: Medical Students' Knowledge and Behaviour. *Advances in Information, Management and Technology in Healthcare*.

Fink, A. (2005). *Conducting Research Literature Reviews: From the Internet to Paper* (2nd ed.). Thousand Oaks, California: Sage Publications.

Fischer, E. A. (2014). *Cybersecurity Issues and Challenges: In Brief.* Congressional Research Service. doi:https://a51.nl/sites/default/files/pdf/R43831.pdf

Garcia-Perez, A., Cegarra-Navarro, J., Sallos, M., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in Healthcare Systems: Cybersecurity and Digital Transformation. *Technovation, 121*. doi:https://doi.org/10.1016/j.technovation.2022.102583

Gioulekas, F. S., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., . . . Marin, S. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare, 10*(327). doi:https://doi.org/10.3390/healthcare10020327

Gordon, W., Fairhall, A., & Landman, A. (2017). Threats to Information Security - Public Health Implications. *The New England Journal of Medicine*. Retrieved from https://www.saudemaispublica.com/uploads/9/8/9/4/98944468/356355652-nejmp1707212.pdf

Gordon, W., Wright, A., Glynn, R., Kadakia, J., Mazzaone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a Mandatory Phishing Training Program for High-Risk Employees at a US Healthcare System. *Journal of the American Medical Informatics Association, 26*(6), 547-552. doi:https://doi.org/10.1093/jamia/ocz005

Grass, E., Ghafur, S., Jennings, N., & Darzi, A. (2019). The Challenges of Cybersecurity in Healthcare: The UK National Health Service as a Case Study. *The Lancet Digital Health, 1*(1), 10-12. doi:https://doi.org/10.1016/S2589-7500(19)30005-6

Grasseggar, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *Procedia Computer Science, 181*, 59-66. doi:https://doi.org/10.1016/j.procs.2021.01.103

Handayani, P., Hidayanto, A., & Sari, P. (2023). Demographic Comparison of Information Security Behaviour toward Health Information System Protection: Survey Study. *JMIR Formative Research, 7*. doi:https://doi.org/10.2196/49439

Harper, R. (2023, May 2). *Information Security Compliance: Addressing People, Processes, and Technology in Harmony*. Retrieved from ISMS: https://www.isms.online/information-security-management-system-isms/information-security-compliance-addressing-people-processes-and-technology-in-harmony/#:~:text=People%20refer%20to%20the%20employees,used%20to%20protect%20information%20assets.

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Healthcare Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal of Medical Internet Research, 23*(4). doi:http://dx.doi.org/10.2196/21747

Hedstrom, K., Kolkowska, E., Karlsson, F., & Allen, J. (2011). Value Conflicts for Information Security Management. *The Journal of Strategic Information Systems, 20*(4), 373-384. doi:https://doi.org/10.1016/j.jsis.2011.06.001

Hochbaum, G., Rosenstock, I., & Kegels, S. (1952). Health Belief Model. *United States Public Health Services*, 1.

Hone, K., & Eloff, J. (2022). Information Security Policy - What do International Information Security Standards Say? *Computers & Security, 21*(5), 402-409. doi:https://doi.org/10.1016/S0167-4048(02)00504-7

Hsu, C., Lee, M., & Su, C. (2013). The Role of Privacy Protection in Healthcare Information Systems Adoption. *Journal of Medical Systems, 37*. doi:https://doi.org/10.1007/s10916-013-9966-z

Hu, Q., Hart, P., & Cooke, D. (2006). The Role of External Influence on Organisational Information Security Practices: An Institutional Perspective. *Annual Hawaii International Conference on System Sciences (HICSS). 9.* Kauia: IEEE. doi:https://doi.org/10.1109/HICSS.2006.481

Humaidi, N., & Balakrishnan, V. (2015). The Moderating Effect of Working Experience on Health Information System Security Policies Compliance Behaviour. *Malaysian Journal of Computer Science, 28*(2).

Humaidi, N., & Balakrishnan, V. (2019). Indirect Effect of Management Support on Users' Compliance Behaviour Towards Information Security Policies. *Health Information Management Journal, 47*(1), 17-37. doi:https://doi.org/10.1177/1833358317700255

Humaidi, N., Balakrishnan, V., & Shahrom, M. (2014). Exploring Users' Compliance Behaviour Towards Health Information System Security Policies Based on Extended Health Belief Model. *2014 IEEE Conference on e-Learning, e-Management and e-Services*, (pp. 30-35). Victoria, Australia. doi:https://doi.org/10.1109/IC3e.2014.7081237

IBM. (2023a). *What is cybersecurity?* Retrieved from IBM: https://www.ibm.com/topics/cybersecurity

IBM. (2023b). *What is Information System?* Retrieved from IBM: https://www.ibm.com/topics/information-security

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behaviour and the Protection Motivation Theory. *Computers & Security, 31*(1), 83-95. doi:https://doi.org/10.1016/j.cose.2011.10.007

InPhySec. (2022, September 2). *Waikato District Health Board (WDHB) Incident Response Analysis.* Retrieved from Te Whatu Ora: https://www.tewhatuora.govt.nz/assets/Publications/Proactive-releases/WDHB-Final-Report-2.0-redacted.pdf

Institute of Medicine. (2009). Summary. In *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research* (pp. 1-5). Washington, DC: The National Academies Press.

Institute of Risk Management. (n.d). *Risk Appetite and Tolerance*. Retrieved from IRM: https://www.theirm.org/what-we-say/thought-leadership/risk-appetite-and-tolerance/

Jalali, M., & Kaiser, J. (2018). Cybersecurity in Hospitals: A Systematic, Organisational Perspective. *Journal of Medical Internet Research, 20*(5). doi:http://dx.doi.org/10.2196/10059

Jalali, M., Bruches, M., Westmattelman, D., & Schewe, G. (2020). *Why Employees (Still) Click on Phishing Links: Investigation in Hospitals* (Vol. 22). Journal of Medical Internet Research. doi:http://dx.doi.org/10.2196/16775

Javaid, M., Haleem, A., Singh, R., & Suman, R. (2023). Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends. *Cybersecurity and Applications, 1*. doi:https://doi.org/10.1016/j.csa.2023.100016

Johnson, A., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. B. (2011). Guide for Security-Focused Configuration Management of Information Systems. In N. I. (NIST), *NIST Special Publication 800-128* (pp. 2-99). NIST. doi:https://doi.org/10.6028/NIST.SP.800-128

Juniper. (2024). *What is IDS and IPS?* Retrieved from Juniper Networks: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html#:~:text=with%20IDS%2FIPS%3F-,Intrusion%20detection%20systems%20(IDS)%20and%20intrusion%20prevention%20systems%20(IPS,reporting%20them%20to%20security%20administrators.

Kadena, E., & Gupi, M. (2021). Human Factors in Cybersecurity: Risks and Impacts. *Security Science Journal, 2*(2). doi:10.37458/ssj.2.2.3

Kaiser, J., & Jalali, M. (2018). Cybersecurity in Hospitals: A Systematic, Organisational Perspective. *Journal of Medical Internet Research, 20*(5). doi:https://doi.org/10.2196/10059

Karaz, B., & Kollar, C. (2020). Leadership Responsibilities in Information Security Awareness Development. *Academic and Applied Research in Military and Public Management Science, 19*(2), 79-91. doi:https://doi.org/10.32565/aarms.2020.2.6

Kellogg, K., Fairbanks, R., & Ratwani, R. (2017). EHR Usability: Get It Right from the Start. *Biomedical Instrumentation & Technology*. Retrieved from https://watermark.silverchair.com/0899-8205-51_3_197.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAA1YwggNSBgkqhkiG9w0BBwagggNDMIIDPwIBADCCAzgGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMiIMiGIUk1kmpUGv9AgEQgIIDCTFKryno8BzEaYVWn4sks_Xn_oePmkRQcXNE

Keshta, I., & Odeh, A. (2021). Security and Privacy of Electronic Health Records: Concerns and Challenges. *Egyptian Informatics Journal, 22*(2), 177-183. doi:https://doi.org/10.1016/j.eij.2020.07.003

Khanra, S., Dhir, A., Islam, N., & Mantymaki, M. (2020). Big Data Analytics in Healthcare: A Systematic Literature Review. *Enterprise Information Systems, 14*(7), 878-912. doi:https://doi.org/10.1080/17517575.2020.1812005

Kim, L. (2022). Cybersecurity: Ensuring Confidentiality, Integrity, and Availability of Information. In U. Hübner, G. Mustata Wilson, M. T., & M. Ball, *Nursing Informatics. Health Informatics* (pp. 391-410). doi:https://doi.org/10.1007/978-3-030-91237-6_26

Kioskli, K., Fotis, T., & Mouratidis, H. (2021). The Landscape of Cybersecurity Vulnerabilities and Challenges in Healthcare: Security Standards and Paradigm Shift Recommendations. *Conference ARES: Availability, Reliability and Security* (pp. 1-9). New York: Association for Computing Machinery - ACM Digital Library. doi:https://doi.org/10.1145/3465481.3470033

Koloseni, D., Lee, C., & Gan, M.-L. (2019). Understanding Information Security Behaviours of Tanzanian Government Employees: A Health Belief Model Perspective. *International Journal of Technology and Human Interaction (IJTHI)*. doi:10.4018/IJTHI.2019010102

Konieczny, F., Trias, E., & Taylor, N. (2015). SEADE: Countering the Futility of Network Security. *Air & Space Power Journal*, 1-14. Retrieved from https://apps.dtic.mil/sti/pdfs/ADA624282.pdf

Kruse, C., Frederick, B., Jacobson, T., & Monticone, D. (2017a). Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends. *Technology and Healthcare*, 1-10. doi:10.3233/THC-161263

Kruse, C., Smith, B., Vanderlinden, H., & Nealand, A. (2017b). Security Techniques for the Electronic Health Records. *Journal of Medical Systems, 41*, 1-9. doi:https://doi.org/10.1007/s10916-017-0778-4

Laukka, E., Huhtakangas, M., Heponiemi, T., & Kanste, O. (2020). Identifying the Roles of Healthcare Leaders in HIT Implementation: A Scoping Review of the Quantitative and Qualitative Evidence. *International Journal of Environmental Research and Public Health, 17*(8). doi:https://doi.org/10.3390/ijerph17082865

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information Security Awareness and Behaviour: A Theory-Based Literature Review. *Management Research Review, 37*(12), 1049-1092. doi:https://doi.org/10.1108/MRR-04-2013-0085

Lee, E., & Seomun, G. (2021). Structural Model of the Healthcare Information Security Behaviour of Nurses Applying Protection Motivation Theory. *International Journal of Environmental Research and Public Health, 18*(4). doi:https://doi.org/10.3390/ijerph18042084

Leeuw, J., Woltjer, H., & Kool, R. (2019). Identification of Factors Influencing the Adoption of Health Information Technology by Nurses Who Are Digitally Lagging: In-Depth Interview Study. *Journal of Medical Internet Research, 22*(8). doi:https://doi.org/10.2196/15630

Lehto, M., Neittaanmaki, P., Poyhonen, J., & Hummelholm, A. (2022). Cybersecurity in Healthcare Systems. *Computational Methods in Applied Sciences, 56*, 183-215. doi:https://doi.org/10.1007/978-3-030-91293-2_8

Li, L., He, W., Ash, I., Anwar, M, & Yuan, X. (2019). Investigating the Impact of Cybersecurity Policy Awareness on Employee's Cybersecurity Behaviour. *International Journal of Information Management, 45*, 13-24. doi:https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Lin, R., & Kujabi, B. (2022). Addressing Challenges in the Development of Health Information Systems in The Gambia. *Health Policy and Technology, 11*(4). doi:https://doi.org/10.1016/j.hlpt.2022.100658

Liu, X., Sutton, P., McKenna, R., Sinanan, M., Fellner, B., Leu, M., & Ewell, C. (2019). Evaluation of Secure Messaging Applications for a Healthcare System: A Case Study. *Applied Clinical Informatics*, 140-150. doi:https://doi.org/10.1055%2Fs-0039-1678607

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and Healthcare: How Safe Are We? *British Medical Journal, 358*. doi:https://www.jstor.org/stable/10.2307/26950051

Martins, A., & Elofe, J. (2002). Information Security Culture. In M. Ghonaimy, M. El-Hadidi, & H. Aslan, *Security in the Information Society. IFIP Advances in Information and Communication Technology* (Vol. 86, pp. 203-214). doi:https://doi.org/10.1007/978-0-387-35586-3_16

McLaughlin, M.-D., & Gogan, J. (2018). Challenges and Best Practices in Information Security Management. *MIS Quarterly Executive*.

McNamee, M. (2021, September 5). *HSE Cyberattack: Irish Health Service still Recovering Months after Hack*. Retrieved from BBC: https://www.bbc.com/news/world-europe-58413448

Microsoft Azure. (n.d). *What is Big Data Analytics?* Retrieved from Microsoft: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-big-data-analytics

Mikuletic, S., Vrhovec, S., Skela-Savic, B., & Zvanut, B. (2023). Security and Privacy Oriented Information Security Culture (ISC): Explaining Unauthorised Access to Healthcare Data by Nursing Employees. *Computers & Security*. doi:https://doi.org/10.1016/j.cose.2023.103489

Moustafa, A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cybersecurity Management. *Frontiers in Psychology, 12*. doi:https://doi.org/10.3389/fpsyg.2021.561011

NAHIT. (2008). Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms. Department of Health and Human Services. Retrieved from http://www.nahit.org/docs/hittermsfinalreport

NCSC. (2022). *Cyber Threat Report.* Wellington: Te Tira Tiaki - Government Communication Security Bureau. Retrieved from https://www.ncsc.govt.nz/assets/NCSC-Documents/2021-2022-Cyber-Threat-Report.pdf

Newaz, A., Sikder, A., Rahman, M., & Ulugac, A. (2021). A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defences. *ACM Transactions on Computing for Healthcare, 2*(3), 1-44. doi:https://doi.org/10.1145/3453176

Ngafeeson, M. N. (2015). Healthcare Information Systems Opportunities and Challenges. *Encyclopedia of Information Science and Technology*(3), 1-9. doi:https://10.4018/978-1-4666-5888-2.ch332

Nifakos, S., Changdramouli, K., Nikolaou, C., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cybersecurity within Healthcare Organisations: A Systematic Review. *Sensors, 21*(5). doi:https://doi.org/10.3390/s21155119

Nunes, P., Antunes, M., & Silva, C. (2021). Evaluating Cybersecurity Attitudes and Behaviours in Portuguese Healthcare Institutions. *Procedia Computer Science, 181*, 173-181. doi:https://doi.org/10.1016/j.procs.2021.01.118

NZ Herald. (2021, September 10). *Waikato DHB Cyber Attack: 4200 People's Personal Details Disclosed on Dark Web*. Retrieved from NZ Herald: https://www.nzherald.co.nz/nz/waikato-dhb-cyber-attack-4200-peoples-personal-details-disclosed-on-dark-web/LCSXDX4W3HTZ4FCISHAL4T32IM/

O'Dowd, E. (2017, July 07). *Considerations for Connected Medical Device Networks*. Retrieved from TechTarget: https://hitinfrastructure.com/news/considerations-for-connected-medical-device-networks

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts: Working Papers on Information Systems, 10*(26), 10-26. doi:http://sprouts.aisnet.org/10-26

Pollini, A., Callari, T., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach. *Cognition, Technology & Work, 24*, 371-390. doi:https://doi.org/10.1007/s10111-021-00683-y

Priestman, W., Anstis, T., Sebire, I., Sridharan, S., & Sebire, N. (2019). Phishing in Healthcare Organisations: Threats, Mitigation and Approaches. *BMJ Health & Care Informatics, 26*(1). doi:https://doi.org/10.1136%2Fbmjhci-2019-100031

Rachmayani, D., Fauzi, M., Yeng, P., & Yang, B. (2021). Examining the Link between Stress Level and Cybersecurity Practices of Hospital Staff in Indonesia. *ARES '21: Proceedings of the 16th International Conference on Availability, Reliability, and Security.* doi:https://doi.org/10.1145/3465481.3470094

Rizzoni, F., Magalini, S., & Coventry, L. (2022). Phishing Simulation Exercise in a Large Hospital: A Case Study. *Digital Health*. doi:https://doi.org/10.1177/20552076221081716

Russell, J., Weems, C., & Richard, C. (2017). Self-Reported Secure and Insecure Cyber Behaviour: Factor Structure and Associations with Personality Factors. *Journal of Cybersecurity Technology, 1*(3-4), 163-174. doi:https://doi.org/10.1080/23742917.2017.1345271

Sari, P. K., Hundayani, P. W., Hidayanto, A. N., Yazid, S., & Aji, R. F. (2022). Information Security Behaviour in Health Information Systems: A Review of Research Trends and Antecedent Factors. *Healthcare (Switzerland)*, 10.

Sari, P., Prasetio, A., Candiwan, Handayani, P., Hidayanto, A., Syauqina, S., . . . Talleli, F. (2021). Information Security Cultural Differences Among Healthcare Facilities in Indonesia. *Heliyon, 7*. doi:https://doi.org/10.1016/j.heliyon.2021.e07248

Sonmez, F., Hankin, C., & Malacaria, P. (2022). Decision Support for Healthcare Cybersecurity. *Computers & Security, 122*. doi:https://doi.org/10.1016/j.cose.2022.102865

Tandon, A., Dhir, A., Islam, N., & Mantymaki, M. (2020). Blockchain in Healthcare: A Systematic Literature Review, Synthesizing Framework and Future Research Agenda. *Computers in Industry, 1222*. doi:https://doi.org/10.1016/j.compind.2020.103290

Tanriverdi, N., & Metin, B. (2021). What is Information Security Behaviour? In *Remote Work and Sustainable Changes for the Future of Global Business.* doi:10.4018/978-1-7998-7513-0.ch008

Tazkarji, M. (2020). The Effect of Patient Centeredness on Nurses' Security Policy Compliance. *AMCIS 2020 Proceedings*. Retrieved from https://www.researchgate.net/profile/Mohamed-Tazkarji/publication/343614390_Association_for_Information_Systems_Association_for_Information_Systems_AIS_Electronic_Library_AISeL_AIS_Electronic_Library_AISeL_The_Effect_of_Patient_Centeredness_on_Nurses'_Sec

Te Whatu Ora. (2022). *Te Whatu Ora - Health New Zealand.* Wellington: Department of the Prime Minister and Cabinet. Retrieved from https://www.futureofhealth.govt.nz/health-nz/

Thapa, C., & Camtepe, S. (2021). Precision Health Data: Requirements, Challenges and Existing Techniques for Data Security and Privacy. *Computers in Biology and Medicine, 129*. doi:https://doi.org/10.1016/j.compbiomed.2020.104130

US Department of Health and Human Services. (2022a, June 27). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Retrieved from Centers for Disease Control and Prevention (CDC): https://www.cdc.gov/phlp/publications/topic/hipaa.html

US Department of Health and Human Services. (2022b). *Lessons Learned from the HSE Cyberattack.* Retrieved from https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS Security Compliance Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3-4), 190-198. doi:https://doi.org/10.1016/j.im.2012.04.002

Veiga, A., Astakhova, L., Botha, A., & Herselman, M. (2020). Defining Organisational Information Security Culture - Perspectives from Academia and Industry. *Computers & Security, 92*. doi:https://doi.org/10.1016/j.cose.2020.101713

Verizon. (2018). *Executive Summary - 2018 Data Breach Investigation Report.* Verizon. Retrieved from https://www.verizon.com/business/resources/reports/DBIR_2018_Report_execsummary.pdf

Wager, K., Lee, F., & Glaser, J. (2009). Introduction to Healthcare Information. In K. Wager, F. Lee, & J. Glaser, *Healthcare Information Systems - A Practical Approach for Healthcare Management* (2nd ed., p. 3). San Francisco: John Wiley & Sons. Retrieved from http://ndl.ethernet.edu.et/bitstream/123456789/91874/1/Health%20Care%20Information%20Systems_%20A%20Practical%20Approach%20for%20Health%20Care%20Management.%20Second%20Edition%20%20%20%28%20PDFDrive%20%29.pdf

Wani, T., Mendoza, A., Gray, K., & Smolenaers, F. (2022). BYOD Usage and Security Behaviour of Hospital Clinical Staff: An Australian Survey. *International Journal of Medical Informatics, 165*. doi:https://doi.org/10.1016/j.ijmedinf.2022.104839

Wei, Q., & Courtney, K. (2018). Nursing Information Flow in Long-Term Care Facilities. *Applied Clinical Informatics, 9*(2), 275-284. doi:https://doi.org/10.1055%2Fs-0038-1642609

WHO. (2023). *Integrating Rehabilitation into Health Systems/ Information*. Retrieved from World Health Organisation: https://www.who.int/activities/integrating-rehabilitation-into-health-systems/information

Widianto, S., Kautsar, A., Sriwidodo, & Abdulah, R. (2021). Pro-Environmental Behaviour of Healthcare Professionals: A Study Applying Theory of Planned Behaviour. *International Journal Business and Globalisation, 28*(3), 219-232. doi:https://doi.org/10.1504/IJBG.2021.115562

Wiig, S., Billett, S., Canfield, C., Roise, O. N., Guise, V., Haraldseid-Driftland, C., . . . Macrae, C. (2020). Defining the Boundaries and Operational Concepts of Resilience in the Resilience in Healthcare Research Program. *BMC Health Services Research, 20*(330). doi:https://doi.org/10.1186/s12913-020-05224-3

Williams, P., Cowley, S., Bolan, C., Fowle, K., & Staynings, R. (2021). Working as a Health Cybersecurity Specialist. *The Health Information Workforce - Health Informatics*, 225-236. doi:https://doi.org/10.1007/978-3-030-81850-0_15

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research, 39*(1), 93-112. doi:https://doi.org/10.1177/0739456X17723971

Yadav, A., Raisurana, S., Balaji, H., Lalitha, P., Caytiles, R., & Iyengar, N. (2017). Information Security in Healthcare Organisations using Low-Interaction Honeypot Intrusion Detection System. *International Journal of Security and its Application, 11*(9), 95-108. doi:http://dx.doi.org/10.14257/ijsia.2017.11.9.07

Yang, B., Fauzi, M., & Yeng, P. (2022). A Comprehensive Assessment of Human Factors in Relation to Cybersecurity Compliance of Healthcare Staff in a Paperless Hospital. *Information*, 1-22. doi:https://doi.org/10.3390/info13070335

Yang, C., & Lee, H. (2016). A Study on the Antecedent of Healthcare Information Protection Intention. *Information Systems Frontiers, 14*, 253-263. doi:10.1007/s10796-015-9594-x

Yasar, K., & Pratt, M. (2021). *Security Awareness Training*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/security-awareness-training

Yeng, P., Fauzi, M., & Yang, B. (2022a). Assessing the Effect of Human Factors in Healthcare Cybersecurity Practice: An Empirical Study. *PCI '21: Proceedings of the 25th Pan-Hellenic Conference on Informatics* (pp. 472-476). Volos, Greece: Association for Computing Machinery. doi:https://doi.org/10.1145/3503823.3503909

Yeng, P., Fauzi, M., Yang, B., & Nimbe, P. (2022b). Investigation into Phishing Risk Behaviour among Healthcare Staff. *Information Security and Privacy*, *13*(8). doi:https://doi.org/10.3390/info13080392

Yeng, P., Szekeres, A., Yang, B., & Snekkenes, E. (2021). Mapping the Psychosocialcultural Aspects of Healthcare Professionals' Information Security Practices: Systematic Mapping Study. *JMIR Human Factors*, *8*(2). doi:https://doi.org/10.2196/17604

Yeng, P., Yang, B., & Snekkenes, E. (2019a). Framework for Healthcare Security Practice Analysis, Modeling, and Incentivization. *2019 IEEE International Conference on Big Data (Big Data)*, 3242-3251. doi:https://doi.org/10.1109/BigData47090.2019.9006529

Yeng, P., Yang, B., & Snekkenes, E. (2019b). Healthcare Staff's Information Security Practices Towards Mitigating Data Breaches. *pHealth 2019: Proceedings of the 16th International Conference on Wearable Micro and Nano Technologies for Personalised Health*.

Zakaria, H., Bakar, N., Hassan, N., & Yaacob, S. (2019). IoT Security Risk Management Model for Secured Practice in Healthcare Environment. *The Fifth Information Systems International Conference*, (pp. 1241-1248). doi:10.1016/j.procs.2019.11.238

Zhang, P., Liu, J., Yu, R., Sookhak, M., Au, M., & Luo, X. (2018). A Survey on Access Control in Fog Computing. *IEEE Communications Magazine*. doi:10.1109/MCOM.2018.1700333

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. (2020). Cybersecurity Awareness, Knowledge and Behaviour: A Comparative Study. *Journal of Computer Information Systems*. doi:https://doi.org/10.1080/08874417.2020.1712269