A MODEL FOR A SECURE SOCIAL MEDIA USAGE IN SELECTED MEDICAL INSTITUTIONS IN UGANDA

BY

MUTEBI JOE (PhD/36911/121/DU)
PhD – MANAGEMENT INFORMATION SYSTEMS (KIU)
MSC – INFORMATION SYSTEMS (MAK), BSC – COMPUTER SCIENCE (MAK)

A DISSERTATION SUBMITTED TO THE DIRECTORATE OF HIGHER DEGREE AND RESEARCH IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF A PHD IN MANAGEMENT INFORMATION SYSTEMS OF KAMPALA INTERNATIONAL UNIVERSITY

SEPTEMBER, 2023

DECLARATION

I, JOE MUTEBI, do hereby declare that this dissertation, titled: "A model for a secure Social Media (SM) usage in selected Medical Institutions in Uganda", to the best of my knowledge has not been presented to any known institution for the purpose of academic or degree award whatsoever. All the literatures and sources used in this study are clearly acknowledged and cited as required by American Psychological Association (APA) format.

Signature  Date 07/3/2023

Joe Mutebi (PhD – Management Information Systems)
School of Computing and Mathematics,
Kampala International University (KIU), Kampala, Uganda.

ACKNOWLEDGEMENT

First of all, I would like to thank almighty God in Christ Jesus for his continuous favor upon my life journey in academic endeavors (1 Thessalonians 5:18). It is indeed a great honor to accomplish a lifelong dream, often cherished by human race. My greatest appreciation goes to my supervisors; Associate Professor, Margaret Kareyo (PhD), and Associate Prof. Chinecherem Umezuruike (PhD). Your persistent encouragement, guidance and wisdom are the reasons for this great day in my life. May the almighty God continue to bless you abundantly. In a distinctive way, I thank my wife, Mrs. Amollo Juliet, who has always been by my side to support me in this journey. Of course, not forgetting the prayer and support from my children; Jordana Atim, Jeremiah Omara, Joshua Opio, Joel Ocen and Jesse Mito. Your prayers and continuous support were not in vain, (1 Corinthians 15:58).

In a special way, I acknowledge and appreciate a generous heart; Hl-Haji Dr. Hassan Bassajjabalaba, Chairman Board of Trustees (CBOT) Kampala International University, for his financial and material support in form of scholarship and guidance. Your generous contribution made it possible for me to sail through this lifelong dream. May the almighty God continue to bless you and your family in all your endeavours. Similarly, special gratitude goes to Mrs. Zerupa Akello Oburu and Mr. Peter Oburu, you have indeed been inspirational to my life through prayers, guidance and financial support. May the almighty God in Christ Jesus bless you abundantly. My final gratitude goes to the technical team who contributed immensely their time, knowledge and resources in this study, including; internal/external examiners, KIU doctoral committee, Heads of departments, professors, and lecturers in the School of Mathematics and Computing. Not forgetting my research assistants, as well as the respondents, all together, I say thank you, and God bless you all.

APPROVAL

This dissertation, titled; "A model for a secure Social Media usage in selected Medical Institutions in Uganda", has been submitted with my endorsement as the candidate's supervisors:

Signed_____ Date_____7/08/2023_____

Associate Professor, Margret Kareyo (PhD)

Department of Information Technology,

School of Computing and Mathematics,

Kampala International University (KIU), Kampala, Uganda.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

AHIMA – American Health Information Management Association

CIPESA – Collaboration on International ICT Policy for East and Southern Africa

DN – Help and documentations

HIPAA – Health Insurance Portability and Accountability Acts

ICT – Information and Communication Technology

ISE – Information Security

IS – Information System

IT – Information Technology

KIU – Kampala International University

LN – Learnability

MIBL – Medical information breaches level

MICT – Ministry of Information and Communications Technology

MISL – Medical Information Safety Level

MUST – Mbarara University of Science and Technology

NITA-U – National Information and Technology Authority Uganda

PR – Privacy and confidentiality

ST – Sustainability

SB – Subjectivity

SC – Security

SDV – System Development

SD – Social Dimension

SEM – Structural Equation Model

SM – Social Media

TD – Technical Dimension

TE – Training and Education

UCC – Uganda Communication Commission

UMDPC – Uganda Medical and Dental Practitioners Council

US – Usability

VB – Visibility

OPERATIONAL DEFINITION OF TERMS

Errors handling factor: SM system development (SDV) factor that provide users with detailed security error messages that they can be understood and acted upon.

Expressiveness factor: SM information security (ISE) factor that guides users on security in a manner that still gives them freedom of expression.

Help and documentation factor: SM training and education (TE) factor that makes security help apparent and easy to find for users.

Learnability factor: SM usability (US) factor which ensures that security actions are easy to learn and remember.

Medical information safety: maintenance of confidentiality, integrity and availability of medical information, during the activities of medical training – learning, teaching and research.

Privacy and confidentiality factor: SM information security (ISE) factor that protects user information against unauthorized access by third parties.

Revocability factor: SM system development (SDV) factor that allows users to revoke any of their security actions.

Satisfaction factors: SM usability factor ensure that users have a good experience when using the system and its security features.

Security factor: SM information security (ISE) factor that provides trusted communication channels between the user and the data servers.

Social Media (SM) usage in medical training: this entails the social (behavioral) and technical aspects of SM usage in enhancing the activities of medical training (learning, teaching, and research).

Social Media socio-technical factors: these are attributes of SM usage that embrace SM operational requirements ranging from hardware, software, personal, and organization.

Subjectivity factor: SM usability (US) factor where users believe in the capability of SM systems in enhancing performance of medical training, as well as safeguarding medical information.

Usability-Security: this is SM usage requirements that embrace both usability and security requirements, in a seamless way, (Ferreira, Koenig, & Lenzini, 2014).

ABSTRACT

Recently, the ubiquitous nature of Social Media (SM) usage, characterized by free flow of information have captivated the interest of higher education including medical institutions. Ironically, the balance of choice between SM usage and medical information safety has generated conflict of interest between the two viewpoints. Thus, hampering ratification (adoption) of SM usage in medical institutions. Fortunately, a socio-technical information security approach, coupled with usable-security principles have the potential to mitigate information security challenges on SM usage. Whereas related studies have remained optimistic, the key SM usage factors responsible for medical information breaches are scantily defined and documented. Thus, the purpose of this study was to identify the key information security factors, and develop a model for adopting a secure SM usage in medical institutions in Uganda. The study followed functionalism paradigm based on post-positivism philosophy, abductive reasoning approach, and online survey techniques involving 710 respondents. The key statistical analysis tools employed include both descriptive and inferential statistics (regression analysis). Notably, 27% to 42% of the respondents acknowledged occurrence of medical information breaches due to SM usage. The key SM usage factors identified include; *visibility, learnability, user satisfaction, help* and *documentation, user language, security, privacy* and *confidentiality*. Regression analysis results ($R^2 = 0.68$) imply that 68% of the changes in dependent variable was attributed to the changes in independent variables. Relatively, the social dimension of SM usage have more influence on SM usage and medical information safety, compared to the technical dimension. Overall, this study provides empirical and theoretical basis for medical institutions, researchers, and system developers to rationalize the vulnerable aspect of SM usage, and effectively leverage SM usage in their operations.

Key words: Social Media usage, Information security, Medical information, Socio-technical information security, usable-security.

CHAPTER ONE

BACKGROUND

1.1 Introduction

This study was intended to develop a model for adopting a secure Social Media (SM) usage in selected medical institutions in Uganda. The study focused on the activity of training undergraduate medical (MBChB) students, with respect to the challenges faced in preserving medical information safety, which hinders ratification and adoption of SM usage in medical institutions (Alunyu, et al., 2021; Kaddu & Mukasa, 2016). Chapter one stipulates the research background from the perspectives of historical, theoretical, conceptual, and contextual viewpoints. The chapter also narrates the problem statement based on the research background, and specifies the research objectives, and research questions, significance of the study, as well as the study scope accordingly.

1.2 General Background

Generally, the endeavor to ratify SM usage in medical institutions in Uganda need to commence with a systematic review of related studies, as well as soliciting the views and experience of SM practitioners in medical institutions in Uganda. From existing literatures, the profound needs of preserving medical information safety seem to be a stumbling block hindering ratification and adoption of SM usage in medical institutions (Katz & Nandi, 2021; Nwankwo & Chinecherem, 2020; Mirembe, Lubega & Kibukamusoke, 2019). Despite the high levels of SM embracement in medical operations in Uganda, medical institutions still lack concerted policy and structures to regulate on SM usage in their operations (Katz & Nandi, 2021; Nwankwo & Chinecherem, 2020; Mirembe, Lubega & Kibukamusoke, 2019). Meanwhile, SM usage embracement levels keep rising amidst significant levels of medical information breaches being reported (Alunyu, et al., 2021; Mirembe, Lubega & Kibukamusoke, 2019; Whyte & Hennessy, 2017; Kaddu & Mukasa, 2016; Roy et al., 2016). Unfortunately, from existing literatures, the key information security factors responsible for SM usage and medical information breaches are scantily defined and documented (Nwankwo & Chinecherem, 2020; Kaddu & Mukasa, 2016).

Comparatively, various studies related to SM usage and medical information safety often focus on the descriptive roles, and practitioners' experience, while stipulating benefits and risks associated with mostly the technical aspect of SM usage (Di Gangi, Johnston, Worrell & Thompson, 2017; Tayouri, 2015; Wilcox, & Bhattacharya, 2015). As such, their findings and measures could be limited

in scopes, and prone to duplications, redundancy, and inconsistency (Lombardo, Mordonini, & Tomaiuolo, 2021; Emamjome et al., 2014). Contrarily, this study focused on information security factors associated with the social, and technical dimensions of SM usage, in line with usable-security principles (Agrawal, et al., 2022; Mujinga, Eloff & Kroeze, 2019; Di Gangi, Johnston, Worrell & Thompson, 2017; Ferreira, Koenig, & Lenzini, 2014). In this case, SM socio-technical information security factors are attributes of information security entities ranging from hardware, software, personal, and organizational structures (Lombardo, Mordonini & Tomaiuolo, 2021; Mujinga, Eloff & Kroeze, 2019). Thus, information security entities in the social dimension would involve the people (SM users), and organizational structures, while the technical dimension include the technology (SM platforms), and tasks performed (Lombardo, Mordonini & Tomaiuolo, 2021). With respect to usable-security principles, SM socio-technical information security factors entails the technical information security factors, as well as the associated usability factors (Agrawal, et al., 2022; Mujinga, Eloff & Kroeze, 2019; Yeratziotis, Pottas, & Van Greunen, 2012).

1.2.1 Historical perspective

From historical perspectives, the embracement levels of SM usage in medical operations have been proliferating since 2010 (Katz & Nandi, 2021; Whyte & Hennessy, 2017; Roy et al., 2016; Pander et al., 2014). At the onset of its proliferations, SM was mainly used in informal settings, supporting largely personal and social needs of individual users, with minimal reported cases of medical information breaches in the mainstream medical settings (Katz & Nandi, 2021; Whyte & Hennessy, 2017; Surani, et al., 2017). Before 2013, IT related breaches accounted for less than 10% of the overall forms of healthcare data breaches, but later surpassed all the other forms of healthcare breaches by 2015 (Katz & Nandi, 2021; Seh et al., 2020). Eventually, by 2019, IT was reported as one of the most dominant form of data breaches in healthcare industry, accounting for over 90% of the overall form of healthcare data breaches, with global estimated cost of $6.45 million (Seh et al., 2020; HIPAA 2020). In Uganda, Alunyu, et al. (2021) study indicates that 22% to 31% of respondents reported IT related breaches in medical records in hospital sites in Uganda. Currently, Makerere University (Mak), Mbarara University of Science and Technology (MUST), and Kampala International University – Western Campus (KIU-WC) are among the key medical institutions providing the bulk of medical interns to hospital sites in Uganda (Kuteesa, et al., 2021; Bongomin et al., 2021). Recently, among the global IT related breaches reported, SM accounted for more than 56% of the 4.5 billion information records compromised in 2018 (Katz & Nandi, 2021; HIPAA 2020).

Relatively, the uniqueness in socio-economic, cultural, and political settings within the developed and developing countries affects how technology could be transferred and adopted (Mukassa, 2012). For instance, in developed countries such as US, healthcare institutions are required to implement "Health Insurance Portability and Accountability Acts" (HIPAA) policy, which was established way back in 1996 to minimize on the risk of information security violations associated with the social dimension of electronic medical data. Similarly, in Europe, Canada, and Australia, electronic document acts came into effect by 1990s (GDPR, 2021). Electronic document acts prevent individuals or institutions from collecting, processing, storing, or sharing of confidential information on electronic devices without consent. Thus, strengthening the social dimension of medical information security requirements (GDPR, 2021). However, in Africa, the "African Union Convention on Cybersecurity and Personal Data Protection" was introduced in 2014, and only eight countries including Rwanda in East Africa have ratified it by June 2020 (CIPESA, 2020). In South Africa, "Protection of Personal Information" (POPI) act came into effect in July 2021, (Lockhat, 2021). In Uganda, Data Protection and Privacy Act came into effect in 2019 (NITA-U, 2019; UCC 2020). Remarkably, the social aspect of electronic medical information security requirements in developed countries are relatively more established compared to Africa and developing countries (Petronilla, Horner & Pemberton 2016).

Notably, the progressive embracement of SM usage in the mainstream medical settings, coupled with the growth in electronic healthcare information is coinciding with the growing demands for effective management of electronic medical information (Coventry & Branley, 2018; Shenoy & Appel, 2017). By definition, electronic medical information are digital version of patient medical history, including treatment plans, diagnosis results, radiology images, medication, allergies, immunization data, and laboratory test results, etc. (Coventry & Branley, 2018; Shenoy & Appel, 2017). With respect to SM usage and medical training, electronic medical information serve the purpose of teaching/learning, research, and provision of medical services (Katz & Nandi, 2021; Whyte & Hennessy, 2017; Roy et al., 2016; Pander et al., 2014). In this case, SM usage enhances real-time interactions by effectively sharing clinical contents, and generating faster feedback among medical students, and medical staff including supervisors (Alenezi & Yaiesh, 2018; Shenoy & Appel, 2017). Thus, the ubiquitous nature of SM usage provide effective means of communication and collaboration. However, the pressing demands for preserving medical information safety still remain a pertinent issue, especially on the use of electronic medical information in medical training, and clinical operations (Coventry & Branley, 2018; Roy et al., 2016; Wendy, Kendall & Jason 2015).

In Uganda, Faculty of Medicine (MUST), and Faculty of Clinical Medicine and Dentistry (KIU-WC) often deploy over 1500 medical (MBChB) students within a semester session, across different healthcare sites, performing multiple clinical rotations – junior and senior clerkships (Kuteesa, et al., 2021). In their clinical years, medical students start getting involved in patient care while attaining hands-on, as well as acquiring professional experience in various domain of medicine including ethical conducts, under expert guidance. At this level of medical training, SM usage becomes a valuable tool in providing a network-space for effective interaction and communication among medical students, and medical staff including supervisors (Alenezi & Yaiesh, 2018; Wendy, Kendall & Jason 2015). Medical students often engage with their supervisors, patients and colleagues online, by sharing clinical contents, and could easily receive feedback on urgent matters related to their trainings as well as clinical services. According to Abraham et al. (2018), skills in time management are considered significant for medical training as students are often confronted with multitasking and time-bound series of activities. Therefore, SM would then provide a ubiquitous network-space for effective collaboration and communication among medical students, and medical staff (Alenezi & Yaiesh, 2018; Panahi, Watson & Partridge, 2014).

However, medical institutions are still conservative in fully ratifying and adopting SM usage in their operations (Katz & Nandi, 2021; Nwankwo & Chinecherem, 2020; Kaddu & Mukasa 2016). This caution is usually attributed to various anticipated challenges and risks often linked to SM usage, especially in the area related to preserving medical information safety (Roy et al., 2016; Wendy, Kendall & Jason, 2015; Pander et al., 2014). The ubiquitous and transparency nature of SM usage, characterized by free flow of information contents make the task of preserving medical information daunting (Roy et al., 2015; Pander et al., 2014). According to Pander et al. (2014) analysis study of the previous literatures on SM usage in medical education, 0.02% to 16% of medical students using SM had acted in unethical way. Their behaviors include various inappropriate acts, ranging from uploading of unprofessional contents, to violation of medical privacy and confidentiality (Wendy, Kendall & Jason 2015; Pander et al., 2014). Nevertheless, while many studies often focus on the information security challenges associated with the technical aspects of SM usage, and probably avoid ratifying SM usage, this study focused on the key information security factors, associated with both the social and technical aspects of SM usage. In this case, the challenge is conceptualized as a socio-technical information security problem (Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, & Lenzini, 2014). Thus, taking into context both the social (behavioral) and technical (technology) attributes of SM usage, with respect to medical information breaches accordingly (Lombardo, Mordonini, & Tomaiuolo, 2021; Petersen & Lehmann, 2018).

1.2.2 Theoretical perspective

Overtime, various theories have been fronted in the domain of information system (IS) and information security research. Among them, socio-technical system theory, DeLone and McLean theory, and activity theory, all exhibit relevant proposition suitable to address information security challenges on SM usage (Lombardo, Mordonini, & Tomaiuolo, 2021; Mujinga, Eloff & Kroeze, 2019; Larsen & Eargle, 2018; Yasnitsky, 2018). Relatively, the attributes of activity theory have elaborative structure akin to SM traits, but lacks consideration about the social factors that may influence the relationship between the constructs (Lombardo, Mordonini, & Tomaiuolo, 2021; Larsen & Eargle, 2018). However, socio-technical systems theory provides effective proposition for rationalizing both the structure and the relationships between the constructs (Lombardo, Mordonini, & Tomaiuolo, 2021; Mujinga, Eloff & Kroeze, 2019; Yasnitsky, 2018). While the extended DeLone and McLean theory describes the adoption of information systems by taking into account the quality of the data/information, system quality, and service quality that have an impact on usage and user satisfaction, and eventually produce the net benefits (Edgardo, Indira, Monica & Wenli, 2018). Typically, application of the other theories including activity theory can be witnessed in various information security models including Bell-LaPadula model, Biba model, Clark-Wilson models, and McCumber model. Whereby, security structures are technically defined by tagging security levels (top secret, secret, confidential, classified, read and write rights etc.) on subjects and objects, with less focus on the social constructs (Cristia & Rossi, 2021; Jayakrishna, Moneer & Christopher, 2020; Yasnitsky, 2018). For instance, deterrence theory focusing solely on disincentive and sanctions of subjects (Gartzke & Lindsay, 2019), while social cognitive theory focus on self-efficacy. Therefore, with respect to SM usage, socio-technical system theory, and the extended DeLone and McLean theory provide an effective foundation to study information security requirements on SM usage and medical information safety meticulously (Katz & Nandi, 2021; Nwankwo & Chinecherem, 2020; Mujinga, Eloff & Kroeze, 2019; Edgardo, Indira, Monica & Wenli, 2018).

Hence, this study is pinned by socio-technical system theory, and the extended DeLone and McLean theory (Mujinga, Eloff & Kroeze, 2019; Edgardo, Indira, Monica & Wenli, 2018). The theories provide effective basis to analyze relationships between SM socio-technical information security factors, SM usage and medical information safety. In congruent with related studies, Ferreira, Koenig, & Lenzini (2014) defines a usable-security information system as; "one that is secure technically, even when used by people". From this definition, Ferreira, Koenig, & Lenzini, (2014) suggests that the design of a secure and usable information security system should embrace both the social, and

technical dimensions of information security systems, in a seamless way. They then advanced a socio-technical information security concepts, and recommended it to guide in the process of developing online information security systems, (Ferreira, Koenig, & Lenzini, 2014). Similar concepts was extended by Mujinga, Eloff & Kroeze, (2019), who came up with validated online information security principles that can be considered in developing an online information systems, such as online-banking, and SM usage. Therefore, a socio-technical system approach to online information security development take into consideration both the social, and technical dimensions of information security requirements, in line with usable-security principles, other than focusing entirely on the technical aspect of information security requirements (Lombardo, Mordonini, & Tomaiuolo, 2021; Mujinga, Eloff & Kroeze, 2019).

Structurally, the construct of a socio-technical information security system comprise of two interdependent, and interactive subsystems; social dimension, and technical dimension accordingly. The theory concepts recognize and embrace the interaction between people; in this case SM users, and SM technology, in workplaces such as medical institutions (Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, & Lenzini, 2014). Specifically, the two dimensions of socio-technical system construct consist of 4 components, which are altogether linked and interactive. Namely, 1) social dimension, comprise of individuals (people) component, and organizations (structures) component. The structure component may include policies, regulations, and responsibilities which guide users on how to accomplish the intended tasks (Paja, Dalpiaz, & Giorgini, 2013). 2) The technical dimension, consist of technology artifact and task components, which comprise of methods and techniques, as well as knowledge used to translate system inputs into outputs (Belanger, Watson-Manheim, & Swan, 2013). Therefore, SM usage being an online system would fit within the domain of socio-technical system constructs. In this case, the usable-security concepts would be treated as seamless processes, both in the social and technical dimensions, other than treated as unilateral, and isolated set of information system requirements (Di Gangi, Johnston, Worrell & Thompson, 2016; Whyte & Hennessy, 2017; Ferreira, Koenig, & Lenzini, 2014). Thus, the relevant information security factors were then identified within the context of SM usage and medical information safety.

On the other hand, the extended DeLone and McLean theory describes the success (adoption) of information systems by taking into account the quality of the data/information, system quality, and the service quality, which have impact on usage and user satisfaction, and eventually produce the net benefits (Edgardo, Indira, Monica & Wenli, 2018). The theory had been extensively used in information system (IS) literatures, but not yet in the context of SM usage. Thus, this study aimed to

close the gap by using variables from IS success model in the context of SM usage and medical information safety, and also include the other variables that are pertinent in the context of SM usage, such as free flow of information contents, and other factors that may hinder the use of SM such as security and privacy concerns. In this case, understanding the adoption criteria of the intended consumers is essential for the success of innovations like SM usage (Nysveen, & Pedersen, 2014). Therefore, beside the extended IS success model, the researcher included components relating to the social information security issues, and usable-security principles in the context of SM usage (Edgardo, Indira, Monica & Wenli, 2018). Ironically, medical institutions may find it challenging to approve the use of SM despite the widespread embracement of the technology, this could be due to the unique security and privacy issues related to SM usage. Therefore, failing to correctly evaluate the appropriate balance of choice between SM usage and medical information safety would hinders SM adoption (Edgardo, Indira, Monica, & Wenli, 2018; Nysveen, & Pedersen, 2014).

1.2.3 Conceptual perspective

Subsequently, the overall concepts to this research was defined within the domain of information security factors, SM usage and medical information safety. In this case, the proposition relates SM socio-technical information security factors, SM usage and medical information safety – defined by the levels of medical information breaches. Thus, SM socio-technical information security factor was conceptualized an independent variable (Agrawal, et al., 2022; Lombardo, Mordonini, & Tomaiuolo, 2021), influencing SM usage and medical information breaches as dependent variable (Whyte & Hennessy, 2017; Roy, et al., 2016). Operationally, the study defines SM socio-technical information security factors as attributes of information security entities ranging from hardware, software, personal, and organization structures (Di Gangi, Johnston, Worrell & Thompson, 2017). While SM usage in this case is the perceived level of usage by medical students, medical staff, and stakeholders. Medical information safety deals with the process of safeguarding medical information during the activities of medical training – learning, teaching, research, and clinical services. In this case, medical information safety is defined by the level of reported cases of medical information breaches (Jomin & Takura, 2019; Brodnik et al., 2012; AHIMA, 2011; McWay, 2010). According to related studies, the key information security challenges associated with SM usage and medical information safety include privacy, confidentiality, and information overload (Wilcox, & Bhattacharya, 2015).

However, with respect to socio-technical system constructs, the social dimensional factors comprise of SM users, and organizational factors – policy, rules and regulations, (Paja, Dalpiaz, & Giorgini, 2013). While the technical dimensional factors are constituted by technology factors, as well as the

task execution accordingly (Mujinga, Eloff & Kroeze, 2019; Belanger, Watson-Manheim, & Swan, 2013). While usable-security concepts entails usability factors, both in the social, and technical dimensions (Di Gangi, Johnston, Worrell & Thompson, 2017; Whyte & Hennessy, 2017; Ferreira, Koenig, & Lenzini, 2014). Therefore, the relevant SM socio-technical information security factors were then identified within the scope of the social, and technical dimensions, with respect to usable-security principles accordingly. In this case, the levels of SM usage and medical information safety is the net benefit realized after embracing information security factors identified in the dimensions of the socio-technical and usable-security principles. Therefore, to effectively assess the net benefit of SM socio-technical information security factors identified, IS success model would provide a suitable framework to analyze the constructs. Thus, the extended DeLone and McLean theory describes the success of information systems by taking into account the quality of the data/information, system quality, and the service quality, which have impact on usage and user satisfaction, and eventually produce the required net benefits accordingly (Edgardo, Indira, Monica & Wenli, 2018).

Altogether, SM technology (system quality), and task performed (data/information quality) fits into the technical dimension of socio-technical system component, while people and structure (service quality) fits into the social dimension of socio-technical system component accordingly (Lombardo, Mordonini, & Tomaiuolo, 2021; Mujinga, Eloff & Kroeze, 2019; Edgardo, Indira, Monica & Wenli, 2018; Ferreira, Koenig, & Lenzini, 2014). Therefore, the key factors (variables) identified and examine under social dimension include; 1) usability factors - *visibility*, *learnability* and *user satisfaction*, 2) training and education factors - *help* and *documentation*, and *user language* (Thilini, Prashant, & Monjur, 2022; Swinney, 2019; Edgardo, Indira, Monica & Wenli, 2018; Schneiderman, el al., 2016). On the other hand, the key factors identified under technical dimension include; 3) SM technology development factors - *error handling*, and *process revocability*; 4) information security factors - *security*, *expressiveness,* and *privacy* and *confidentiality* (Lombardo, Mordonini, & Tomaiuolo, 2021; Swinney, 2019; Edgardo, Indira, Monica & Wenli, 2018; Albladi, & Weir, 2018). Therefore, with respect to SM socio-technical information security factors, SM usage and medical information safety, the relevant factors (variables) would be the common factors emphasized by related literatures cutting across the key SM usage dimensions – social and technical dimensions, taking into consideration usable-security principles (Agrawal, et al., 2022).

Subsequently, the following hypothesis were identified and tested; H_1: *Visibility* is a significant and positive predictor of *intention to use SM*. H_2: *Visibility* is a significant and positive predictor of *SM user satisfaction*. H_3: *Learnability* is a significant and positive predictor of *intention to use SM*. H_4:

Learnability is a significant and positive predictor of *SM user satisfaction*. H_5: *User language* is a significant and positive predictor of *intention to use SM*. H_6: *User language* is a significant and positive predictor of *SM user satisfaction*. H_7: *Help and documentation* is a significant and positive predictor of *intention to use SM*. H_8: *Help and documentation* is a significant and positive predictor of *SM user satisfaction*. H_9: *Security* is a significant and positive predictor of *intention to use SM*. H_{10}: *Security* is a significant and positive predictor of *SM user satisfaction*. H_{11}: *Privacy and confidentiality* is a significant and positive predictor of *intention to use SM*. H_{12}: *Privacy and confidentiality* is a significant and positive predictor of *SM user satisfaction*. H_{13}: *Error handling* is a significant and positive predictor of *intention to use SM*. H_{14}: *Error handling* is a significant and positive predictor of *SM user satisfaction*. H_{15}: *Process revocability* is a significant and positive predictor of *intention to use SM*. H_{16}: *Process revocability* is a significant and positive predictor of *SM user satisfaction*. H_{17}: *Intention to use SM* is a significant and positive predictor of *secure SM usage*. H_{18}: *User satisfaction* is a significant and positive predictor of *secure SM usage*. H_{19}: *User satisfaction* is a significant and positive predictor of *intention to use SM*. H_{20}: *Intention to use SM* is a significant and positive predictor of *user satisfaction*.

1.2.4 Contextual perspective

Relatively, it is necessary to re-engineer technology tools and apps created for a setting in the developed world to improve the contextual social settings in the developing countries (Yigzaw, Jormanainen & Tukiainen, 2018; Petronilla, Horner & Pemberton 2016; Mukassa, 2012). The uniqueness in socio-economic, cultural, and political space within the developed and developing countries affects how a technology tool or application can be transferred and adopted (Mukassa, 2012). For instance, in Uganda, Buganda kingdom riots of September 2009, and walk to work demonstration of 2011 affected SM operations (Joachim, 2014), compared to George Floyd protests in US in 2020, where SM usage remained operational (Taylor, 2020). Recently, the aftermath of Uganda presidential and parliamentary elections of 2016 led to the closure of SM network by Uganda government (Chibita, 2016; UN, 2016). The closure was purported to circumvent spread of rumors, incitement and unofficial declaration of election results by some political agents. Elsewhere, the insurrections in Tunisia and Egypt in 2011, Libya 2012 and Burundi in 2015, were attributed to situations escalated to greater extend, by incitement on SM posts (UN, 2016; Pointer, et al., 2016; Mare, 2014). Notably, much of the purported problems associated with SM usage in developing countries were more of social other than technology problem. Hence, this study was intended to provide empirical evidence necessary to strengthen the social dimension of usage.

Therefore, a system solution needs to be more thoroughly considered and constructed in order to maintain the necessary relationship and interaction between the technological instruments or application in the current social context. It is clear that re-engineering is necessary for a technology solution to be useful in other domains once it has been created and developed to address challenges in a specific area (Yigzaw, Jormanainen & Tukiainen, 2018; Petronilla, Horner & Pemberton 2016; Mukassa, 2012). When we apply technology or system solutions from the market to the context of developing economies, where the social environment demands substantial consideration, this issue even becomes more obvious and crucial (Yigzaw, Jormanainen & Tukiainen, 2019; Mukassa, 2012). According to the Socio-technical systems theory (Yigzaw, Jormanainen, & Tukiainen, 2018), despite how effective or expensive a technology solution may be, a system is only holistic and complete when it has an appropriate relationship with the social settings and the actors, and interacts with both technological and non-technical factors. Many information systems studies frequently overemphasize the use of technological tools and applications to solve the intended problem, ignoring the need for an integrated approach that calls for proper interconnection between the subsystems. Hence, this study examined the status quo and provide solution that need to be taken into consideration while planning and adopting SM usage in medical institutions in Uganda.

1.3 Problem Statement

From existing studies, medical institutions are still conservative in ratifying (adopting) SM usage in their operations (Katz & Nandi, 2021; Nwankwo & Chinecherem, 2020; Mirembe, Lubega & Kibukamusoke, 2019; Fenwick, 2016; Roy et al., 2016). The caution is often attributed to various anticipated challenges, and risks linked to SM usage, especially in the area related to preserving medical information safety (Nwankwo & Chinecherem, 2020; Coventry & Branley, 2018; Roy et al., 2016; Wendy, Kendall & Jason, 2015; Pander et al., 2014). According to Pander et al. (2014) analysis study of the previous literatures on SM usage in medical institutions, 0.02% to 16% of medical students using SM had acted in unethical way (Pander et al., 2014). According to Kaddu & Mukasa (2016) study of SM usage in higher education in Uganda, 29% to 38% of students got involved in unethical behaviors, including medical information breaches, (Mirembe, Lubega & Kibukamusoke, 2019). Recently, Alunyu, et al. (2021) study indicates that 22% to 31% of respondents reported IT related breaches in medical data in healthcare sites in Uganda. Globally, SM incidents accounted for more than 56% of the 4.5 billion information records compromised in 2018 (Katz & Nandi, 2021; HIPAA 2020). The consequences of medical information breaches include; loss of trust and reputations, legal suit, or financial harm, etc. (Jomin & Takura, 2019; Adler et al., 2015; Roy et al.,

2015; Pander et al., 2014). According to Liaw & Hannan (2011), 49.1% of patients in Australia confirmed withholding information from clinicians based on privacy and confidentiality concerns (Usher et al., 2014). In healthcare industry, the global estimated cost of electronic data breaches in 2019 was $6.45 million (Seh et al., 2020).

Formally, Uganda's National Development Programme (NDP III), in line with Sustainable Development Goals (SDG 4 & 9) acknowledged the potential of ICT in advancing the new post-2015 development agenda, which includes high-quality education and lifelong learning (UN, 2016; Kind & Evans, 2015). However, lack of adequate integration of ICT technologies in medical education could hinder the national development objectives. Hence, addressing the gaps in IT and business process integration would be ideal for the national and global educational development agenda, (UN, 2016). In the context of SM usage and medical training, little is known about the influence of SM socio-technical information security factors associated with SM usage (adoption) and medical information breaches. Related studies and existing models such as Bell-LaPadula model, Biba model, Clark-Wilson models, and McCumber model, etc. often focus on the technological aspect of information security requirements (Whyte & Hennessy, 2017; Roy et al., 2016; Pander et al., 2014). And yet, numerous studies have reported social dimensional factors such as social-engineering (behavioral) attack as some of the prevalent form of online information breaches (Nwankwo & Chinecherem, 2020; Mujinga, Eloff & Kroeze, 2019; Coventry & Branley, 2018; Roy et al., 2016; Wendy, Kendall & Jason, 2015; Pander et al., 2014). Therefore, this study was intended to identify, examine, and validate the key SM socio-technical information security factors associated with SM usage and medical information breaches. The factors identified supported the development of the intended model, which could be used to guide stakeholders in the process of adopting SM usage in medical institutions in Uganda. Hence, this study was intended to provide empirical evidence necessary to strengthen the social dimension of usage (Alunyu, et al. 2021; Nwankwo & Chinecherem, 2020; Petersen & Lehmann, 2018; Pander et al., 2014). Thus, the challenge is deductively conceptualized as a socio-technical system problem (Mujinga, Eloff & Kroeze, 2019; Edgardo, Indira, Monica & Wenli, 2018; Ferreira, Koenig, & Lenzini, 2014).

1.4 Objectives of the Study

1.4.1 General objective

The general objective of this study was to develop a model for adopting a secure SM usage, in selected medical institutions in Uganda.

1.4.2 Specific objectives

The specific objectives to the study was to:

1) Identify the key information security factors in line with SM usage and medical information safety, in selected medical institutions in Uganda.
2) Establish the type of relationships existing between SM socio-technical information security factors, and SM usage.
3) Design a model for adopting a secure SM usage in medical institutions in Uganda.
4) Validate the model for adopting a secure SM usage in medical institutions in Uganda.

1.5 Research Questions:

1.5.1 General research question

What kind of information security model would be required to appropriately adopt a secure SM usage in medical institutions in Uganda?

1.5.2 Specific research questions

1) What are the key information security factors in line with SM usage and medical information safety, in selected medical institutions in Uganda?
2) What type of relationships exist between SM socio-technical information security factors, and SM usage?
3) What is the appropriate model design required to adopt a secure SM usage in medical institutions in Uganda?

1.6 Significance of the Study

From related literatures, the profound need of preserving medical information safety seem to be a stumbling block hindering ratification and adoption of SM usage in medical institutions in Uganda, (Katz & Nandi, 2021; Nwankwo & Chinecherem, 2020; Mirembe, Lubega & Kibukamusoke, 2019). Ironically, the social dimensional aspect of SM usage, accentuated by transparence and free flow of information make the task of preserving medical information safety daunting (Katz & Nandi, 2021; Roy et al., 2015; Pander et al., 2014). Therefore, despite the high levels of SM embracement in medical operations in Uganda, medical institutions still lack concerted policy and organizational structures to regulate on SM usage in their operations (Katz & Nandi, 2021; Nwankwo & Chinecherem, 2020; Mirembe, Lubega & Kibukamusoke, 2019). Meanwhile, SM usage embracement levels keep rising amidst significant levels of medical information breaches being

reported (Alunyu, et al., 2021; Mirembe, Lubega & Kibukamusoke, 2019; Whyte & Hennessy, 2017; Kaddu & Mukasa, 2016; Roy et al., 2016). Considerably, when making decisions on adopting information system (SM usage), it would be important for decision makers and stakeholders to be well informed with appropriate information required so as to come up with informed decisions (Mukassa, 2012). Hence, this study offers empirical and theoretical support necessary to rationalize and manage information security issues related to SM usage and medical information safety. The study focus on medical institutions, and SM researchers. As a result, the study is important to medical institutions and other related organizations, medical students, medical staff, including supervisors, SM researchers, and ICT fraternity at large.

1) Medical institutions: the study outcome would provide guidance on information security requirements needed to rationalize and standardize SM usage in medical training and operations, including curricula and policy development. In this case, formalizing SM usage would help to enforce accountability in SM operation, and would protect the institutions against uncensored usage of SM by stakeholders. This would promote and help to leverage SM usage, and protect medical institutions against negative consequences such as; loss of trust and reputations, legal suit, or financial harm (Nwankwo & Chinecherem, 2020; Jomin & Takura, 2019; Surani, et al., 2017; Adler et al., 2015; Roy et al., 2015; Pander et al., 2014).
2) Medical students and staff: the study outcomes would help to improve on the level of awareness on the vulnerable aspects of SM usage with respect to the profound nature of medical information security. This would guide SM users to effectively manage and control SM operations in line with associated risks in medical operations, as well as medical training activities – teaching, learning and research (Nwankwo & Chinecherem, 2020; Jomin & Takura, 2019). This would also enhance medical students and staff to share quality contents, knowledge and information among the students and their supervisors, with better control and understanding of medical information security (Roy et al., 2015).
3) Researchers: the output of this research add more insight into the perspectives of information security requirements, SM usage, and medical information safety. Thus, the research added value by identifying and validating the key SM socio-technical information security factors, with respect to the developing and improving of information security concepts and standards appropriate for SM usage and medical information safety.
4) ICT knowledge base: the research output (the model and the factors identified) provides a basis for information scientist, software engineers, information system analyst, etc. to

comprehend, design and develop appropriate SM information security structures and policies in line with medical education, and other related settings.

1.7 Study Scope

The study scope explains the limitation to which the research area covers. In this case, the scope specifies the parameters, concepts, entities, variables and process appropriate to the study subjects. The key sub-sections covered under study scope include the general purpose of the study, geographical scope, the population and sample size scope, content scope, theoretical and conceptual scope, as well as the time scope and duration of the study accordingly.

1.7.1 General purpose of the study

The general purpose of this study was to develop a model for adopting a secure SM usage in selected medical institutions in Uganda. This would enhance SM practitioners, medical institutions, and SM researchers with empirical and theoretical basis to rationalize and leverage information security requirements on SM usage and medical information safety.

1.7.2 The geographical scope

This study was conducted within selected medical institutions in Uganda. Among the 12 top medical institutions in Uganda, 6 are government affiliated, while 6 are private owned (Bongomin et al., 2021). Using purposive sampling technique, 2 medical institutions were selected; 1 from government, and 1 from private. The selection criterion was guided by accreditation and recognition status by national regulatory authority, which signify adequate standards of system establishment warranting for such a study (Khamala, Makori & Njiraine 2018). More so, the balance of choice between government and private institutions would help to compare and contrast the research outcomes in the 2 categories of medical institutions in Uganda. Based on the above criteria, the appropriate medical institutions selectable included; 1) Mbarara University of Science and Technology (MUST) Faculty of Medicine; 2) Kampala International University (KIU) Faculty of Clinical Medicine and Dentistry (Bongomin et al, 2021). More so, both MUST and KIU have dedicated teaching hospitals, handling over 1500 medical students, within a single semester (Bongomin et al., 2021).

1.7.3 The population and sample size scope

Altogether, from the 2 selectable medical institutions (MUST and KIU), the study population was constituted by medical (MBChB) students; MUST 800 students, and KIU 1500 students, and medical staffs; MUST 75 staffs, and KIU 100 staffs, (Bongomin et al., 2021; Olum & Bongomin 2020). Specifically, the target population were medical (MBChB) students in year 3, 4 and 5, who start

getting involved in patient care while attaining hands-on experience in various domain of medicine, under expert guidance (Olum & Bongomin 2020; Najjuma et al, 2016). From the target population identified, stratified sampling was used to ensure all categories of respondents in the population sets were represented in the study sample, taking into consideration the margin of error, confidence interval level, and estimated response rate. On the other hand, the study was limited to the dominant SM platforms reported in higher institutions in Uganda, namely; WhatsApp, Facebook, Twitter and YouTube (Olum & Bongomin 2020; Mirembe, Lubega & Kibukamusoke, 2019).

1.7.4 Content scope

The content scope of this study is confined within 6 chapters of this report. Chapter one stipulates the research background from the perspectives of historical, theoretical, conceptual, and contextual viewpoints. Chapter one also narrates the problem statement based on the research background, and specifies the research objectives, and research questions, significance of the study, as well as the study scope accordingly. Chapter two covers literature reviews, while chapter three covers the appropriate research methodologies used. Chapter four covers data presentations, the results and the findings accordingly. Chapter five covers discussion of research results and the findings, and chapter six covers recommendations, study limitations and conclusion. The key concepts within each chapter is based on SM socio-technical information security factors, SM usage, and medical information safety (Agrawal, et al., 2022; Lombardo, Mordonini, & Tomaiuolo, 2021).

Logically, the researcher identified the key information security factors through literature search, while the corresponding primary data were collected using online survey (Google form). Afterwards, factor validation process was performed and the process included both empirical and theoretical methods. Thus, validity test was conducted on 45 Likert scale items, using validity form, and involving 10 subject experts. The validity form was developed with 4-points Likert scale rating items, focusing on the "relevancy", and "clarity" of the items. On the other hand, reliability test was conducted on 45 Likert scale items, using questionnaire, and involving 710 respondents. The main statistical analysis tools employed include Chi-square (x^2) test, Spearman's Rank correlations, and Ordinal Regression analysis. Subsequently, results were presented in a narrative, tabular and chart formats, respectively. Interview was used to generate more open-ended qualitative data. Interviews tend to be open and unstructured, which helped to provide information needed to comprehend the concepts behind the observed outputs, as well as evaluating changes in peoples' opinions. The statistical packages used in analysis include; SPSS version 26, for both descriptive, and inferential statistics, but supported by MS Excel, and SmartPLS accordingly.

1.7.5 Theoretical scope

The theoretical scope to this study is confined within the domain of socio-technical system theory, extended DeLone and McLean theory, and usable-security principles (Mujinga, Eloff & Kroeze, 2019; Edgardo, Indira, Monica & Wenli, 2018; Ferreira, Koenig, & Lenzini, 2014). Structurally, socio-technical system theory comprise of two interdependent and interactive components – social (behavioral) dimension, and technical dimension. The theory recognizes the interaction between people – in this case SM users, and technology (SM artifact), in workplaces (medical institutions). Therefore, SM users and the organization structure fits into the social dimension, while SM technology and the tasks performed fits into the technical dimension (Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, & Lenzini, 2014). The structural components of the social dimension consist of organizational structures such as policies, rules, and regulations that guide system users on completion of the required tasks. However, some of the key concepts were borrowed from the other related theories accordingly.

1.7.6 Conceptual scope

The conceptual scope to this research is defined within the domain of SM socio-technical information security factors, SM usage, and medical information safety. In this case, the main proposition is association between SM socio-technical information security factors, SM usage, and medical information safety – defined by the levels of medical information breaches. SM socio-technical information security factors were conceptualized an independent variables, influencing the tasks of SM usage and medical information safety (dependent variable). Operationally, the study defines SM socio-technical information security factors as attributes that embrace SM information security requirements ranging from hardware, software, personal, and organization structures. While medical information safety is operationally defined as the process of ensuring privacy, confidentiality, integrity and availability of medical information, during the activities of medical training – teaching, learning, and research (Jomin & Takura, 2019; Brodnik et al., 2012; AHIMA, 2011). With respect to socio-technical information security concepts, SM usage entails SM technology, task performed, the users (people), and organizational structures (Mujinga, Eloff & Kroeze, 2019).

1.7.7 The time duration of the study

The overall time duration for this study is defined by the following logical set of activities; literature review and problem formulation, concept and proposal development including approval, instrument development and validation (pre-test and pilot test of data collection instruments), data collection and

data cleaning process, data analysis process, and results presentations, report writing and dissemination of results and the findings, including publication in reputable journals. As guided by the logical set of activities, the overall time period for these study is 2 to 3 years excluding the redundant time period of the study. Since this study also depended on secondary data, document review process dated back to 2018, which was commensurate with the enrollment years of the current medical (MBChB) students in year 3, 4 and 5, accordingly (Bongomin et al., 2021; Olum & Bongomin 2020; UMDPC, 2017).

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Literature review conducted revealed considerable amount of studies related to information security factors, Social Media (SM) usage, and medical information safety (Katz & Nandi, 2021; Mirembe, Lubega & Kibukamusoke, 2019; Whyte & Hennessy, 2017; Roy et al, 2016). In congruent with research objectives, chapter two examines and summarizes the relevant literatures under the following subsections; medical information safety, challenges in the use of SM in medical training and information dissemination, review of the current models used in securing medical information in communication, existing information security models, knowledge gap identified, socio-technical system theory, extended DeLone and McLean theory, usable-security principles, and chapter two summary, (Edgardo, Indira, Monica & Wenli, 2018).

2.2 Medical information safety

From operational definition, medical information safety is the practice of ensuring security and privacy of any individually identifiable information or record in electronic or physical form, derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding patients' medical history, mental or physical condition, or treatment (HIPAA 2020; Bowman & Maxwell, 2018). The record may include treatment plan, diagnosis results, allergies, medication data, radiology images, immunization data, and laboratory test results, etc. (Shenoy & Appel, 2017). With respect to medical training, medical information serve the purpose of teaching, learning, research, as well as providing clinical services to patients (Katz & Nandi, 2021; Whyte & Hennessy, 2017; Roy et al., 2016). However, medical information breaches normally occur when identifiable medical information is acquired, used, or disclosed illegally (HIPAA, 2020; Househ et al., 2018; Kagoya et al., 2013). In case of breaches, the patient or institutions may lose trust, or confidence in the medical profession, which could results into loss of reputations, legal suit, or financial harm (Seh et al., 2020; Usher et al., 2014). Thus, compromising the quality of healthcare services provided (Seh et al., 2020; Jomin & Takura, 2019; Birkhauer et al, 2017; Adler et al., 2015; Roy et al., 2015). Therefore, with respect to SM usage and medical information safety, the key information security resource in this study is "identifiable medical information", hence the act of breaches entails illegal acquisition, access, usage, or disclosure of electronic format of identifiable medical information (HIPAA, 2020; Househ et al., 2018; Shenoy & Appel, 2017).

Generally, medical information breaches could occur as a results "unlawful acquisition, use or discloser of protected data/information in various formats" (HIPAA, 2020; Househ et al., 2018; HIPAA, 2021; Wikina, 2014). However, with respect to SM usage, the key information security resource is the electronic format of identifiable medical information". In this case, the act of breaches entails illegal acquisition, access, usage, and disclosure of identifiable medical information on SM platforms. In the current era of digital technology such as smartphone devices and web-based technologies, the transmission rate of medical information among stakeholders have become efficient, effective and ubiquitous. Thus, digital technology devices empower users to ubiquitously acquire, access, share and communicate medical information proficiently (Alenezi & Yaiesh, 2018; Panahi, Watson & Partridge, 2014). Unfortunately, the use of digital devices have also become a major source of medical information breaches (Katz & Nandi, 2021; Seh et al., 2020).

Usually, medical information breaches could affect individual, or organization in numerous ways. Besides financial harm, medical information breaches could jeopardize the image of the institutions, by ruining their reputation, and brands (Seh et al., 2020; Jomin & Takura, 2019). From the recent analysis of literatures conducted, out of 6355 information breaches reported within the period from 2005 to 2019, 62% of information/data breaches incidents were solely registered in healthcare settings (Seh et al., 2020; HIPAA 2020). According to Seh et al. (2020), the total number of healthcare records that was unlawfully divulged in 2019 was 41.2 million records. In the same year, IT was reported as one of the most predominant form of healthcare data breaches in healthcare industry, accounting for over 90% of the overall forms of healthcare breaches, with global estimated cost of $6.45 million, (Seh et al., 2020; HIPAA 2020). In Uganda, Alunyu, et al. (2021) study indicates that 22% to 31% of respondents reported IT related breaches in medical records in hospital sites in Uganda. Recently, among the global IT related breaches reported, SM accounted for more than 56% of the 4.5 billion of data records compromised in 2018 (Katz & Nandi, 2021; HIPAA 2020). Therefore, SM seem to be the leading source of IT related breaches in healthcare industry.

Relatively, the reported case of IT related breaches of 22% to 31% in hospital sites in Uganda by Alunyu, et al (2021), 29% to 38% by Kaddu & Mukasa (2016), are relatively high in a developing country where internet penetration is just 39% by 2021, and SM users are only 25% of the population (World Bank 2021). Compared to 0.02% to 16% breaches reported in developed countries where internet penetration was 87% by 2021, and SM users were over 70% of the population (Katz & Nandi, 2021; World Bank, 2021). This could imply that breaches in electronic medical information in developing countries is relatively deep-rooted, and would escalate with increase in internet

penetration and digital technologies, at a rate higher than the developed countries. The key affected setting would then be medical training since over 80% of medical services in hospital sites in Uganda are provided by medical interns (Kuteesa, et al., 2021), and over 70% of SM users in Uganda are found in higher institution of learning (Mirembe, Lubega & Kibukamusoke, 2019). It is on this basis that the researcher chose to study SM usage in medical institution settings in Uganda.

2.3 Challenges of SM usage and Medical information safety.

In congruent with SM researchers, SM is can be defined as; "a group of internet-based applications built on ideological and technological foundation of Web 2.0 concepts, which enable creation, modification, and sharing of user-generated contents online" (Obar & Wildman, 2015; Kaplan & Haenlein, 2012). Generally, the unique characteristics of SM usage is allowing free flow of information, which enable individual users to subjectively create, modify, and share information contents online ubiquitously. However, with respect to medical institutions, the balance of choice between SM usage and medical information safety has generated conflict of interest between the two viewpoints. On one side, SM usage has become a valuable tool for effective interaction and communication among medical students, medical staff, and stakeholders (Olum & Bongomin, 2020; Mirembe, Lubega & Kibukamusoke, 2019; Alenezi & Yaiesh, 2018). Whereby, medical students often engage with their supervisors, and colleagues online by sharing clinical contents, and could easily receive feedback on urgent matters related to their trainings, as well as handling of clinical cases during their training (Bongomin et al, 2021; Olum & Bongomin, 2020Mirembe; Roy et al, 2016). In this case, electronic medical information shared on SM serves multiple purposes, including teaching, learning, research, and providing clinical services to patients (Nwankwo & Chinecherem, 2020; Warboys, Mok & Frith 2014). However, in the course of conducting their training, clinicians are mandated to preserve medical information safety, especially on the issue related to medical privacy and confidentiality (Katz & Nandi, 2021; Nabimanya, et al., 2020).

Unfortunately, the subjective nature of SM usage propagates new information security challenges propounded by mainly the social (behavioral) aspect of SM usage (Lombardo, Mordonini, & Tomaiuolo, 2021; Tayouri, 2015; Wilcox, & Bhattacharya, 2015). According to Pander et al., (2014) analysis study of previous literatures on SM usage in medical institutions, 0.02% to 16% of medical students using SM had acted in unethical manner (Pander et al., 2014). While Kaddu & Mukasa (2016) study of SM usage in higher education in Uganda indicates that 29% to 38% of SM users in Uganda higher education face the challenge of inappropriate information, including medical information breaches (Alunyu, et al., 2021; Chan & Leung, 2018). Recently, Roy et al., (2016) study

mentions that patients often share their private information, and communicate with their physicians online. It is therefore professionally important for physicians, as well as students and clinical instructors to act in professional manners, and maintain the privacy and confidentiality of medical information (Pander et al., 2014). Consequently, various medical institutions are conservative in fully ratifying and adopting SM usage in their operations (Nwankwo & Chinecherem, 2020; Roy et al., 2016). This caution is mainly due to the numerous anticipated challenges associated with the social dimension of SM usage and medical information safety (Lie et al., 2013).

Basically, medical information breaches are viewed as having the possibilities of depressing both patients and physician from participating in healthcare systems. In case patients lose trust in the privacy and confidentiality of personal information, they would be reluctant to divulge sensitive medical information to clinicians (Usher et al., 2014; Liaw & Hannan, 2011). On the other hand, clinicians would be less-willing to participate in healthcare systems which are uncertain about the comprehensiveness of the information provided. For instance, a study survey conducted in Australia assessing the privacy and confidentiality concerns on patients' healthcare decision making, which might jeopardize medical services. The findings showed that more than 49.1% of the patients in Australia confirmed withholding information from clinicians based on privacy and confidentiality concerns (Usher et al., 2014; Liaw & Hannan, 2011). Nevertheless, as many existing studies often focus on the challenges associated with mainly the technical aspects of SM usage, to explain information security challenges associated with SM usage and medical information safety, this study focused on both the social, and technical aspects of SM usage.

Relatively, the technical aspects of the various SM platforms are enhanced with customizable information security functions to support SM users in managing information security requirements (Obrain et al., 2021; Jain, Sahoo & Kaubiyal, 2021). For instance, Facebook and Twitter use two-factor verification process; password, as well as verification codes established using mobile devices. This authentication process would help to diminish the risk of compromising user accounts by unauthorized users (Jain, Sahoo & Kaubiyal, 2021). Furthermore, Facebook users can adjust security configurations (public or private), and select users who can view their contents. It can also authorize the users to allow or reject access of third party applications to access their own contents. On the other hand, WhatsApp communication is end-to-end encrypted between two parties. The other security functions include anti-virus updates, firewall, anti-spam filter, VPN and intrusion detection. This therefore, could imply that much of the dreaded risks associated with SM usage and medical information safety could emanate from the social (behavioral) aspect of SM usage, other than

technical (Mutebi, et al., 2022; Mujinga, Eloff & Kroeze, 2019; Whyte & Hennessy, 2017; Wilcox, & Bhattacharya, 2015; Roy et al., 2015).

Therefore, the researcher's view is that the technical dimension of SM information security requirements are evidently more established, compared to the social dimension (Lombardo, Mordonini, & Tomaiuolo, 2021; Wilcox, & Bhattacharya, 2015). This could also reinforce the researchers' argument that medical institutions need to develop concerted policy to regulate on SM usage, which all point to the security gap associated with the social dimensional aspects of SM information security (Katz & Nandi, 2021; Nwankwo & Chinecherem, 2020; Mirembe, Lubega & Kibukamusoke, 2019). More so, numerous studies have reported social-engineering (behavioral) attack as one of the vulnerable and prevalent form of online breaches (Wilcox, & Bhattacharya, 2015). Consequently, as SM usage embracement levels keep rising amidst significant levels of medical information breaches being reported, it would be prudent to specify the key information security factors within the social, and technical dimensions of SM usage accordingly (Alunyu, et al., 2021; Mirembe, Lubega & Kibukamusoke, 2019; Whyte & Hennessy, 2017; Kaddu & Mukasa, 2016; Roy et al., 2016). Elsewhere, John Hopkins, and Harvard School of Medicine in US, and University of Aberdeen in UK, strengthen the social dimension of SM usage with concerted policies and guidelines (Katz & Nandi, 2021). In this case, SM practitioners, and SM researchers would avoid overloading their focus of information security challenges on the technical aspect of information security, and appropriately identify and manage the right cause.

Therefore, to avoid narrowing the scope of identifying the relevant information security factors associated with SM usage and medical information safety, both the social, and technical dimensions needed to be taken into considerations (Yigzaw, Jormanainen & Tukiainen, 2018; Di Gangi, Johnston, Worrell & Thompson, 2017). In line with the research questions, the researcher presupposed that much of the challenges (vulnerable attributes) associated with medical information breaches could emanate from the social (behavioral) dimension of SM usage (Whyte & Hennessy, 2017; Ferreira, Koenig, & Lenzini, 2014). Nevertheless, the key SM socio-technical information security factors were identified by reviewing the relevant literatures within the domain of SM usage and online information security, as guided by socio-technical system theory, the extended DeLone and McLean theory, and usable-security principles (Edgardo, Indira, Monica & Wenli, 2018; Yigzaw, Jormanainen & Tukiainen, 2018). Altogether, the common factors emphasized across related literatures were considered relevant for inclusion in this study. Notably, the dominant form of information security risk associated with SM usage and medical information safety include; privacy,

confidentiality, and information overload (HIPAA, 2021; Katz & Nandi, 2017; Whyte & Hennessy, 2017; Wilcox, & Bhattacharya, 2015; Wikina, 2014; Pander et al., 2014).

2.4 Review of the current Information security Theories and Models

Overtime, various theories have been propounded and proposed in the domain of information security researches. Among them, socio-technical system theory, DeLone and McLean theory, and activity theory exhibit relevant proposition appropriate for addressing information security challenges on SM usage (Mujinga, Eloff & Kroeze, 2019; Edgardo, Indira, Monica & Wenli, 2018; Larsen & Eargle, 2018). Relatively, the attributes of activity theory have elaborative structure akin to SM traits, but lack consideration about the relevant factors that may influence the relationship between the social constructs (Larsen & Eargle, 2018). However, socio-technical systems theory, and extended DeLone and McLean theory provide effective proposition for rationalizing both the structure and the relationships between the social constructs (Mujinga, Eloff & Kroeze, 2019). Typically, application of activity theory can be witnessed in various information security models including Bell-LaPadula model, Biba model, Clark-Wilson model, and McCumber model. Whereby, security structures are technically defined by tagging security levels (top secret, secret, confidential, classified, read and write rights etc.) on subjects and objects, with less focus on the social aspect of information security components (Cristia & Rossi, 2021). The other lopsided theories include; deterrence theory focusing solely on disincentive and sanctions of subjects (Gartzke & Lindsay, 2019), while social cognitive theory focus on self-efficacy. Therefore, with respect to SM usage, socio-technical system theory provides an effective foundation to study both the structure and relationship between constructs, meticulously (Mujinga, Eloff & Kroeze, 2019; Yigzaw, Jormanainen & Tukiainen, 2018). According to Yigzaw, Jormanainen, & Tukiainen (2018), despite how effective or expensive a technology solution may be, a system is only holistic and complete when it has an appropriate relationship with the social settings and actors, and should embrace both technological and non-technical factors.

Hence, this study is appropriately pinned by socio-technical system theory. The theory provides a basis to study relationship between SM socio-technical information security factors, SM usage and medical information safety effectively. In congruent with related studies, Ferreira, Koenig, & Lenzini (2014) defines a usable-security information system as; ‘‘one that is secure technically, even when used by people”. From this definition, Ferreira, Koenig, & Lenzini, (2014) suggests that the design of a secure and usable information security system should embrace both the social, and technical dimensions of information security requirements, in a seamless way. They then advanced a socio-technical information security concepts, and recommended it to guide in the process of developing

online information security systems. Similar concepts was extended by Mujinga, Eloff & Kroeze, (2019), who came up with validated online information security principles that can be considered in modeling an online information systems, such as online-banking, ecommerce and SM usage. Therefore, a socio-technical system approach to online information security development take into consideration both the social, and technical dimensions of information security requirements, in line with usable-security principles, other than focusing entirely on the technical aspect of information security requirements (Mujinga, Eloff & Kroeze, 2019). Table 1 below summarizes existing information security models, showing their strength, weakness, and the gaps.

Table 1: Existing information security models

	Source	Model	Security Focus (Strength)	Security Focus (Weakness)	Security Dimension (Strength)	Security Dimension (Weakness)
1	(Tang, Z., et al, 2018; Bell, D. E., 2015)	Bell-LaPadula model	Confidentiality and controlled access to information	Usability, Visibility, Ease of use, Satisfaction, and Authentication	Provide technical measures	Lack social measures
2	(Cristia & Rossi, 2021)	Biba model	Integrity	Privacy, Confidentiality, Satisfaction, Usability, Visibility	Provide technical measures	Lack social measures
3	(Cristia & Rossi, 2021)	Clark-Wilson models	Integrity and partially confidentiality	Require a well-structured computer systems, Usability, Visibility, and Satisfaction	Provide technical measures	Lack social measures
4	(Jayakrishna, Moneer & Christopher, 2020)	McCumber model	Confidentiality, Integrity, Authentication	Usability, Visibility, Satisfaction, and Ease of use	Provide social technical measures	Lack usable-security measures

2.5 Knowledge gap identified

Notably, none of the existing information security models combine socio-technical information security concepts, and usable-security principles, to address information security challenges on SM usage and medical information safety. The existing models and related studies often focus on the descriptive roles of SM usage in medical education, while specifying the benefits, and the risks associated with mainly the technical aspect of SM usage (Whyte & Hennessy, 2017; Roy et al., 2016; Sherbino & Frank, 2014; Pander et al., 2014). Thus, existing security models are lopsided, context specific, and mainly driven by the technical concepts of information security requirements. For

instance, Bell-LaPadula, Biba, and Clark-Wilson are technically defined by tagging security levels (top secret, secret, confidential, classified, read and write rights etc.) on subjects, and objects. Subject at a given level may only access/read/write to objects at its corresponding level and below (Cristia & Rossi, 2021). Contrarily, in web 2.0 (social and technical) and SM usage contexts, information contents are characterized free flow of information, accentuated by user-generated content and ease of usability for end-users compared to its earlier version of web 1.0 (technical) (Obar & Wildman, 2015; Kaplan & Haenlein, 2012). Therefore, it would be appropriate to adjust information security focus from the technical dimension (web 2.0), to embrace both the technical and social dimension (web 2.0) accordingly (Obar & Wildman, 2015).

Relatively, Bell-LaPadula model is used to provide confidentiality, while Biba, and Clark-Wilson models is used to provide integrity. However, the models are limited by their technical assumption that all data are classified, and the classification does not change (Cristia & Rossi, 2021). However, besides their limitations of being technical focused, various existing information security principles lack the social and usability attributes in their design (Agrawal, et al., 2022). In this case, existing information security models are technical focused, context specific, and less applicable in addressing information security challenges on web 2.0, and SM usage context (Agrawal, et al., 2022). Therefore, as SM usage embracement levels keep rising amidst significant levels of medical information breaches being reported, medical institutions would require a broader empirical and theoretical basis to rationalize and ratify SM usage in their operations (Katz & Nandi, 2021; Nwankwo & Chinecherem, 2020; Mirembe, Lubega & Kibukamusoke, 2019; Roy et al., 2016). In response to this study gap, the researcher identified and validated the key SM socio-technical information security factors, and developed a model for adopting a secure SM usage in medical institution in Uganda (Mujinga, Eloff & Kroeze, 2019; Roy et al., 2015).

Overall, the construct of a socio-technical information security system comprise of two interdependent, and interactive subsystems; social dimension, and technical dimension accordingly (Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, & Lenzini, 2014). The theory concepts recognize the interaction between people; in this case SM users, and SM technology, in workplaces such as medical institutions. Specifically, the two dimensions of socio-technical system construct consist of 4 components, which are altogether linked and interactive. Namely, 1) social dimension, comprise of individuals (people) component, and organization (structure) component. The structure component may include policies, regulations, and responsibilities which guide users on how to accomplish the intended tasks (Paja, Dalpiaz, & Giorgini, 2013). 2) The technical dimension consist of technology

artifact components, and task components, which comprise of methods and techniques, as well as knowledge used to translate system inputs into outputs (Mujinga, Eloff & Kroeze, 2019; Belanger, Watson-Manheim, & Swan, 2013). Therefore, SM usage being a web 2.0 and an online system would fit within the domain of socio-technical system constructs. In this case, the usable-security concepts would be treated as seamless processes, both in the social and technical dimensions, other than treated as unilateral, and isolated set of information system requirements (Di Gangi, Johnston, Worrell & Thompson, 2016; Whyte & Hennessy, 2017; Ferreira, Koenig, & Lenzini, 2014). Thus, the relevant information security factors were then identified within the range of requirements as emphasized by SM socio-technical information security concepts, ISSM, usable-security principles, SM usage, and medical information safety (Mujinga, Eloff & Kroeze, 2019; Obar & Wildman, 2015; Kaplan & Haenlein, 2012). Table 2 below presents list of relevant literatures, indicating the authors, country, study purpose, methodology used, type of sources, and summary of key points specifying SM usage and information security factors relevant to the study.

Table 2: SM usage, and information security factors

Social Media usage, and Information Security Factors (SMISF)				
Author	Country	Purpose	Type of source (Methodology)	Summary of key points (factors)
(Tayouri, 2015)	Israel	"Identify cyber security risks, and mitigations, focusing on the human factor and social media usage."	Conference proceeding (Literature Review)	Education and training Error handling Information security - Privacy/confidentiality - Availability
(Wu He, 2012)	USA	"Review social media security risks and mitigation techniques"	Journal article (Literature review)	Security policy User monitoring Education and training Software update Error handling
(Jain, Sahoo, & Kaubiyal, 2021)	India	"Review different security and privacy threats, and existing solutions that can provide security to social network users"	Journal article (Literature review)	Security and privacy setting Authentication mechanism Report users
(Wilcox, & Bhattacharya, 2015)	Australia	"Countering Social Engineering through Social Media: An Enterprise Security Perspective"	Book chapter (Literature Review)	Effective security policy Increase awareness Education and training Legal factors Technical factors - Anti-virus - Firewalls - Anti-spam filter - Access control - VPN

				- Intrusion detection - Encryption - Two factors authentication
(Ma, Zhang, Li, & Wu, 2019)	China	"Exploring information security education on social media use: Perspective of uses and gratifications theory"	Journal article Survey and (Literature review and modeling)	Education and training User satisfaction Information security awareness
(Di Gangi, Johnston, Worrell & Thompson, 2016)	USA	"A multi-panel Delphi study of organizational social media risk"	Journal article (Delphi approach)	Social factors - Effective policy - Awareness - Education and training Technical factors Legal factors
(Philip Nyblom, Gaute Wangen, & Vasileios Gkioulos, 2020)	Norway	"Risk Perceptions on Social Media Use in Norway"	Journal article (Survey)	Security awareness
(Andrew Swinney, 2019)	USA	"Creating a Social Media risk Assessment"	Journal article (Literature review)	User training Effective policy Awareness
(Obrain et al., 2021)	South Africa	"Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa"	Journal article (Literature review)	Information Security awareness
(Albladi, & Weir, 2018)	Saudi Arabia	"Identify user characteristics that influence judgment of social engineering attacks in social networks"	Journal article Literature review, (Expert validation of factors)	Socio-emotional - Social network trust - Usage motivation Socio-psychological - Education - Computer knowledge - Information security awareness Perceptual - Privacy awareness
(Thilini, Prashant, & Monjur, 2022).	Switzerland	"Cybersecurity Practices for Social Media Users: A Systematic Literature Review"	Journal article (Literature review)	Awareness Training and education Information security
(Yeratziotis, Pottas, & Van Greunen, 2012)		"Usable-security Heuristic Evaluation for the Online Health Social Networking Paradigm"	Journal article (Literature review, heuristics)	Usability factors - Visibility - Learnability - Satisfaction - Aesthetic and minimalist design - User language - User suitability - User assistance - Error handling

				- Clarity - Revocability - Identity signal - Expressiveness Security and privacy - Availability - Privacy - Integrity - Confidentiality
(Mujinga, Eloff & Kroeze, 2019)	South Africa	"Investigates design principles for usable security and proposes a validated framework usable security design principles."	Journal article Literature, (Validation using Expert)	Social dimension - Visibility - Learnability - Satisfaction - Help and documentation - User language - User suitability Technical dimension - Error handling - Revocability - Availability - Security - Privacy/confidentiality - Expressiveness
(Ferreira, Koenig, & Lenzini, 2014)	Portugal	"A Conceptual Framework to Study Socio-Technical Security"	Book chapter (Literature review)	Social factors Technical factors
(Lombardo, Mordonini, & Tomaiuolo, 2021)	Italy	"Adoption of Social Media in Socio-Technical Systems: A Survey"	Journal article (Survey)	Social factors Technical factors Legal factors

2.6 Usable-security principles

From usable-security perspective, existing studies have recognized that using information security systems that lack usability features could undermine overall information security goals (Yeratziotis, Pottas, & Van Greunen, 2012). Usability in this context can operationally be defined as "the extent to which information security system, product or service can be used by specified users to achieve information security goals with effectiveness, efficiency and satisfaction" (Agrawal, et al., 2022; Ferreira, Koenig, & Lenzini, 2014; Yeratziotis, Pottas & Van Greunen, 2012). Thus, developing information security that is usable has become a requirement. Ferreira, Koenig, & Lenzini (2014) describes a usable-security information system as; "one that is secure technically, even when used by people". Therefore, usable-security concepts propound on the need for having effective information security functions technically, as well as taking into consideration the usability of those factors (Di Gangi, Johnston, Worrell & Thompson, 2017; Ferreira, Koenig, & Lenzini, 2014). Traditionally, information security parse, focus on mainly privacy, confidentiality, integrity, and

availability (Yeratziotis, Pottas & Van Greunen, 2012). Whereby, information security functions are solely developed with emphasis placed on technical (objective) concepts of information security. For instance, information security models such as; Bell-LaPadula, Biba, and Clark-Wilson, etc., are technically defined by tagging security levels (top secret, secret, confidential, classified, read and write rights etc.) on subjects, and objects, accordingly. Subject at a given level can only access/read/write to objects at its corresponding levels and below (Cristia & Rossi, 2021). However, those objective security models are limited by their technical assumption that all data are classified, and the classification does not change (Cristia & Rossi, 2021). However, besides their limitations of being technical (objective) focused, various existing information security models lack social and usability attributes in their design (Agrawal, et al., 2022; Cristia & Rossi, 2021).

Contrarily, this study take into consideration the broader context of socio-technical information security concepts, and usable-security principles to conceptualize SM information security requirements, with respect to SM usage and medical information safety. According to Agrawal, et al. (2022), the key usable-security factors, which could be considered for web 2.0 and online information systems include; 1) Security factors – *confidentiality, availability, accessibility, accountability* and *non-repudiation*; 2) Usability factors – *effectiveness, efficiency, satisfaction* and *error protection*. Another perspective propounded by Yeratziotis, Pottas, & Van Greunen (2012) include; 1) Usability factors – *visibility, learnability, satisfaction, aesthetic and minimalist design, user language, user suitability, user assistance, error handling, clarity, revocability, identity signal, and expressiveness*; 2) Security and privacy – *confidentiality, integrity, availability,* and *privacy*. The other usable-security factors identified by other related authors include; usability – *visibility, learnability,* and *satisfaction*; Information security – *security, privacy, confidentiality,* and *expressiveness* (Mutebi, et al., 2022; Mujinga, Eloff & Kroeze, 2019). Usability – *help* and *documentation*, and *learning* (Shneiderman et al., 2016; Yeratziotis, Pottas & Van Greunen, 2012). Usability – *user satisfaction* (Zahidi, Yan Peng Lim, & Woods, 2014; Yeratziotis, Pottas & Van Greunen, 2012). However, according to Mujinga, Eloff & Kroeze (2019), online information security factors could be categorized into the social, and technical dimensions. From the precept of socio-technical system theory, and SM being a web 2.0 and an online information system, the term SM socio-technical information security factor would then fit the nomenclature adopted in this study (Mutebi et al., 2022; Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, & Lenzini, 2014). Overall, Table 3 below presents list of relevant literatures, indicating the author's details, and summary of key points specifying usable-security factors relevant to the study (Mutebi et al., 2022).

Table 3: Usable-security factors

Usable-security factors (USF)				
(Agrawal, et al., 2022)	India	"Develop factors for assessment of usable-security systems"	Journal article (Survey)	- Security factors – *confidentiality, availability, accessibility, accountability and non-repudiation*, - usability factors – *effectiveness, efficiency, satisfaction* and *error protection*
(Yeratziotis, Pottas, & Van Greunen, 2012)		"Usable-security Heuristic Evaluation for the Online Health Social Networking Paradigm"	Journal article (Literature review, heuristics)	Usability factors - Visibility - Learnability - Satisfaction - Aesthetic and minimalist design - User language - User suitability - User assistance - Error handling - Clarity - Revocability - Identity signal - Expressiveness Security and privacy - Availability - Privacy - Integrity - Confidentiality
(Shneiderman et al., 2016)		"Identify grand challenges for HCI researchers."	Journal (Literature review)	Help and documentation Learning
(Mujinga, Eloff & Kroeze, 2019)	South Africa	"Investigates design principles for usable security and proposes a validated framework usable security design principles."	Journal article (validation using experts)	Usability - Visibility - Learnability - Satisfaction Information security - Security - Privacy/confidentiality - Expressiveness
(Zahidi, Yan Peng Lim, & Woods, 2014)		"Understanding the user experience (UX) factors that influence user satisfaction."	Conference proceeding	User satisfaction factors

2.7 Socio-technical system theory

Fundamentally, socio-technical system construct comprise of 2 interdependent, and interactive main components – social dimension components (people and organizational structures), and technical dimension components (technology and task performed) (Mujinga, Eloff & Kroeze, 2019; Ferreira,

Koenig, & Lenzini, 2014). The theory recognize the interaction between people – in this case SM users, and technology (SM platform), in workplaces (medical institutions). Socio-technical system concepts have been extended to develop principles that could be used to address online information security challenges, (Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, & Lenzini, 2014). Thus, the principles were developed in recognition for the need to have a broader, integrated, and interactive perspectives of online information security requirements. Thus, a socio-technical information security approach advocates for usable-security principles, both in the social, and technical dimensions of information security design, in a holistic and seamless way (Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, & Lenzini, 2014). Therefore, SM usage being an online application would fit within the domain of socio-technical system theory, and usable-security concepts. Figure 1 below shows the structure of a socio-technical system theory.

Socio-technical system theory

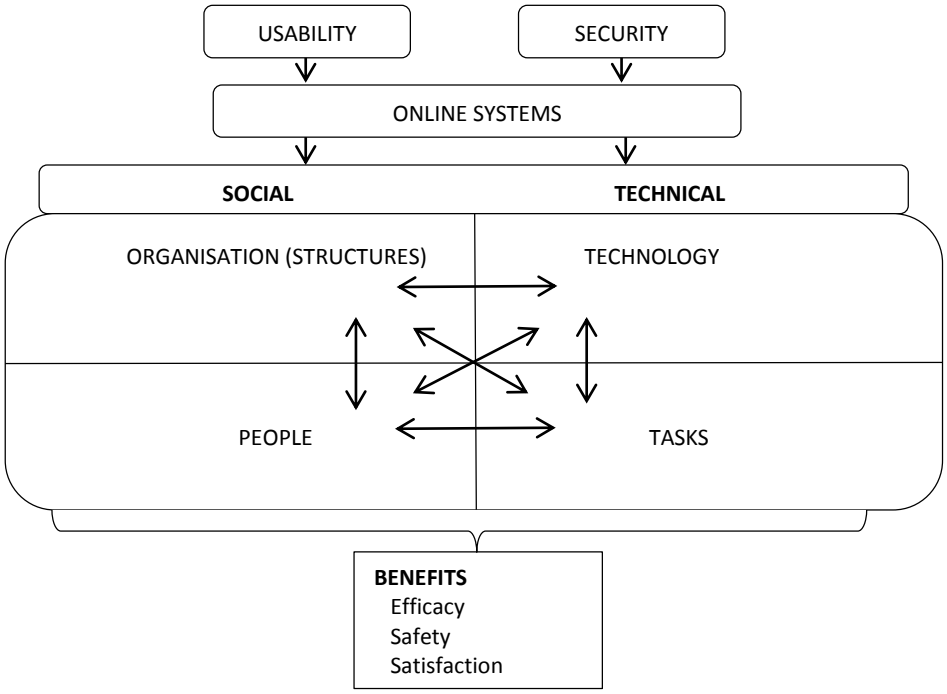


Figure 1: Structure of socio-technical system theory (Mujinga, Eloff & Kroeze, 2019)

Structurally, the main components of a socio-technical system theory include; 1) social dimension, comprising of individuals (people), and organizational structure (Paja, Dalpiaz, & Giorgini, 2013). In this case, the structure aspect consists of the policy and regulations, as well as responsibilities that guide the users on completion of related processes. 2) The technical dimension, consist of technology artifact, and task performed, which comprise of methods, techniques, and knowledge needed by users in translating system inputs into outputs (Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, &

Lenzini, 2014). With respect to SM usage, the corresponding subcomponents include; people – SM users (medical students, and medical staff including supervisors), structure – policy and regulations on SM usage, technology – SM platforms, and task performed – preserving the privacy and security of medical information. Therefore, this study would fit within the domain of socio-technical system constructs, as guided by the structure of the theory (Mujinga, Eloff & Kroeze, 2019). Each of the relevant usable-security principles identified in Section 2.4 would then fits within the 4 corresponding subcomponents of socio-technical system theory. However, according to Mujinga, Eloff & Kroeze, (2019), social dimension factors can be categories into; usability factors – education and training factors, and communication factors. While the technical dimension could be categorized into security and privacy factors, and system development factors, accordingly.

2.8 SM socio-technical information security factors

Subsequently, from the precept of socio-technical system theory, and SM being an online information system, the term SM socio-technical information security factor would then fit the nomenclature adopted in this study (Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, & Lenzini, 2014). From Table 1, and 2, the common factors dominating in all the 3 main sets of literatures (SMISF, STF and USF) were considered appropriate and relevant for inclusion into the list of SM socio-technical information security factors. In this case, the key factors scrutinized and identified under social dimension include; 1) usability factors – *visibility*, *learnability* and *satisfaction*, 2) training and education factors – *help* and *documentation*, and *user language* (Schneiderman, el al., 2016; Preece, Rogers & Sharp, 2015; Zahidi, Yan Peng Lim, & Woods, 2014; Yeratziotis, Pottas, & Van Greunen, 2012). On the other hand, the key factors identified under technical dimension include; 3) SM technology development factors – *error handling*, and *process revocability*; 4) information security factors – *security*, *privacy* and *confidentiality*, and *expressiveness* (Tayouri, 2015; Yeratziotis, Pottas, & Van Greunen, 2012). Therefore, with respect to SM usage, the relevant factors would then be the common factors of the elements represented by intersection set, (SMISF ∩ STF ∩ USF). Figure 2 below present a venn-diagram indicating the common factors of the set elements accordingly.

SM socio-technical information security factors

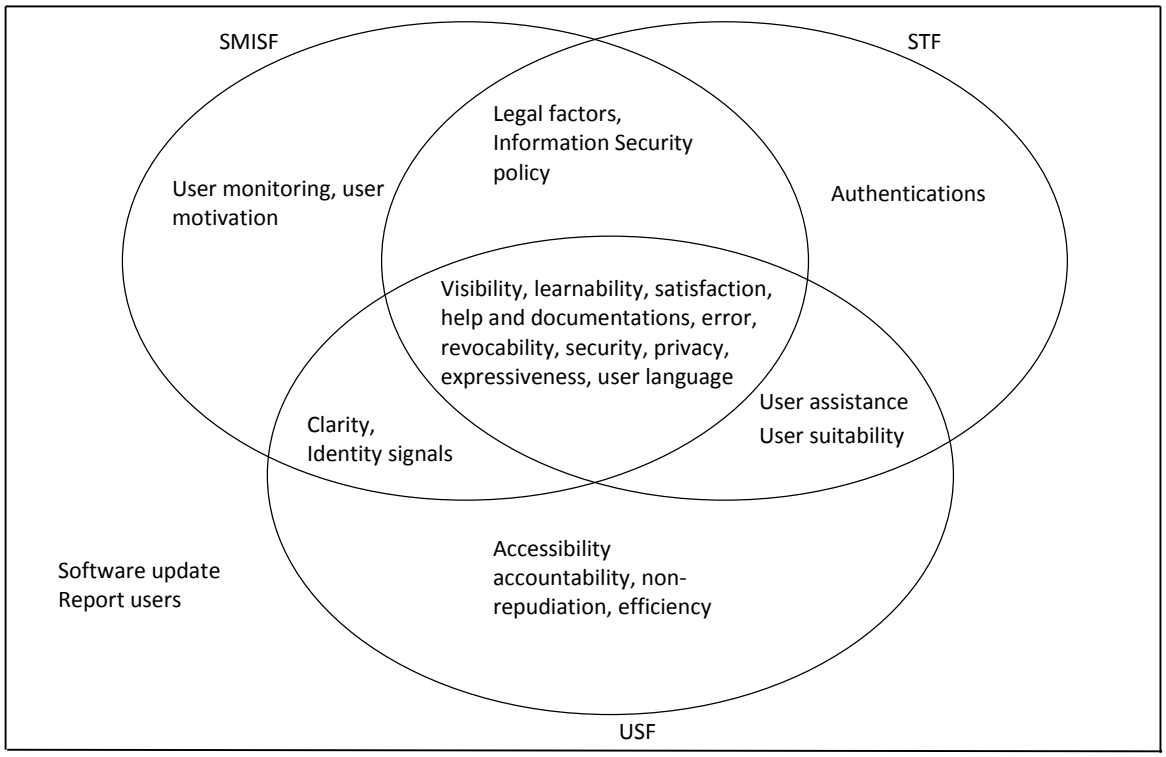


Figure 2: SM socio-technical information security factors (Mutebi, et al., 2022)

2.9 Guiding Model

Subsequently, from the structure and constructs of socio-technical system theory, and the extended DeLone and McLean theory of ISSM, a secure adoption of SM usage would then be the net benefits, both in the socio-technical system theory, and the extended DeLone and McLean theory of ISSM. (Edgardo, Indira, Monica & Wenli, 2018). In this case, socio-technical system theory provide a basis to identify the relevant information security factors in the context of SM usage. While ISSM provide a suitable framework for analyzing the relationships between information security factors, SM usage (adoption), and medical information safety. Thus, the extended DeLone and McLean theory describes the success of information systems by taking into account the quality of the data/information, system quality, and the service quality, which have impact on usage and user satisfaction, and eventually produce net benefit – SM usage (adoption), (Edgardo, Indira, Monica & Wenli, 2018). In this case, information quality, system quality, and service quality are factors identified under technology dimension, which correspond to the system development factors and information security factors identified under socio-technical system constructs (Mujinga, Eloff & Kroeze, 2019; Schneiderman, el al., 2016; Preece, Rogers & Sharp, 2015). Additionally, the social dimensional factors added include usability factors, and education and training factors (Mujinga, Eloff & Kroeze, 2019;

Tamarah & Samantha, 2018; Tayouri, 2015). Figure 3 below presents the structure of the guiding model for this study (Edgardo, Indira, Monica & Wenli, 2018).

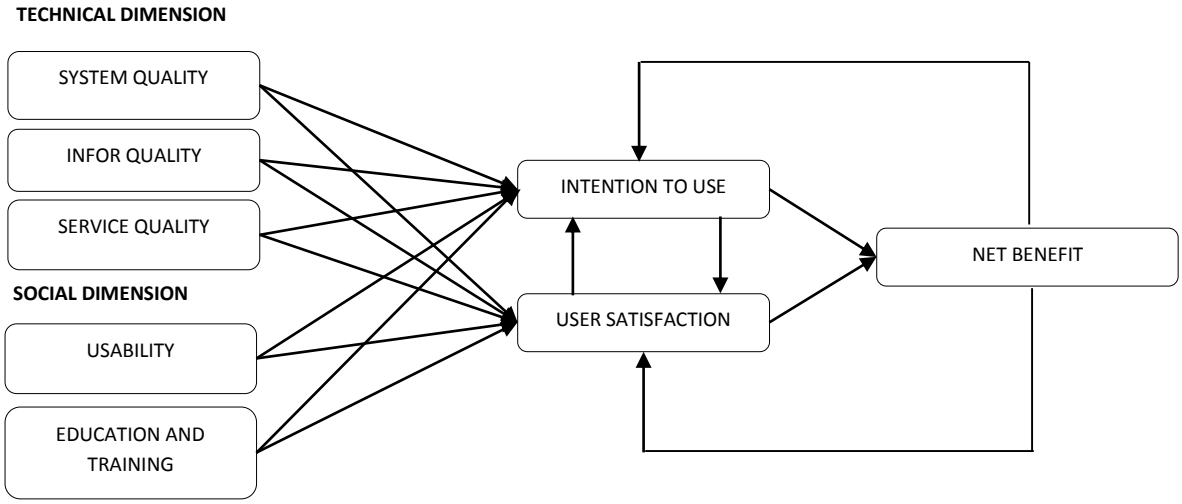


Figure 3: Guiding Model, IS success model (Edgardo, Indira, Monica & Wenli, 2018)

2.10 Conceptual Model

On the basis of the literature reviewed, and the theoretical guideline advanced, the researcher opted for an abductive reasoning approach, pinned by socio-technical systems theory, extended DeLone and McLean theory, and usable-security principles (Edgardo, Indira, Monica & Wenli, 2018; Tamarah & Samantha, 2018; Bhattacherjee, 2012). Subsequently, the researcher derived the following key study constructs, and variables in the context of SM usage, and medical information safety. The constructs identified under SM usage include; 1) social dimensional factors, comprising of individuals (people), and structure (organizations) (Paja, Dalpiaz, & Giorgini, 2013). In this case, the structure component consists of the policy, regulations, and responsibilities that guide the users on completion of related processes. 2) The technical dimensional factors, consist of technology, and task performed, which comprise of methods, techniques, and knowledge needed by users in translating system inputs into outputs (Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, & Lenzini, 2014). Therefore, each of the usable-security principles identified in section 2.6 fits into the 4 subcomponents of socio-technical system theory; people – SM users (medical students, and medical staff), structure – policy and regulations on SM usage, technology – SM platforms, and task performed – preserving medical information safety during teaching, learning, research, and clinical services. Hence, this study would fit within the domain of socio-technical system theory, ISSM, and usable-security principles as guided by the model (Figure 2). Therefore, using the abductive reasoning approach, the relevant variables were then derived from the 4 subcomponents of the social, and technical dimensions of SM usage domain, accordingly. Figure 4 below summarizes the key factors

identified and used in formulating the conceptual model, (Mujinga, Eloff & Kroeze, 2019; Edgardo, Indira, Monica & Wenli, 2018; Tamarah & Samantha, 2018).

Conceptual model: SM socio-technical information security factors: SM usage (adoption)

SM socio-technical Information Security factors (**IV**) SM usage (adoption) (**DV)**

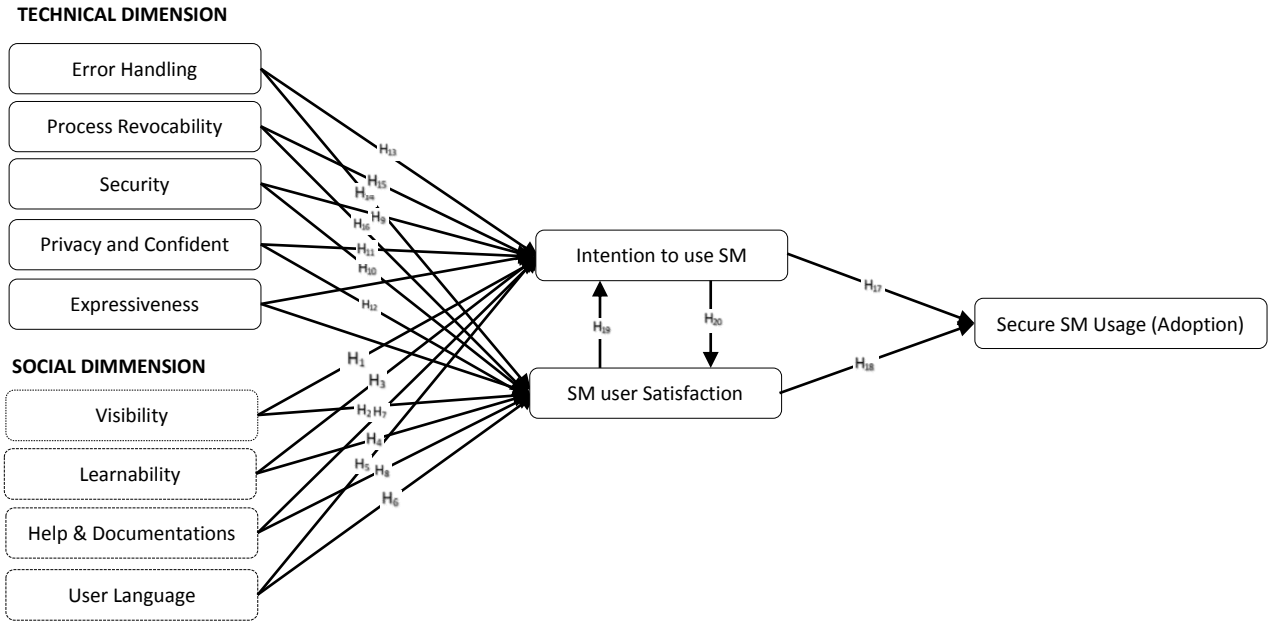


Figure 4: Conceptual model (Mutebi et al., 2022)

The conceptual model is based on socio-technical system theory concepts, IS success model, and usable-security principles, adopted from existing literatures, as guided by socio-technical system theory, extended DeLone and McLean theory of ISSM, and usable-security principles (Mujinga, Eloff & Kroeze, 2019; Edgardo, Indira, Monica & Wenli, 2018; Ferreira, Koenig, & Lenzini, 2014). In this case, SM socio-technical information security factors (predictor) was conceptualized as independent variables, influencing the activity of SM usage and medical information safety. Therefore, as guided by the theories, SM socio-technical information security factors were identified and associated with SM usage and medical information safety – defined by the levels of medical information breaches (Mujinga, Eloff & Kroeze, 2019; Househ et al., 2018; Ferreira, Koenig, & Lenzini, 2014; Kagoya et al., 2013). Thus, the key factors identified under social dimension include; 1) usability factors – *visibility*, *learnability*, and *satisfaction*; 2) training and education factors – *help* and *documentation*, and *user language*. While factors identified under technical dimension include; 3) SM technology development factors – *error handling*, and *revocability*; 4) task performed factors – *security*, *privacy* and *confidentiality*, and *expressiveness* (Mutebi, et al., 2022; Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig, & Lenzini, 2014). However, to operationalize the study concepts and variables,

appropriate research methods, approaches, and techniques were identified. Hence, the overall research doctrine was guided by research philosophy and research design relevant to the study (Boucher, 2015). Overall, this study was conducted in a formal organization settings, and mainly guided by objectivity principles, but also recognized the influence of subjectivity in the study process. Subsequently, the following hypothesis were formulated and tested accordingly.

H_1: *Visibility* is a significant and positive predictor of *intention to use SM*. H_2: *Visibility* is a significant and positive predictor of *SM user satisfaction*. H_3: *Learnability* is a significant and positive predictor of *intention to use SM*. H_4: *Learnability* is a significant and positive predictor of *SM user satisfaction*. H_5: *User language* is a significant and positive predictor of *intention to use SM*. H_6: *User language* is a significant and positive predictor of *SM user satisfaction*. H_7: *Help and documentation* is a significant and positive predictor of *intention to use SM*. H_8: *Help and documentation* is a significant and positive predictor of *SM user satisfaction*. H_9: *Security* is a significant and positive predictor of *intention to use SM*. H_{10}: *Security* is a significant and positive predictor of *SM user satisfaction*. H_{11}: *Privacy and confidentiality* is a significant and positive predictor of *intention to use SM*. H_{12}: *Privacy and confidentiality* is a significant and positive predictor of *SM user satisfaction*. H_{13}: *Error handling* is a significant and positive predictor of *intention to use SM*. H_{14}: *Error handling* is a significant and positive predictor of *SM user satisfaction*. H_{15}: *Process revocability* is a significant and positive predictor of *intention to use SM*. H_{16}: *Process revocability* is a significant and positive predictor of *SM user satisfaction*. H_{17}: *Intention to use SM* is a significant and positive predictor of *secure SM usage*. H_{18}: *User satisfaction* is a significant and positive predictor of *secure SM usage*. H_{19}: *User satisfaction* is a significant and positive predictor of *intention to use SM*. H_{20}: *Intention to use SM* is a significant and positive predictor of *user satisfaction*.

2.11 Chapter Two summary

In conclusion, chapter two examined, and summarizes the relevant literatures in line with the study objectives. With respect to specific objective 1, the relevant literatures articulate medical information security requirements with respect to SM usage. Thus, from patient's charter 2019, used in safeguarding patient's rights to medical information safety in Uganda was a useful reference document guiding on medical information security requirements (UCC 2020; Nabimanya, et al., 2020; Kagoya et al., 2013). According to the charter, and the other related literatures, preserving medical information safety mandates an individual to control the acquisition, access, uses, and disclosure of identifiable medical information (HIPAA, 2020; Househ et al., 2018; Brodnik, 2012). However, individual rights could be extended through informed consent or by law to other parties,

but the extended parties must ensure confidentiality (Kagoya et al., 2013). Therefore, confidentiality mandates those who access medical information, such as medical students, supervisors and stakeholders to safeguard the privacy interests of the persons to whom the information is related (Beltran-Aroca, et al. 2016; Brodnik, 2012). In this case, medical information breaches would occur when identifiable medical information is acquired, used, or disclosed without informed consent, or legal mandate. Therefore, the definition of what constitute medical information breaches was clarified by the patient's charter of 2019, while taking into considerations the other relevant literatures, accordingly (HIPAA, 2020; Nabimanya, et al., 2020; Househ et al., 2018; Kagoya et al., 2013).

Furthermore, the key SM socio-technical information security factors were identified as guided by socio-technical system theory, SM usage, and usable-security principles (Mujinga, Eloff & Kroeze, 2019; Ferreira, Koenig & Lenzini, 2014; Yeratziotis, Pottas & Van Greunen, 2012). In this case, the key factors identified under social dimension include; 1) usability factors – *visibility*, *learnability* and *satisfaction*, 2) training and education factors – *help* and *documentation*, and *user language* (Schneiderman, et al., 2016; Preece, Rogers & Sharp, 2015; Yeratziotis, Pottas & Van Greunen, 2012). Meanwhile, the key factors identified under technical dimension include; 3) SM technology development factors – *error handling*, and *process revocability*; and 4) information security factors – *security*, *privacy* and *confidentiality*, and *expressiveness (*Mujinga, Eloff & Kroeze, 2019; Yeratziotis, Pottas & Van Greunen, 2012). Altogether, the outputs of specific objectives 1 was used to provide data inputs to specific objective 2, 3 and 4, accordingly. Whereby, the relevant constructs, concepts and variables were identified and defined within the domain of SM usage, and medical information safety. In this case, relating SM socio-technical information security factors with SM usage and medical information safety levels – defined by the levels of medical information breaches. Thus, SM socio-technical information security factors were conceptualized as independent variables, influencing the activity of SM usage and medical information safety as dependent variable accordingly (Tamarah & Samantha, 2018; Bhattacherjee, 2012).

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Research methodology stipulates scientific approaches, tools and techniques intended to realize the objectives of the study (Tamarah & Samantha, 2018). Therefore, appropriate methods were identified and selected based on their matching suitability to handle data requirements relevant to this study. In line with the study objectives, chapter three specifies the relevant approaches, tools and techniques, and explained them under the following sections of the chapter; research philosophy, research approach and strategy, research design, the study population and sampling design, instrument development and pretesting, pilot testing, data collection procedures, data processing, data analysis, and ethical consideration accordingly.

3.2 Research Philosophy

The philosophy of this study was based on post-positivism philosophy – functionalist paradigm (Tamarah & Samantha, 2018). Relatively, functionalist paradigm postulate that; "social order or patterns could be understood in terms of their functional compositions, and therefore try to break down a problem into small components and study one or more components in detail using objectivist techniques such as survey" (Tamarah & Samantha, 2018). The appropriate method for such orderly system is to epistemologically employ objectivist approach, which is autonomous from the researcher's observation or interpretation. In line with this study, the researcher believes in such orderly setting, thus seeking to study pattern of orderly entities and social happening. In this case, the social (subjective) and technical (objective) attributes that defines SM usage in medical education are presumed to be established in an orderly settings, where operations are rationally defined by policy, rules and regulations (Mujinga, Eloff, & Kroeze, 2019; Roy et al., 2016). Hence, post-positivism and functionalist paradigms take into context both the subjective and objective nature of the study environment, but employed objectivist approaches to tailor the research process accordingly (Zamanzadeh, et al., 2015; Boucher, 2015; Bhattacherjee, 2012).

Thus, activities defined under functionalism research paradigm are normally categorized into 3 phases of research processes. The phases include; 1) *exploration phase*, 2) *research design phase*, and 3) *research execution phase* (Tamarah & Samantha, 2018; Bhattacherjee, 2012). *Exploration phase* deal with exploration of literatures, and selection of research questions leading to further investigation. In this case, published literatures related to the study area were reviewed, and the

relevant research objectives, and research questions identified accordingly. The details of what has been done in the exploration phase are stipulated and summarized in chapter one, and two respectively. However, the subsequent chapters and corresponding sections covered research design phase, and research execution phase accordingly. *Research design phase* focused on the work plan (blue print) and tasks to be executed, and reasonably provide answers to the research questions formulated. In this case, the work plan included selection of appropriate research methods, and research techniques, implementation of identified constructs, and developing a suitable strategy of sampling process. Meanwhile, *research execution phase* entailed validation (pretesting, and pilot testing) of the research instruments, identification and operationalization of appropriate data collection tools and techniques, data analysis as well as report writing, and publishing of results and the findings accordingly (Zamanzadeh, et al., 2015; Bhattacherjee, 2012).

3.3 Research Approach

This study followed an abductive reasoning approach. Typically, abductive reasoning starts with a partial set of observations and moves on to the most likely explanation for the set (Tamarah & Samantha, 2018). Thus, making observations and looking for the hypothesis that best fits or explains the situation is the logical process of abductive reasoning (Tamarah & Samantha, 2018). A new hypothesis is then reached through deductive reasoning that involve a theory. In this case, the socio-technical system theory, the extended DeLone and McLean theory of Information System Success Model (ISSM), coupled with usable-security principles guided the research process. Whereby, the process logically moved from the stated theories to the particular constructs, concepts, and variables of the study. Subsequently, the hypothesis is then put to the test by comparing the hypothesis to observations, which either corroborate or disprove it. In this case, the theories provided a basis for identification and validation of SM socio-technical information security factors and the development of the intended model accordingly.

3.4 Research Design

Research design suited for this study is mixed method design, combining qualitative and quantitative methods. Mixed method design brought together multifaceted techniques that combined and exploited on the strength of specific methods and techniques, while minimizing weaknesses that may emanate due to a single design approach (Kabir, 2016). Therefore, using quantitative approach, descriptive and correlational designs allowed variables to be objectively described, and the relationships between them tested accordingly. While quasi-experimental design allowed researcher to examine cause-effect relationships between independent and dependent variables. For data

collection instrument, online questionnaire survey were developed, validated and operationalized accordingly. Typically, the key respondents included medical students, and medical staff from Mbarara University of Science and Technology (MUST), and Kampala International University (KIU) accordingly. The main items captured in the questionnaire include respondents' demographic profiles, SM usage characteristics, SM socio-technical information security factors, and medical information breaches. Both descriptive and inferential statistics were employed in data analysis process. However, qualitative approach (interview) was intended to mainly help in probing and clarifying on the quantitative findings, as well as checking on the reliability of the datasets. As such, data collection process took into consideration both primary and secondary data sources accordingly (Tamarah & Samantha, 2018; Kabir 2016; Bhattacherjee, 2012).

3.5 Study Population

The study population (N) was constituted by 2300 medical (MBChB) students, and 175 medical staff (Bongomin et al, 2021; Olum & Bongomin 2020). The population members were identified from 2 selected medical institutions in Uganda; 1) Mbarara University of Science and Technology (MUST) Faculty of Medicine; 2) Kampala International University (KIU) Faculty of Clinical Medicine and Dentistry accordingly. Relatively, both MUST and KIU have dedicated teaching hospitals, handling over 1500 medical students in a single semester (Bongomin et al, 2021). Thus, the criterion used in selecting the medical institutions was based on recognition by national authority, which signify a better status of system establishment favorable for such a study (Khamala, Makori & Njiraine, 2018; UMDPC, 2017). From MUST, the estimated population of medical (MBChB) students within a semester session were 800, and the number of corresponding medical staff and supervisors were 75; while at KIU, the estimated population of medical (MBChB) students within a semester session were 1500, and the corresponding medical staff and supervisors were 100. Overall, the total estimated population was 2300 + 175 = 2475 accordingly (Bongomin et al, 2021; Olum et al, 2020; Olum & Bongomin 2020). Altogether, the appropriate sample size was then determined based on the estimated population of 2475, taking into consideration the minimum response rate of 50%, and attrition rates associated with online survey (Tamarah & Samantha, 2018; Taherdoost, 2016).

3.6 Sample Size

Therefore, using the target population (N) of 2475, appropriate sample size (n) was determined using a generated sample size table, but based on Morgan and Krejcie techniques (Taherdoost, 2016; Gill et al., 2010). The sampling process took into considerations the finite and heterogeneous characteristics of the target population. In this case, the researcher intended to include all the sub-

groups of the target population into the study sample. Therefore, Morgan and Krejcie technique was considered appropriate technique for determining the sample size, since the technique takes into consideration the heterogeneous characteristics of the population, confidence interval level of 95%, and minimum response rate of 50%. Which were commensurate with the study design, and research work-plan (Taherdoost, 2016). Therefore, using Morgan and Krejcie method, the researcher derived appropriate sample size using a generated sample size table, but based on the formula below (Casteel & Bridier, 2021; Taherdoost, 2016; Gill et al., 2010):

"$n = X^2NP(1-P) / d^2(N-1) + X^2P(1-P)$

n = required samaple size

X^2 = the table value of chi-square for 1 degree of freedom at the desired confidence level (3.841)

N = the population size

P = the population proposation (assumed to be 50 since this would provide the maximum sample size)

d = the degree of accuracy expressed as a propoation (0.05)"

Subsequently, the required sample size was then estimated based on population and sample size table, taking into consideration the minimum of 50% response rate (Taherdoost, 2016; Amin, 2005). Table 4 below shows the summary of the target population, and the expected sample sizes within each category of the target population, which add up to the composite sample size of 710 including medical students and medical staff from both MUST and KIU, accordingly.

Table 4: Population and Sample size

MEDICAL INSTITUTIONS	MUST			KIU		
Respondents	Medical Students	Medical staff	**Total**	Medical Students	Medical staff	**Total**
Target population	800	75	**875**	1500	100	**1600**
Sample size	260	64	**324**	306	80	**386**
Morgan and Krejcie technique (N = 2475, n = 710) (Tamarah & Samantha, 2018; Taherdoost, 2016)						

3.7 Sampling Method

From the target population and sample size defined, proportional stratified sampling was used to ensure that all the categories of potential respondents in the target population were fairly represented in the sample study. Taking into consideration the estimated minimum response rate of 50%, and attrition rates associated with online survey (Taherdoost, 2016; Bhattacherjee, 2012). In this case, the researcher stratified sub-groups of medical (MBChB) students in year 3, 4 and 5, together with their corresponding medical staff including supervisors. Subsequently, simple probability sampling was

carried out within each stratum (sub-group). The advantage of proportional stratified sampling is that the unique proportionality of the sub-group identified in the target population is retained in the study sample (Taherdoost, 2016). While, simple probability sampling ensured that all the members within the sub-group were given equal probability chance of being selected in the final study sample (Taherdoost, 2016; Bhattacherjee, 2012).

3.8 Instrument Development Process

The questionnaire design and development processes was guided by study objectives and the characteristics of respondents (Appendix C & D). The questionnaire items consist of mainly 4 sections; 1) introduction section; explains the intention of the researcher, the purpose of data collection, and anonymity assurance to respondents. 2) Demographic profile section; covers demographic characteristics of the respondents. 3) SM usage section; covers the types of SM platform used, the level of SM usage engagement, and medical information breaches. 4) usable-security factors section; covers the views, perceptions, and experience of respondents on the key SM socio-technical information security factors identified in line with medical information safety. The response on SM socio-technical information security factors were then developed with a 5-points Likert scale measures, including; "1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree" (Zamanzadeh, et al., 2015; Joshi et al., 2015). However, interview guide (Appendix E) focused on probing and filling questionnaire gaps, by clarifying on quantitative evaluation findings, as well as checking on some of the reliability of data generated through questionnaire. Documents such as policy on ICT and SM usage, and medical curricula were scrutinized through document review to reveal additional details linked to SM usage, and medical information safety accordingly.

3.9 Instrument Testing

Eventually, instrument validation (pre-test, and pilot-test) were conducted to assess the validity, and reliability of the data collection instrument – questionnaire, as well as checking how the selected techniques would perform under the intended study conditions. Pre-test and pilot-testing assisted in identifying incomprehensible questions as well as any issues with the questionnaire that could result in biased results. (Tamarah & Samantha, 2018; Zamanzadeh, et al., 2015). In this case, the primary objective of the instrument validation was to identify and correct problems before implementing the instruments in the actual data collection and analysis process. Therefore, instrument pre-test focused on the validity of the questionnaire instrument, while pilot-test focused mainly on reliability of the instrument. In this case, validity was concerned with "how the measures sufficiently represent the construct that it was supposed to measure", while reliability was mainly concerned with "the extent

to which the measures of the construct were consistent and dependable" (Tamarah & Samantha, 2018; Zamanzadeh, et al., 2015).

3.10 Validity Test

In line with abductive reasoning approach, this study followed empirical approach of validity testing, which is the most widely used technique (Zamanzadeh, et al., 2015). The technique focuses more on how the constructs are translated into operational measures. In this case, face validity was performed using 8 subject experts (Lecturers), and 2 potential respondents (Students), who evaluated how each indicator match the definition of the constructs. Similarly, content validity was also performed to evaluate how the scale indicators match the content aspect of the constructs. Validity forms were then developed based on a 4-points rating scales (Appendix H), focusing on the "relevancy", and "clarity" of the items (questions). The form also contained section on instructions to guide the reviewers. From the score ratings of the reviewers, Content Validity Index (CVI) was calculated using Item Content Validity Index (I-CVI) and Scale Content Validity Index (S-CVI). Thus, taking into consideration the minimum expected CVIs of 0.78 (Zamanzadeh, et al., 2015; Joshi et al., 2015; Bhattacherjee, 2012). Items which were responsible for lower CVIs were revised as guided by the experts accordingly. Table 5 below shows the results of the computed CVIs, based on the reviewers rating of relevancy, and clarity of the questionnaire items (questions) accordingly.

Table 5: Validity test results (Item relevancy, and clarity)

FACTORS	No of Items	No of Strong Validity Items	No of Weak Validity Items	Relevancy CVI ≥ 0.78	Clarity CVI ≥ 0.78	Conclusion
Visibility (VB)	5	3	2	0.91	0.77	Revised
Learnability (LN)	5	5	0	0.87	0.91	Acceptable
User satisfaction (US)	5	5	0	0.84	0.90	Acceptable
Intention to use (ITU)	5	5	0	0.85	0.87	Acceptable
Error handling (EH)	5	3	0	0.84	0.86	Acceptable
Revocability (RV)	5	5	0	0.78	0.82	Acceptable
Help and *documentation (HD)*	5	4	1	0.96	0.74	Revised
User language (UL)	5	5	0	0.84	0.90	Acceptable
Security (SC)	5	5	0	0.83	0.89	Acceptable
Privacy and *confidentiality (PC)*	5	5	0	0.94	0.81	Acceptable
Expressiveness (EX)	5	4	1	0.83	0.72	Revised
Secure SM usage (SM US)	5	4	1	0.82	0.81	Acceptable
MIBR	4	3	1	0.92	0.84	Acceptable
Weaker items were revised as guided by the experts accordingly (Tamarah & Samantha, 2018; Zamanzadeh, et al., 2015)						

3.11 Reliability test

On the other hand, reliability test was performed to assess the extent to which the measures of the constructs were consistent and dependable. Specifically, the researcher used inter-rater reliability test, which is usually the degree of consistency between independent raters of similar construct (Taherdoost, 2016; Bhattacherjee, 2012). Normally, this could be done in two ways as guided by the different levels of measurements. 1) For categorical measures, category sets were defined, and independent raters indicated the category set for each observation, and percentage of agreement among independent raters was then used to estimate the consistency in the response. Altogether, 32 respondents rating the observations were selected and used, and their agreement rating score was greater than 80%, which suggests satisfactory level of reliability results (Taherdoost, 2016). 2) For ordinal scale measures, Cronbach's alpha coefficient (α-values) was used to estimate the reliability of the ordinal items (Taherdoost, 2016; Joshi et al., 2015). Items with $\alpha \geq 0.70$ were considered to be strong reliability items, while those with α-values ranging from 0.50 to 0.70 were considered moderate reliability items, and those with $\alpha < 0.50$ were considered weak reliability items (Joshi et al., 2015). Table 6 below shows the reliability test results for the ordinal items.

Table 6: Reliability test results

FACTORS	No of Items	No of Strong Reliability Items	No of Moderate Reliability Items	$0.70 \leq \alpha \leq 0.90$	Conclusion
Visibility (VB)	5	5	0 revised	0.811	Acceptable
Learnability (LN)	5	5	0 revised	0.701	Acceptable
User satisfaction (US)	5	5	0 revised	0.859	Acceptable
Intention to use (ITU)	5	5	0 revised	0.887	Acceptable
Error handling (EH)	5	4	1 revised	0.722	Acceptable
Revocability (RV)	5	3	2 revised	0.649	Acceptable
Help and documentation (HD)	5	4	1 revised	0.716	Acceptable
User language (UL)	5	5	0 revised	0.812	Acceptable
Security (SC)	5	5	0 revised	0.721	Acceptable
Privacy and confidentiality (PC)	5	5	0 revised	0.799	Acceptable
Expressiveness (EX)	5	4	1 revised	0.860	Acceptable
Secure SM usage (SM US)	5	5	0 revised	0.863	Acceptable
MIBR	4	4	0 revised	0.843	Acceptable
Weak and moderate items were revised accordingly, (Tamarah & Samantha, 2018; Zamanzadeh, et al., 2015). Additionally, visual display: graphs and charts were generated to revel outlier in the dataset.					

Furthermore, visual displays (graphs and charts) were generated to reveal the behavioral pattern within the datasets. The results helped to gain more insight into the datasets, such as identifying

outliers and features of the data that were not anticipated, (Appendix G). Nevertheless, the researcher is cognizant of the fact that instrument development process is often a challenging task, and if poorly handled, would results into inappropriate results, and any good analysis would not remedy the situation (Joshi et al., 2015; Bhattacherjee, 2012). And so, amendment and refinement of the questionnaire items (questions) were done repeatedly to further streamline the questions which were ambiguous. Subsequently, the final instruments developed was used in the confirmatory phase of the study, which dealt with the final data collection, data presentations, data analysis, results discussion, recommendation, and publishing accordingly (Bhattacherjee, 2012). Not forgetting the objective of the instrument testing, which was to identify and correct ambiguity before implementing the instruments in the final phase of the study (Zamanzadeh, et al., 2015).

3.12 Data Collection

Beside instrument development and validation, data collection process is in itself a significant aspect of many researches, and any imprecise data could negatively influence on the outcomes of the study and eventually lead to unacceptable or inaccurate results (Tamarah & Samantha, 2018; Bhattacherjee, 2012). And so, the researcher took into consideration the relevance of the instruments selected, and the design process followed. In questionnaire design, replies were restricted to answer the prepared questions, whereas interviews offered the chance to collect nonverbal data while decoding the meaning of questions. Largely, the study relied on questionnaire instrument to collect quantitative data. Logically, the questionnaires were designed to have structured responses to fit the varied experiences into prearranged response categories. And so, close-ended questionnaires generated results that were simple to generalize, compare and summarize, but limited by the structural nature of the responses (Zamanzadeh, et al., 2015; Joshi et al., 2015). Therefore, using questionnaire, the researcher collected data on respondent demographic profiles, SM usage characteristics, medical information breaches, and SM socio-technical information security factors, while statistically controlling the influence of intervening variables. And since the intent of this study was to generalize from the sample to the population, the researcher capitalized on probability sampling in selecting the study participants (Zamanzadeh, et al., 2015; Bhattacherjee, 2012).

However, interview was used to generate more open-ended qualitative data. Interviews tend to be open and unstructured, which helped to provide information needed to comprehend the concepts behind the observed outputs, as well as evaluating changes in peoples' opinions. In this case qualitative methods helped to improve on the quality of quantitative evaluations. Some respondents were followed numerous times to trail on specific issues, and concepts, or confirm reliability in the

datasets. However, both questionnaire and interview methods were meant for primary data. However, the researcher employed content and document analysis to collect secondary data to substantiate some of the facts generated through questionnaire and interview. In this case, selected SM contents and the historical records of SM contents were examined to reveal and confirm some of the relevant facts related to medical information safety. The researcher took records of important and relevant facts, using photographs, audio recording and other appropriate means (Appendix G). Nevertheless, to minimize errors and process flaws, data gathering process seriously took into consideration data processing, and data cleaning process accordingly.

3.13 Data Processing and Data Cleaning

After data collection, datasets were processed, cleaned and prepared for analysis. In this case, data processing and data cleaning dealt with the following sets of activities; 1) Questionnaire checking to eliminate improper questionnaires; thus 8 questionnaires were found inadequate, where instructions were not followed properly, while 6 were incomplete. 2) 5 questionnaires were edited to correct anomalies such as; illegibility, incomplete data, inconsistent and vague answers. 3) Coding was then performed to allocate alpha and numeric codes to responses that did not have them so that objective statistical methods could be applied on SPSS. 4) Cleaning was done to review data and correct data inconsistencies that came from faulty reasoning, out of range or outlier. 5) Statistical regulations to data requiring weighting and scale translation were done; thus medical information breaches dataset were transformed to medical information safety. 6) Analysis strategy choice (normality test) was performed to select data analysis approach following earlier work used in developing the research, but was concluded after consideration of the characteristics of the data that has been gathered, (Taherdoost, 2016). Eventually, 710 valid questionnaires were considered and sanctioned for analysis process using statistical tools outlined in the following sections.

3.14 Data Analysis

Ultimately, quantitative data analysis was performed using SPSS version 26, supported by SmartPLS, and MS Excel. While qualitative dataset were analyzed using thematic content analysis method (Tamarah & Samantha, 2018). The advantage of SPSS over the other statistical analysis packages is its ability of being comprehensive, and can easily import and display quantitate datasets captured from other sources, specifically data captured in MS Excel format linked to online Google forms, which helped the researcher to ease the impact of the time constraint limitations (Tamarah & Samantha, 2018). Overall, the analysis process took into consideration both the descriptive, and inferential statistics. In this case, appropriate statistical tools were then identified and used to generate

meaningful information useful for answering the intended research questions. Afterwards, make recommendations, suggestions and draw conclusion appropriately (Tamarah & Samantha, 2018; Taherdoost, 2016; Bhattacherjee, 2012).

3.15 Descriptive data analysis

Eventually, descriptive statistics was intended to generate results necessary to explain the sample variables without generalizing the results to the population. Therefore, using SPSS software, appropriate statistical tools employed included univariate and bivariate statistical analysis tools accordingly; 1) Univariate analysis tools included frequency counts, and percentage distributions, measure of central tendency such as median and mode. 2) Bivariate analysis statistical tools included mainly visual display such as; scatter plots, tables and charts (Appendix G). Altogether, the detailed analysis results are presented in chapter four and five accordingly.

3.16 Inferential data analysis

On the other hand, inferential statistics dealt with statistical analysis process used to make inferences from the sample to the general population. In this case, the respective ordinal datasets were first converted into their numerical equivalents of 5-points Likert scales, with the following levels of measurements; "1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree". According to Joshi et al. (2015), interval scale/ordinal measures is appropriate for a composite Likert scale items. As guided by the preliminary test results of the datasets, the appropriate statistical options included chi-square test, Spearman's Rank correlations, and Ordinal Regression analysis. In line with this study, regression analysis provides a more detailed analysis including equations, which can be used for prediction and/or optimization based on numbers and statistics. However, regression may not be appropriate for qualitative phenomenon (Tamarah & Samantha, 2018). Chi-square test was mainly used to assess the level of associations between selected demographic datasets and medical information breaches. While, Spearman's Rank correlation estimated the strength and direction of correlations between SM socio-technical information security factors, and SM usage and medical information breaches. Overall, Ordinal Regression analysis results (R^2-*values,* and *p-values*) were used to determine the predictive strength of the relationships between independent variables – SM socio-technical information security factors, and dependent variable – SM usage and medical information safety levels respectively. Thus, hypothesis test was performed between SM socio-technical information security factors and SM usage accordingly. The detail of the analysis results, and the findings are stipulated in chapter four and five respectively.

3.17 Ethical Considerations

A set of guidelines called ethical considerations in research serve as a guide for research procedures and designs. The key ethical consideration linking research participants and this study was informed consent, where the anticipated risk was related to potential harm that could result from breach of confidentiality. Thus, this study did not involve human or animal material, (UNCST, 2014). Nevertheless, the researcher went through the due process of approval by respective research committees of the relevant institutions, including doctoral committee and medical institutions where data were solicited from. Procedurally, the different stages of research process were followed, including; concept and proposal approval, pre/pilot test approval, and examination process. With respect to research participants, the major issue included voluntary participations, anonymity, confidentiality, and analysis and reporting of the results to scientific community.

1) Voluntary participation by respondents: the participants in this study were informed and assured of their rights to voluntary participation (Appendix A & B). Therefore, participants had the liberty to consent or withdraw their participations from the study at their choice and will. In this case, all respondents obtained and signed a copy of informed consent form in the language they could easily read and understand. The form clearly described their rights of participation, and withdrawal, before capturing their responses, (Appendix B). The researcher also ensured that respondents participating were in good state of mindset, and 18 years and above. Therefore had the right to volunteer their participation in the study (Kabir, 2016; Bhattacherjee, 2012).

2) Anonymity and confidentiality: The identities of the institutions and participants in this study are protected using duel principles of anonymity. In this case, the researcher, or other readers of the final report would not be able to identify a specific respondent by their response in the study. Furthermore, anonymity ensured protection of subjects against authorities who could have interest in identification or tracking the participants later. In this case, the researcher ensured confidentiality of participants is not divulged in the final report, or paper as well as public forum.

3) Analysis and reporting: furthermore, the researcher also recognize the importance of ethical requirements concerning analysis process, and reporting research findings to the scientific community. Hence, any negative or unexpected findings was disclosed fully, irrespective of the research findings. Altogether, the researcher ensured that all the principles under voluntary participation, anonymity and confidentiality of participant, and scientific honesty were followed and maintained as would be expected (Kabir, 2016; Bhattacherjee, 2012).

3.18 Chapter Three Summary

In conclusion, this study followed post-positivism philosophy – functionalist paradigm, abductive reasoning approach, and mixed methods design. According to Bhattacherjee (2012), a functionalism research process can be categorized into 3 phases, namely; *exploration phase*, *research design phase*, and *research execution phase* respectively. 1) *exploration phase*; where the researcher explored the research area and selected research questions leading to further investigations, examining related literatures to understand the current knowledge gaps in existing studies, as well as identifying the relevant theory that helped to postulate and answer the research questions. The detail of the literatures reviewed are covered in chapter one and two accordingly. 2) The next phase was *research design phase*, which was used as a "blueprint" to empirically answer the research questions, taking into consideration three sub-processes; a) data collection process, b) instrument development process, and c) sampling process. The details under each sub-process are covered in chapter three. 3) The last phase is *research execution phase*, which dealt with pre/pilot test of data collection instruments, followed by actual data collection, data analysis, report writing, and results dissemination and publication respectively. While *research execution phase* is covered in the subsequent chapters – four, five, and six accordingly (Zamanzadeh, et al., 2015; Kabir, 2016).

CHAPTER FOUR

DATA PRESENTATIONS, AND ANALYSIS

4.1 Introduction

In line with the study objectives and research questions, chapter four covers data presentations, and data analysis. However, the opening sections of the chapter begins with a recap of the characteristics of the study population (N = 2475), and the derived sample size (n = 710) used. Followed by summary of the respondent demographic profiles, and analysis results and the findings, all presented in a narrative, tabular and chart formats accordingly. The statistical packages used include SPSS version 26, for both descriptive and inferential statistics, supported by SmartPLS, MS Excel and thematic content analysis accordingly.

4.2 Data Evaluation

The data used in this study was collected using online questionnaire (Google form) survey, and later processed and prepared for analysis. Overall, the sample size computed was 710, though 740 questionnaires were distributed to respondents consisting of 580 medical students, and 160 medical staff, all from MUST and KIU accordingly. In response, 718 questionnaires were duly completed and returned by respondents. However, after performing data cleaning process and sorting, 710 valid questionnaires were considered for analysis. Afterwards, data was coded and analyzed using SPSS version 26, taking into consideration the descriptive and inferential statistical requirements. As guided by specific objectives, the researcher intended to identify the key SM socio-technical information security factors, and establish the types of relationships between SM socio-technical information security factors, SM usage and medical information breaches. Subsequently, with respect to objective 4, Ordinal Regression analysis was performed to estimate the influence of independent variables on dependent variable. Thus, SM socio-technical information security factors (predictors) was conceptualized as independent variables, influencing the activity of SM usage and medical information safety as dependent variable.

4.3 The target Population, and Sample size

Overall, this study was conducted within selected medical institutions in Uganda. Using purposive sampling techniques, 2 medical institutions were selected; 1 from government affiliated institutions, and 1 from private owned institutions. The selection criteria was based on the accreditation and recognition status by national regulatory authority, which would imply a better status of system establishment appropriate for such a study (Khamala, Makori & Njiraine 2018). Therefore, medical

institutions selected were; 1) Mbarara University of Science and Technology (MUST) Faculty of Medicine; 2) Kampala International University (KIU) Faculty of Clinical Medicine and Dentistry (Bongomin et al., 2021; Olum & Bongomin 2020). Table 7 below presents a recap of estimated target population, and appropriate sample size derived from each medical institution, indicating the categories of respondents within the sub-groups, accordingly.

Table 7: Target population, and computed sample size

MEDICAL INSTITUTIONS	MUST			KIU		
Respondents	Medical Students	Medical staff	**Total**	Medical Students	Medical staff	**Total**
Target population (N)	800	75	**875**	1500	100	**1600**
Sample size (n)	260	64	**324**	306	80	**386**
Based on population and sample size determination table, (Taherdoost, 2016)						

Approximately, the sample size presented in Table 7 above were exaggerated to compensate for errors that could arise due to low response rate, or elimination due to data cleaning process, (Taherdoost, 2016). Thus, out of 710 exact sample size expected, the total inflated number of questionnaires sent to respondents were 740. However, after receiving and compiling all the questionnaires, the valid questionnaire considered for analysis were 710. Subsequently, both descriptive and inferential statistics were followed in analyzing the dataset, taking into consideration the research objectives, research questions, and the data types accordingly.

4.4 Descriptive Statistical Data

Comparatively, descriptive statistics was mainly used to help in understanding the characteristics of the datasets without inferring the result to the general population. In this case, the researcher summarized the datasets using narrative, and simple graphical illustrations such as; charts, and tables. The key items of the dataset considered under descriptive statistics include summary of demographic profiles, SM usage characteristics, medical information breaches, and respondent levels of agreement on SM socio-technical information security factors accordingly. The summary of the results within each section are presented with brief explanation about the key outputs and the findings of the section. However, the detailed discussion and interpretation of the analysis results and the findings are stipulated and presented in chapter five and six accordingly.

4.4.1 Summary of demographic profiles

As indicated in Table 7 above, the key respondents used in this study include 566 medical students, and 144 medical staff, accordingly. Therefore, with respect to the selected medical institutions

(MUST and KIU), Table 8 below presents the demographic profiles of the respondents, showing the representativeness of the members within the category divides. Thus, indicating the frequency counts, and the corresponding percentage distributions accordingly.

Table 8: Respondents demographic profiles.

	MEDICAL INSTITUTIONS	MUST				KIU			
	Demographic profiles	Medical students		Medical staff		Medical students		Medical staff	
1	Gender	*n = 260*	*(100%)*	*n = 64*	*(100%)*	*n = 306*	*(100%)*	*n = 80*	*(100%)*
	Male	151	58%	038	61%	171	56%	047	59%
	Female	109	42%	025	39%	135	44%	033	41%
2	Age group								
	18 – 25	195	75%	001	02%	197	64%	005	06%
	26 – 35	049	19%	014	22%	085	28%	022	27%
	36 – 45	011	04%	040	64%	014	05%	047	58%
	46 years and above	005	02%	008	13%	010	03%	007	09%
3	Nationality								
	Ugandan	235	90%	050	79%	270	88%	061	75%
	International	025	10%	013	21%	036	12%	020	25%
4	Year of study or class taught								
	Year 3/class 3	127	49%	031	49%	151	49%	041	51%
	Year 4/class 4	081	31%	018	28%	090	29%	027	33%
	Year 5/class 5	052	20%	014	22%	065	21%	013	16%
5	Denomination								
	Catholic	136	52%	038	60%	097	32%	028	35%
	Protestant	055	21%	011	18%	087	28%	034	42%
	Muslim	050	19%	007	11%	070	23%	005	06%
	Others	019	07%	007	11%	052	17%	014	17%
6	Medical department								
	Internal medicine	029	11%	007	11%	037	12%	010	12%
	Pathology	026	10%	010	16%	037	12%	010	12%
	Anesthesia	037	14%	006	10%	036	12%	012	15%
	Dermatology	042	16%	004	06%	036	12%	009	11%
	Obstetrics and gyn	030	12%	013	21%	041	13%	007	09%
	Pediatrics	033	13%	010	16%	039	13%	009	11%
	Psychiatry	030	12%	009	14%	041	13%	010	12%
	Others	033	13%	004	06%	039	13%	014	17%

From Table 8 above, both MUST and KIU dataset shows similar trends in percentage distribution within the category divides. Which could suggest a consistency in representation of the membership

in the study sample (Casteel & Bridier, 2021). Notably, the leading categories within student sample include; gender (MUST male: 58%; KIU male: 56%); age-group: 18 to 26 years (MUST: 75%; KIU: 64%); nationality: Ugandan (MUST: 90%; KIU: 88%); year of study: year 3 (MUST: 49%; KIU: 49%); denomination: catholic (MUST: 52%; KIU: 32%); medical department: (MUST: 16%; KIU: 12%). However, the disparity in percentage between MUST and KIU seem less significant, except for denomination where the difference is 10%.

4.4.2 SM usage characteristics.

As stated in Section 1.6.3, the scope of this study was limited to a formal organization setting where SM usage is dominant in Uganda. According to Mirembe, Lubega & Kibukamusoke (2019), SM usage is more dominant in higher educational institutions compared to other formal organizational settings in Uganda. Meanwhile, according to Olum & Bongomin (2020), over 90% of medical students in Uganda are using SM in their operations. Thus, the most dominant SM platforms in medical institutions in Uganda include; WhatsApp, Facebook, Twitter, and YouTube (Olum & Bongomin 2020; Mirembe et al., 2019). Therefore, the selected medical institutions, and SM platforms used in this study fit within the geographical and content scope definition of the study. Table 9 below summarizes and presents SM usage characteristics, with respect to the selected medical institutions (MUST and KIU), indicating the frequency counts, and percentage distributions within the category divides accordingly.

Table 9: SM usage characteristics, with respect to medical institutions

	MEDICAL INSTITUTIONS	MUST				KIU			
	SM usage characteristics	Medical students		Medical staff		Medical students		Medical staff	
1	SM Platform used	*n = 260*	*(100%)*	*n = 64*	*(100%)*	*n = 306*	*(100%)*	*n = 80*	*(100%)*
	WhatsApp	252	97%	052	82%	300	98%	070	88%
	Facebook	203	78%	038	60%	233	76%	051	64%
	Twitter	161	62%	042	67%	202	66%	056	70%
	YouTube	135	52%	040	64%	187	61%	043	54%
	Others	122	47%	021	34%	132	43%	025	32%
2	Experience of SM usage								
	Less than a year	004	02%	002	03%	005	02%	004	05%
	1 – 2 years	004	02%	001	02%	011	04%	003	04%
	3 – 4 years	045	17%	007	11%	057	19%	017	21%
	5 – 6 years	076	29%	019	30%	090	29%	023	28%
	More than 6 years	131	50%	034	54%	143	47%	034	42%
3	Frequency of SM usage								

	Never use SM	001	00%	001	02%	001	00%	002	03%
	Rarely	034	13%	007	11%	037	12%	013	16%
	Sometimes	031	12%	011	18%	043	14%	012	15%
	Often	122	47%	028	44%	137	45%	038	47%
	Always	072	28%	016	25%	088	29%	016	20%
4	Contacts/friends connected								
	Less than 50	008	03%	002	03%	004	01%	001	01%
	51 – 100	031	12%	009	14%	031	10%	009	11%
	101 – 150	041	16%	009	14%	022	07%	019	24%
	151 – 200	052	20%	007	11%	033	11%	022	27%
	More than 200	128	49%	036	57%	216	71%	030	37%
5	Share medical information on SM								
	Yes	227	87%	051	81%	260	85%	065	80%
	No	033	13%	012	19%	046	15%	016	20%
6	Encounter medical information breaches								
	Yes	103	40%	017	27%	130	42%	029	36%
	No	157	60%	046	73%	176	58%	052	64%
7	Frequency in medical information breaches								
	Never	079	30%	025	40%	092	30%	032	40%
	Rarely	035	14%	008	13%	038	12%	009	12%
	Sometimes	028	11%	009	14%	044	14%	013	16%
	Often	082	32%	006	10%	083	27%	023	28%
	Always	036	14%	015	24%	049	16%	004	05%

Notably, the leading types of SM platforms reported among respondents include WhatsApp (MUST: 97%; KIU: 98%); and Facebook (MUST: 78%; KIU: 76%). Comparatively, the dataset for MUST, KIU, and related studies conducted in Uganda shows similar trends in percentage distributions among SM usage categories (Olum & Bongomin 2020; Mirembe, Lubega & Kibukamusoke, 2019). However, the leading SM usage engagement levels were recorded among students; experience in SM usage: > 5 years (MUST: 79%; KIU: 76%); frequency of SM usage: always and often (MUST: 75%; KIU: 74%); number of contacts/friends connected: > 150 (MUST: 69%; KIU: 82%). Remarkably, SM usage engagement levels among medical students ranges from 72% to 94%, compared to medical staff (55% to 70%). Overall, over 80% of the respondents across category divides acknowledged sharing medical information on SM. The percentage distributions of respondents who share medical data on SM shows similar trend between MUST and KIU. Thus medical students: yes (MUST: 87%; KIU: 85%), medical staff: yes (MUST: 81%; KIU: 80%). Overall, the dataset for MUST and KIU shows similar trends in percentage distributions among SM usage categories. Figure 5 below indicates

the percentage distributions of the types of SM platform used among medical students, with respect to medical institutions, (MUST *n = 260*, KIU *n = 306*).

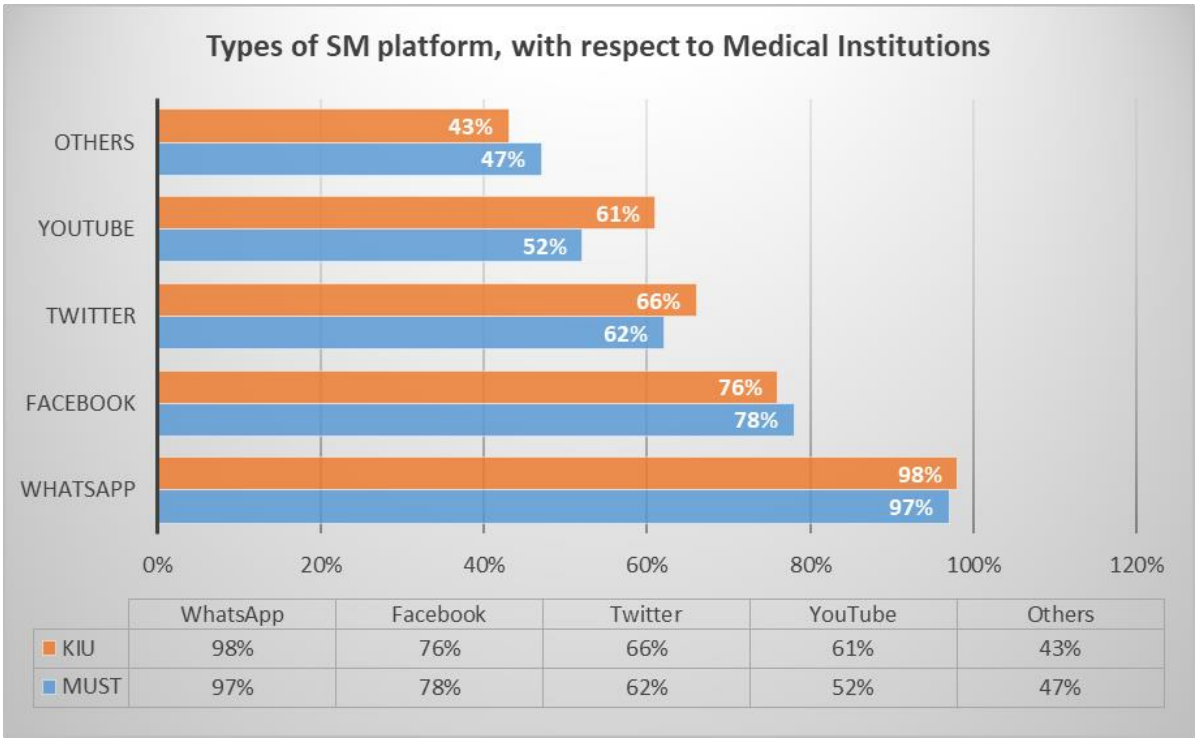


Figure 5: Types of SM platform, with respect to Medical Institutions

According to Figure 5 above, the leading type of SM platforms reported among medical students include WhatsApp (MUST: 97%; KIU: 98%), Facebook (MUST: 78%; KIU: 76%), Twitter (MUST: 62%; KIU: 66%), YouTube (MUST: 52%; KIU: 61%), and others (MUST: 47%; KIU: 43%). Relatively, the chart shows some level of uniformity in percentage distribution between MUST and KIU dataset. Overall, WhatsApp platform and Facebook were reported as the most dominant type of SM platforms among medical students.

4.4.3 Medical information breaches, acknowledgement levels

Remarkably, with respect to medical information breaches (Table 10), 27% to 42% of the respondents within different category divides acknowledged occurrence of medical information breaches, due to SM usage. Relatively, medical students acknowledged higher level of medical information breaches compared to medical staff. Thus, medical student: yes (MUST: 40%; KIU: 42%); compared to medical staff: yes (MUST: 27%; KIU: 36%). Overall, the percentage distributions among MUST, KIU, and related studies in Uganda shows similar trends in the level of medical information breaches reported (Alunyu, et al., 2021; Mirembe, Lubega & Kibukamusoke, 2019; Roy et al., 2016; Pander et al., 2014). Nevertheless, the level of the breaches is slightly higher among KIU respondents,

compared MUST. This could also be attributed to the slight over-edge in the population and sample size representation between the two medical institutions. Figure 6 below indicates the percentage distributions of medical information breaches among respondents, with respect to medical institutions, (MUST *n = 260* students *n = 64* staff, KIU *n = 306* students *n = 80* staff).

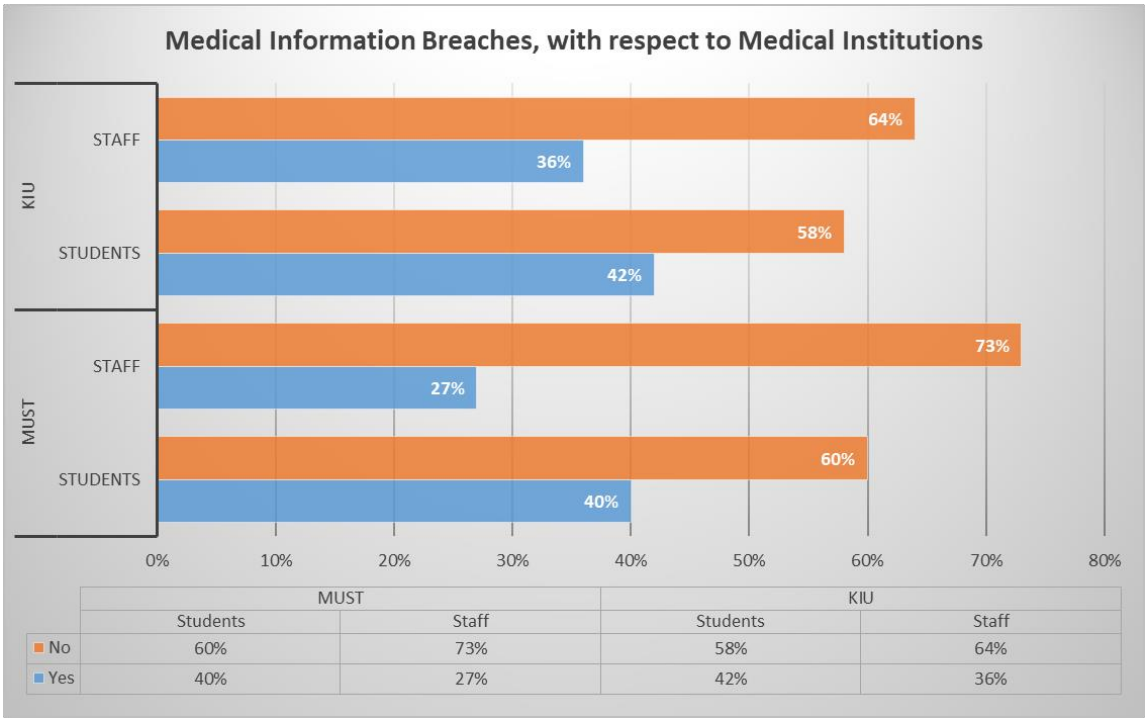


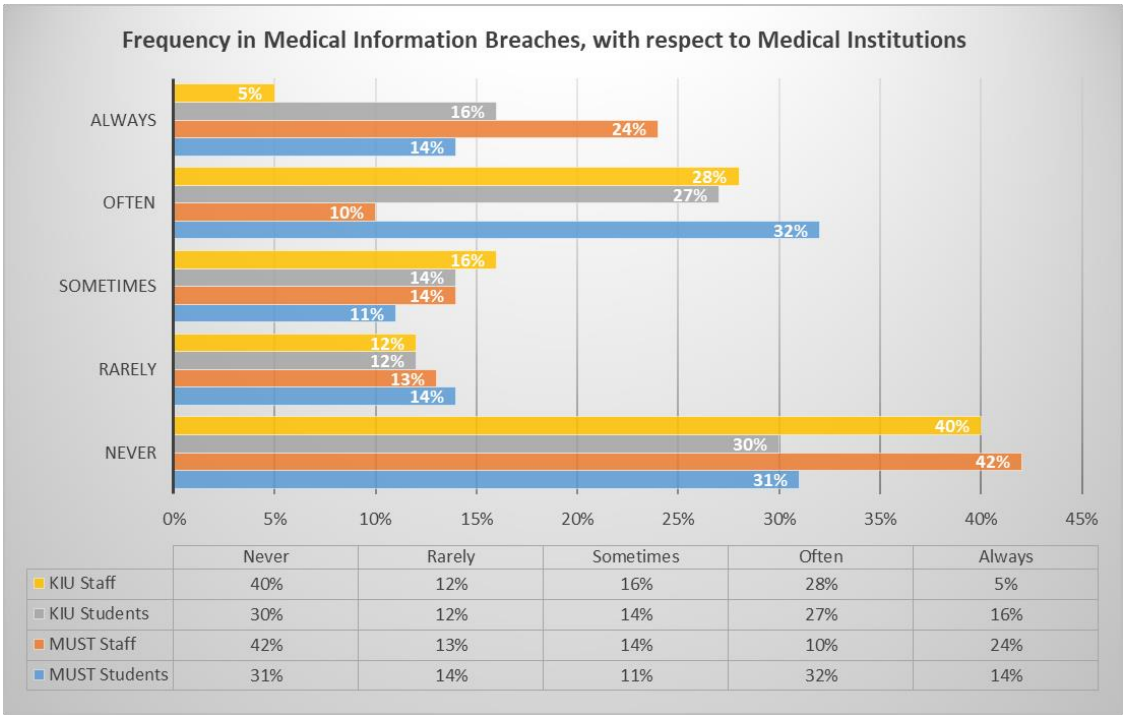
Figure 6: Medical Information Breaches, with respect to Medical Institutions

According to Figure 6 above, the lowest level of percentage distribution in medical information breaches was reported among medical staff of MUST (27%). While, the highest percentage was reported among medical students of KIU (42%). Thus, as indicated in Table 9, 27% to 42% of the respondents within category divides (medical institutions) acknowledged occurrence of medical information breaches, due to SM usage.

4.4.4 Frequency in medical information breaches

On the other hand, frequency in medical information breaches helped to gauge the rate at which medical information breaches occurs. The measures include; "1 = never", "2 = rarely", "3 = sometimes", "4 = often", and "5 = always". However, for easy interpretation of the results, the lowest level of medical information breaches correspond to the highest level of medical information safety. Likewise, the highest level of breaches correspond to the lowest level of medical information safety. In line with specific objective 1, frequency in medical information breaches would help to explain the prevalence in medical information breaches, due to SM usage. Among the different categorical

responses recorded, 33% to 46% of the respondents were recorded within the upper limits of frequency in medical information breaches, (always and often). Relatively, higher levels of frequency in breaches were reported among male student category (43% to 58%), and WhatsApp users (44% to 62%). Figure 7 below indicates the percentage distributions of frequency in medical information breaches among respondents, with respect to medical institutions, (MUST *n = 260* students *n = 64* staff, KIU *n = 306* students *n = 80* staff).



	Never	Rarely	Sometimes	Often	Always
KIU Staff	40%	12%	16%	28%	5%
KIU Students	30%	12%	14%	27%	16%
MUST Staff	42%	13%	14%	10%	24%
MUST Students	31%	14%	11%	32%	14%

Figure 7: Frequency in Medical Information Breaches, with respect to Medical Institutions

According to Figure 6 above, the level of frequency in medical information breaches can be interpreted by focusing on the response options; “always” and “often” percentage bar. In this case adding the percentage figures for always + often, the response recorded under medical staff would then be 34% for MUST, and 33% for KIU. Likewise, the response recorded under medical students would be 46% for MUST, and 43% for KIU. Notably, the lowest level of frequency in medical information breaches would then be 33% for KIU staff, and the highest would be 46% for MUST students. Thus, among the different categorical responses recorded, 33% to 46% of the respondents reported some level of frequency in medical information breaches, due to SM usage.

4.4.5 SM socio-technical information security factors

Presumably, the key SM socio-technical information security factors associated with medical information breaches were mainly adopted from existing literatures, as guided by socio-technical

system theory, the extended DeLone and McLean theory, and usable-security principles (Mujinga, Eloff & Kroeze, 2019; Lombardo, Mordonini, & Tomaiuolo, 2021). In this case, the key factors identified under social dimension include; 1) usability factors – *visibility*, *learnability* and *user satisfaction*; 2) training and education factors – *help* and *documentation*, and *user language* (Yeratziotis et al 2012; Preece et al, 2015; Nielsen, 2010; Ogara, Koh, & Prybutok, 2014; Zahidi, Lim & Woods, 2014; Schneiderman et al., 2016; Price & Shanks, 2005). On the other hand, the key factors identified under technical dimension include; 3) SM technology development factors – *error handling*, and *process revocability*; 4) task performed factors – *security*, *expressiveness*, and *privacy* and *confidentiality* (Mujinga, Eloff & Kroeze 2019; Schnneiderman et al., 2016; Yeratziotis et al., 2012). Table 10 below summarizes and presents the key SM socio-technical information security factors, indicating the responses on the level of agreement on the factors accordingly.

Table 10: SM socio-technical information security factors, level of agreement

Level of agreement	Strongly Disagree (%)		Disagree (%)		Neutral (%)		Agree (%)		Strongly Agree (%)	
Factors (Item percentage averages)	MUST *n = 260*	KIU *n = 306*	MUST *n = 260*	KIU *n = 306*	MUST *n = 260*	KIU *n = 306*	MUST *n = 260*	KIU *n = 306*	MUST *n = 260*	KIU *n = 306*
Visibility (VB)	05%	06%	16%	18%	41%	42%	25%	24%	13%	13%
Learnability (LN)	04%	04%	16%	17%	40%	40%	29%	28%	13%	12%
User satisfaction (US)	07%	08%	16%	17%	41%	40%	26%	25%	11%	10%
Intention to use (ITU SM)	08%	07%	14%	19%	39%	42%	23%	28%	09%	12%
Error handling (EH)	04%	05%	19%	17%	42%	40%	25%	26%	13%	13%
Process revocability (RV)	07%	06%	16%	17%	40%	38%	26%	26%	10%	11%
Expressiveness (EX)	06%	07%	15%	18%	39%	41%	27%	25%	12%	10%
Help and *documentation (HD)*	07%	06%	17%	16%	38%	39%	26%	28%	10%	12%
User language (UL)	06%	07%	16%	17%	40%	37%	25%	29%	09%	13%
Security (SC)	06%	06%	14%	18%	40%	26%	27%	24%	13%	10%
Privacy and *confidentiality (PC)*	06%	07%	16%	18%	39%	39%	27%	25%	12%	11%
Secure SM usage (SM-US)	05%	08%	15%	21%	32%	40%	27%	27%	10%	13%
MIBR	06%	07%	18%	18%	34%	34%	28%	30%	11%	12%

According to Table 10 above, factors with high levels of percentage agreement would imply better compliance in SM socio-technical information security factor. While low level of agreement could imply weakness/vulnerability in SM socio-technical information security factor (Mujinga, Eloff & Kroeze, 2019). In this case, the level of percentage agreement combined ("agree" + "strongly agree") include; *visibility* (MUST: 38%; KIU: 37%), *learnability* (MUST: 41%; KIU: 40%), *user satisfaction* (MUST: 37%; KIU: 35%), *intention to use* (MUST: 32%; KIU: 40%), *errors handling* (MUST: 38%; KIU: 39%), *process revocability* (MUST: 36%; KIU: 37%), *expressiveness* (MUST: 39%; KIU: 35%), *help* and *documentation* (MUST: 36%; KIU: 40%), *user language* (MUST: 34%; KIU: 42%) *security* (MUST: 40%; KIU: 34%), *privacy* and *confidentiality* (MUST: 39%; KIU: 36%), *secure SM*

usage (MUST: 37%; KIU: 40%), and *MIBR* (MUST: 39%; KIU: 42%). Relatively, *learnability* and *security* factors shows slight over-edge in the level of percentage agreement, which could imply better compliance in SM socio-technical information security factor, compared to the other factors. On the other hand, agreement level of medical information breaches include; (MUST: 39%; KIU: 42%), which could also serve as a complementary measure to the level of frequency in medical information breaches dataset (Table 9). Figure 8 below indicates the percentage distribution levels of agreement in medical information breaches among medical students, with respect to medical institutions, (MUST *n = 260*; KIU *n = 306*).

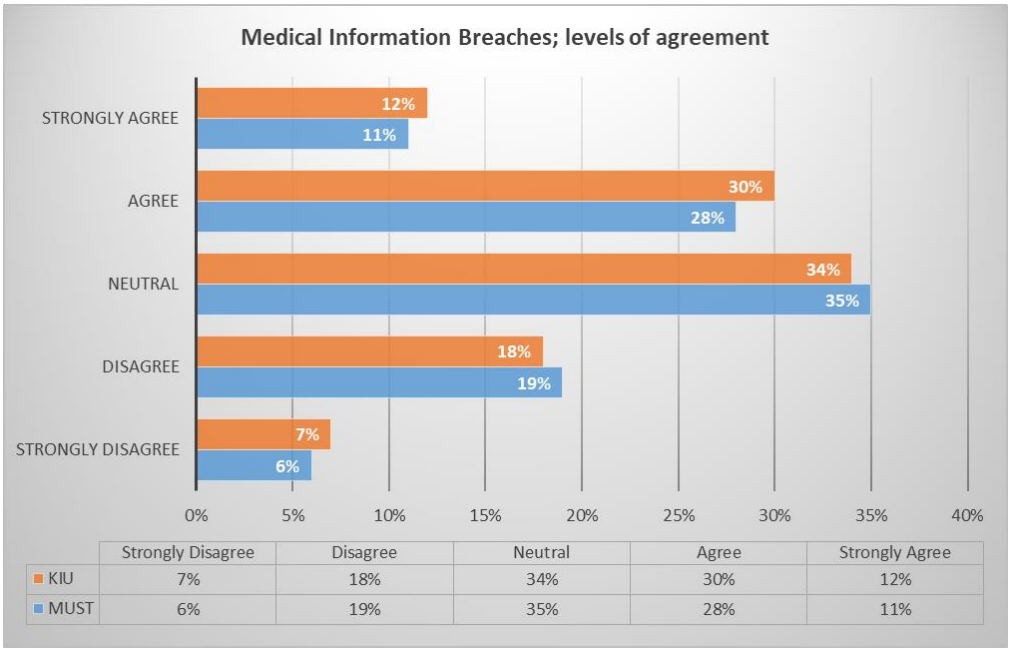


Figure 8: Medical Information Breaches; levels of agreement

Notably, occurrence of medical information breaches reported within respondent categories ranges from 27% to 42% (Figure 5), while frequency in medical information breaches ranges from 33% to 46% (Figure 6), and level of agreement in medical information breaches ranges from 39% to 42% (Figure 7). Overall, the percentage values complement each other by revealing the trend of consistency in respondents' opinions. However, the dataset used in correlational relationship was the level of SM usage and agreement in medical information breaches. In the final analysis, the lowest level of medical information breaches correspond to the highest level of medical information safety. Likewise, the highest level of medical information breaches correspond to the lowest level of medical information safety, respectively. Notably, the prevalence rate of medical information breaches due to SM usage ranges from 27% to 42% in line with acknowledgment levels (yes, no). However, with respect to frequency in medical information breaches, the prevalence rate is 33% to 46%, and with

respect to level of agreement in medical information breaches, the prevalence is 39% to 42%, respectively. In any case, the percentage ranges are similar and complementary to each other, and could be used to explain the prevalence rate of medical information breaches.

4.5 Interview Results

On the other hand, qualitative data was collected using semi-structured interview, and analyzed using thematic content analysis method. The respondents consisted of 14 Heads of Departments (HODs) and 2 Deans, all selected from MUST and KIU accordingly. The department involved included Internal Medicine, Pathology, Anesthesia, Dermatology, Obstetrics and Gynecology, Pediatrics and Psychiatry. Table 11 below summaries and presents the response generated.

Table 11: Interview Results

	AREA	INTERVIEW GUIDE FOR INSTITUTION/FACULTY HEADS	MUST (*n = 8*)		KIU *(n = 8*)		
		Questions	Yes	No	Yes	No	Comments
1	Social Media usage	Do you allow Social Media usage in your institution/department? If yes, Why?	8 100%	0 0%	8 100%	0 0%	Effective communication and collaboration tool
		Have you ever considered formalizing Social Media usage in your institution/department? If yes or no, why?	3 38%	5 62%	2 33%	6 67%	Yes, good communication tool No, its new phenomena No, not thought of it No. difficult system to manage
		What do you consider to be some of the benefits and risks of formally adopting Social Media usage in your operations?	NA	NA	NA	NA	Effective communication and collaboration Difficult to control privacy on SM
		What do you think could be some of the solutions to Social Media risks in your area of operations? Manage the risks or avoid Social Media?	NA	NA	NA	NA	Manage the risk
		Have you had any Social Media training as an institution/department?	0 0%	8 100%	0 0%	8 100%	NA
		Do you have any documents or procedures regulating Social Media usage in teaching/learning, or research?	0 0%	8 100%	0 0%	8 100%	NA
		Do you normally use Social Media in communicating and sharing of medical information to staff and student?	6 67%	2 33%	7 86%	1 14%	NA
2	Medical privacy and confidentiality	Do your staff and students understand the legal or ethical requirements governing medical privacy and confidentiality in your institution/department?	8 100%	0 0%	8 100%	0 0%	NA
		Have you ever been a victim of breaches related medical privacy and confidentiality on Social Media? If yes, what do you attribute the breaches to?	5 62%	3 38%	4 50%	4 50%	Technical error Lack of knowledge in SM usage
		How many breaches have you witnessed in medical privacy and confidentiality, due to Social Media usage in the last one year in your institution?	NA	NA	NA	NA	Few instances Twice a month Weekly
		How do you often safeguard medical privacy and confidentiality on Social Media?	NA	NA	NA	NA	I don't know Setting security functions
		Do you believe Social Media usage is important in medical education, irrespective of the associated risks?	NA	NA	NA	NA	Very important

From Table 11 above, the key response obtained indicates that SM usage is considered important in medical education. 100% of the respondents from both MUST and KIU confirmed the need for SM usage in their departments, while acknowledging that SM is an effective tool for communication and collaboration. On the issue of formalizing SM usage, 38% (MUST) and 33% (KIU) believe in the need for formalizing SM usage in medical education. On the question of benefits and risks of associated with SM usage, respondents attributed SM benefits to effectiveness in communication and collaboration, while the risks are attributed to the needs for privacy and confidentiality in medical information. 62% (MUST) and 50% (KIU) acknowledged instances of medical information breaches. 100% of the respondents confirmed lack of training and proper guidelines in SM usage. Nevertheless, the respondents still prefer to manage the risks than avoid SM usage.

4.6 Inferential Statistics

Subsequently, the key steps that guided inferential statistical data analysis include research objectives, research questions, and the data types. However, before performing detailed analysis process, reliability test, and test of normality were performed on the datasets as perquisites to determine the appropriate choice for inferential statistical methods. Earlier on, pre/pilot test (validity and reliability tests) were performed to validate the questionnaire instruments, but using 10 experts and 32 respondents accordingly (Section 3.3.2). Nevertheless, the reliability test conducted in this section used 710 respondents, but with the same purpose of checking and confirming the extent to which the measures of the construct is reliable and dependable, (Taherdoost, 2016).

4.6.1 Reliability test

Thus, using SPSS software, 51 items from 710 questionnaires were subjected to reliability test to check the internal consistency within the items. Earlier on, each item was developed with a 5-point Likert scale, with responses ranging from "1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree" (Zamanzadeh, et al., 2015; Joshi et al., 2015). Subsequently, Cronbach's alpha (α) values were then generated to reveal the consistency in response within the datasets. Items with Cronbach's Alpha values ($\alpha \geq 0.70$) were considered strong reliability items, while those with Cronbach's alpha values between 0.50 to 0.70 were considered moderate reliability items, and those with Cronbach's alpha values ($\alpha < 0.50$) were considered weak reliability items (Mutebi, et al., 2022; Tamarah & Samantha, 2018; Zamanzadeh, et al., 2015; Joshi et al., 2015). Table 12 below presents the summary of reliability test results for the items under each factor, indicating the Cronbach's alpha (α) values for each factor, and the conclusion thereof.

Table 12: Reliability test results

FACTORS	No of Items	No of Strong Reliability Items	No of Moderate Reliability Items	Cronbach's alpha α – values	Conclusion
Visibility (VB)	5	5	0 revised	0.922	Reliable
Learnability (LN)	5	5	0 revised	0.849	Reliable
User satisfaction (US)	4	3	1 revised	0.832	Reliable
Intention to use (ITU)	4	3	1 revised	0.872	Reliable
Error handling (EH)	5	2	3 revised	0.711	Reliable
Revocability (RV)	5	2	3 revised	0.701	Reliable
Expressiveness (EX)	5	3	2 revised	0.722	Reliable
Help and *documentation (HD)*	5	5	0 revised	0.802	Reliable
User language (UL)	5	5	0 revised	0.802	Reliable
Security (SC)	5	5	0 revised	0.899	Reliable
Privacy and *confidentiality (PC)*	7	5	2 revised	0.820	Reliable
Secure SM usage (SM US)	5	4	1 revised	0.778	Reliable
MIBR	4	3	1 revised	0.821	Reliable
VB (Visibility), LN (Learnability), US (User satisfaction), ITU (Intention to use), EH (Error handling), RV (Process revocability), EX (Expressiveness), HD (Help and documentations), UL (User language), SC (Security), PR (Privacy and confidentiality), SM US (Secure SM usage), MIBR (Medical information breaches).					

From Table 12 above, weak reliability items were dropped, while moderate reliability items were revised and maintained together with strong reliability items. Altogether, the factors with reliable items were considered and maintained in next stages of the analysis process. The factors include; *visibility (VB), learnability (LN), user satisfaction (SU), intention to use (ITU), errors handling (EH), process revocability (RV), expressiveness (EX), help* and *documentations (HD), user language (UL), security (SC), privacy* and *confidentiality (PR), Secure SM usage (SM-US),* and *medical information breaches (MIBR)*. While factors with generally very weak reliability items, which were excluded include *user suitability*. However, the reliable factors were further subjected to test of normality, to determine the appropriate regression analysis options.

4.6.2 Test of normality

Before performing a regression analysis, test of normality was performed to check the normality distribution of the datasets. According to Joshi et al. (2015), if the dataset are normally distributed, then appropriate regression analysis option could be parametric test; which could be Linier Regression analysis, and Pearson's Correlation. Otherwise, the alternative analysis option would be non-parametric test; Ordinal Regression analysis, and Spearman's Rank correlation. Therefore using SPSS software, the datasets were subjected to test of normality. Subsequently, test of normality results (z-scores, Kolmogorov Smirnov results, Histograms, and normal Q-Q plots) were generated, and verified based on the following key assumptions (Keya & Rahmatullah, 2016):

Assumption 1: z-scores values for both skewness and kurtosis were expected to span within the range of *-1.96 to +1.96*.

Assumption 2: Kolmogorov Smirnov *p-values* were expected to be greater than 0.05, for all the tested factors.

Assumption 3: Histograms, and normal Q-Q plots should visually display symmetric shapes, for all the factors. Scatter plot should display monotonic shape, (Appendix G).

Table 13 below summarizes and presents test of normality results, indicating the z-scores, and Kolmogorov Smirnov results accordingly.

Table 13: Test of normality results

FACTORS	Skewness z-scores values	Kurtosis z-scores values	Kolmogorov Smirnov Statistics	P > 0.05
Visibility (VB)	1.500	-2.295	0.108	0.000
Learnability (LN)	3.076	-1.950	0.107	0.000
User satisfaction (US)	-1.435	-1.847	0.098	0.002
Intention to use (IU)	3.122	1.998	0.217	0.020
Error handling (EH)	2.793	1.118	0.117	0.001
Revocability (RV)	-5.500	1.244	0.016	0.021
Expressiveness (EX)	1.226	-1.092	0.033	0.008
Help and documentation (HD)	-0.045	-1.432	0.074	0.012
User language (UL)	-1.436	-1.837	0.088	0.003
Security (SC)	0.457	-1.366	0.092	0.001
Privacy and confidentiality (PC)	4.891	0.148	0.081	0.011
Secure SM usage (SM-US)	-3.310	-2.742	0.224	0.000
MIBR	-2.120	-2.612	0.114	0.000
Conclusion: Dataset were not normally distributed; possible analysis option: Ordinal Regression analysis, and Spearman's Ranks correlation (Taherdoost, 2016; Joshi et al., 2015)				

According to Table 13 above, the skewness and kurtosis (z-scores) results indicate violation of assumption 1. The factors with z-score values outside the range of -1.96 to +1.96 include; *learnability* (z = 3.076), *error handling* (z = 2.793), *privacy* and *confidentiality* (z = 4.891), *medical information breaches* (z = -2.120), *visibility* (z = -2.295), and *revocability* (z = -5.500). Thus, suggesting that the datasets were not normally distributed. With respect to assumption 2, the Kolmogorov Smirnov values (*p-vales*) are all less than 0.05. Thus, confirming that the datasets are still not normally distributed, since $p < 0.05$ for all the factors. More so, the histograms and normal Q-Q plots (Appendix G) shows non-symmetrical results. Thus, still confirming non-normality of the dataset. Therefore, based on the 3 assumptions, and the test of normality results, the dataset are not normally distributed. In this case, the appropriate regression analysis options would be non-parametric test;

Chi-square test, Spearman's Rank correlation, and Ordinal Regression analysis accordingly (Keya & Rahmatullah, 2016, Zamanzadeh, et al., 2015; Joshi et al., 2015). The following sections stipulates the detailed analysis steps followed, and the corresponding results obtained.

4.7 Associations between Variables

Subsequently, inferential statistical analysis was performed using SPSS version 26. The analysis steps were guided by the assumptions and conclusion made in Section 4.6 above. In this case, the datasets were not normally distributed. Therefore, appropriate statistical analysis options preferred included; Chi-square test, Spearman's Rank correlation, and Ordinal Regression analysis (Zamanzadeh, et al., 2015). In this case, Chi-square test was purposely performed to assess the level of associations between selected demographic datasets and medical information breaches. While, Spearman's Rank correlation estimated the strength and direction of the association between SM socio-technical information security factors and SM usage (Joshi et al., 2015). Subsequently, Ordinal Regression analysis was performed to determine the predictive strength of the relationships between independent variables, and dependent variable accordingly. The detail analysis results and the findings are presented in the following sections.

4.7.1 Chi-square test

Chi-square (x^2) test was performed to examine the type of association existing between selected categorical variables, and medical information breaches reported. The key categorical factors selected include medical institutions, gender and age-group. The test was conducted at the critical alpha value of $\alpha = 0.05$. In this case, for all the 3 categorical variables, null hypothesis (H_0) states that there is statistically no significant association between each of the selected categorical variables, and medical information breaches (MIBR). The selected categorical variables included medical institutions (MUST and KIU), gender (male and female), and age-groups (18 to 25, 26 to 35, 36 to 45, and above 45). Table 14 below summarizes and presents chi-square test results, indicating chi-square values (x^2), degree of freedom (*df*), *p-values* accordingly.

Table 14: Chi-square test results

CATEGORICAL FACTORS	*chi-square (x^2)*	*df*	*p-values ($\alpha \leq 0.05$)*	*Conclusion*
Medical institutions -> MIBR	07.890	04	0.096	Insignificant
MUST and KIU : Gender -> MIBR	17.348	04	0.002	Significant
MUST: Gender -> MIBR	17.822	04	0.001	Significant
KIU: Gender -> MIBR	06.084	04	0.193	Insignificant
MUST and KIU: Age-group - > MIBR	23.738	12	0.022	Significant

MUST: Age-group - > MIBR	17.872	12	0.120	Insignificant
KIU: Age-group - > MIBR	15.631	12	0.209	Insignificant
Significant associations: Gender -> MIBR ($x^2 = 7.890$, $df = 4$, $p = 0.096$), MUST: Gender -> MIBR ($x^2 = 17.822$, $df = 4$, $p = 0.001$), Age-group - > MIBR ($x^2 = 23.738$, $df = 12$, $p = 0.022$). It should be noted that Chi-square test is an association test to check if there is a difference among the demographic category divides, with respect to SM usage and medical information breaches				

According to Table 14 above, Chi-square (x^2) results generated ($x^2 = 7.890$, $df = 4$, $p = 0.096$) show insignificant association between medical institutions (MUST and KIU) and medical information breaches (MIBR). With respect to gender, chi-square (x^2) results generated ($x^2 = 17.348$, $df = 4$, $p = 0.002$) show significant association between gender and MIBR. However, with respect to medical institutions, chi-square (x^2) results generated for MUST: gender ($x^2 = 17.822$, $df = 4$, $p = 0.001$) shows significant association between gender and MIBR, while KIU: gender ($x^2 = 6.084$, $df = 4$, $p = 0.193$) shows insignificant difference between gender and medical information breaches. With respect to age-group, chi-square (x^2) results generated ($x^2 = 23.738$, $df = 12$, $p = 0.022$) shows significant association between age-groups and MIBR. However, with respect to medical institutions, chi-square (x^2) results generated for MUST: age-group ($x^2 = 17.872$, $df = 12$, $p = 0.120$), and KIU: age-group ($x^2 = 15.631$, $df = 12$, $p = 0.209$) both shows insignificant association between age-groups and MIBR. It should be noted that Chi-square test is an association test to check if there is a difference among the selected demographic category divides, with respect to SM usage and medical information breaches. For correlational strength and variable prediction, Spearman's Rank correlations, and Ordinal Regression analysis were performed accordingly.

4.7.2 Spearman's Rank correlation

Spearman's Rank correlational analysis was performed to measure the strength and direction of associations between SM socio-technical information security factors, SM usage and medical information safety. Thus, Spearman's Rank correlation coefficient (*r-value*) indicates the level of strength and direction of association between the variables. The level of the strength ranges within $r = \pm 1.00$, and the *p-values* determines the significance level of the correlation. In this case, $p \leq 0.05$ were considered significant (Appendix G). While for correlational direction, the positive/negative *r-value* indicate the direction of the correlation between the variables. Altogether, Table 15 below presents the key Spearman's Rank correlational results, indicating the factors, correlation coefficient (*r-value*), *p-values*, and conclusion accordingly.

Table 15: Spearman's Rank correlation results

FACTORS	User satisfaction (US)	Intention to use (ITU)	Secure SM usage (SM-US)	MIBR
Visibility (VB)	0.724 *	0.566 *	0.640 *	- 0.580 *
Learnability (LN)	0.540*	0.630*	0.570*	- 0.620*

User satisfaction (US)	NA	0.760*	0.670*	- 0.750*
Intention to use (ITU)	0.680*	NA	0.880*	- 0.780*
Error-handling (EH)	0.560*	0.480	0.450	0.360
Revocability (RV)	0.411	0.213	0.545*	- 0.420
Expressiveness (EX)	0.522*	0.321	0.422	0.440
Help and documentation (HD)	0.740*	0.657*	0.470	- 0.770*
User language (UL)	0.722*	0.823*	0.790*	0.680*
Security (SC)	0.650*	0.560*	0.422	- 0.760*
Privacy and confidentiality (PC)	0.423	0.510*	0.220	- 0.620*
* Correlation is significant at 0.05 level (2-tailed). SM socio-technical information security factors and SM-US/US/ITU are mainly positive, strong and significant. While SM socio-technical information security factors and MIBR are mainly negative, strong and significant. However, *EH, RV* and *EX* had weak correlations and were dropped from the next stage of analysis.				

With respect to specific objective 2, the correlational relationships between SM socio-technical information security factors and SM-US/US/ITU are positive, strong and significant. While the correlation between SM socio-technical information security factors and MIBR are negative, strong, and significant. The negative correlations include; visibility (r = - 0.58, p = 0.000), learnability (r = - 0.62, *p = 0.000*), *user satisfaction* (*r = - 0.75, p = 0.000*), *intention to use* (*r = - 0.78, p = 0.000*), *help* and *documentation* (*r = - 0.77, p = 0.000*), *user language* (*r = - 0.68, p = 0.002*), *security* (*r = -0.76, p < 0.000*), *privacy* and *confidentiality* (*r = - 0.62, p = 0.000*). On the other hand, factors with weaker but significant associations include; *errors handling* (*r = 0.36, p = 0.041*), *process revocability* (*r = - 0.42, p < 0.029*), and *expressiveness* (*r = 0.44, p < 0.002*). Notably, strong correlations could suggest consistency in the responses (Keya & Rahmatullah, 2016). While the negative correlations suggest that the level of medical information breaches decrease with increase in the level of compliance in SM socio-technical information security factors. Subsequently, *error handling*, *process revocability*, and *expressiveness* were weak but maintained in the next stage of the analysis. Nevertheless, regression analysis was conducted to reveal more details about the predictive strength of the considered factors, and the types of relationships existing between the independent and dependent variables accordingly.

4.7.3 Regression analysis and modeling

Subsequently, Ordinal Regression analysis was performed to predict the influence of SM socio-technical information security factors (independent variables), on SM usage (dependent variable). After conducting the preliminary tests (reliability test, Chi-square test, and Spearman's Rank correlation), the relevant factors maintained under social dimension included; 1) usability – *visibility* (VB), and *learnability* (LN); 2) training and education – *help* and *documentation* (HD), and *user language* (UL). While technical dimension include; 3) SM technology development – *error handling*,

and *process revocability* (RV); 4) task performed – *security* (SC), *privacy* and *confidentiality* (PC), and *expressiveness* (EX); 5) IS success model – *intention to use* (ITU), *user satisfaction* (US) and *Secure SM usage* (SM-US). From Ordinal Regression analysis results, the key parameters considered in validating the model include; Model Fitting Information, Goodness-of-fit test, Pseudo R-square Statistics, Parameter estimate values, and Test of Parallel Line. Altogether, the measurement values generated under each parameter helped to explain how well the model fit the dataset. Table 16 below summarizes and presents the key measures generated under each parameter, including parameter estimate (*β-value* and $p \leq 0.05$), R-square (*pseudo* R^2), model fitting information (*p-values*), Goodness-of-Fit test (*p-values*), and test of parallel line (*p-values*) accordingly.

Table 16: Ordinal Regression analysis results

DIMENSIONS/FACTORS	SM-US: Parameter Estimates:		Nagelkerke:	Model fitting information:	Goodness-of-Fit: Pearson	Goodness-of-Fit: Deviance	Test of parallel lines:
SOCIAL DIMENSION	*β-value*	*p ≤ 0.05?*	*pseudo R^2*	*x^2 (p ≤ 0.05?)*	*x^2 (p > 0.05?)*	*x^2 (p > 0.05?)*	*x^2 (p > 0.05?)*
Usability Factors				Note: the above assumptions should not be violated			
H_1: VB -> ITU SM H_2: VB -> US	2.860 2.099	0.000 0.000		0.002	0.458	0.341	0.278
H_3: LN -> ITU SM H_4: LN -> US	1.603 1.771	0.010 0.006					
H_5: UL -> ITU SM H_6: UL -> US	2.123 2.000	0.000 0.000					
Training and Education				0.002	0.458	0.341	0.278
H_7: HD -> ITU SM H_8: HD -> US	3.414 2.790	0.000 0.000	ITU: $R^2 = 0.510$				
TECHNICAL DIMENSION							
Information Security				0.002	0.458	0.341	0.278
H_9: SC -> ITU SM	1.980	0.046					
H_{10}: SC -> US	1.230	0.051					
H_{11}: PC -> ITU SM	1.750	0.053	US: $R^2 = 0.586$				
H_{12}: PC -> US	2.112	0.022					
System Development				0.002	0.458	0.341	0.278
H_{13}: ER -> ITU SM	0.012	0.141					
H_{14}: ER -> US	0.001	0.901					
H_{15}: RV -> ITU SM	0.101	0.587	SM-US: $R^2 = 0.680$				
H_{16}: RV -> US	0.008	0.423					
H_{17}: ITU SM -> secure SM usage	2.981	0.004					
H_{18}: US -> secure SM usage	3.752	0.001					
H_{19}: US -> ITU SM	1.803	0.020					
H_{20}: ITU SM -> US	0.812	0.040					
Conclusion: VB, LN, ST, DN, SC and PR were maintained and used in the model. EX, ER and RV were dropped.							

For the model to fit the dataset appropriately, chi-square (x^2) results under Model Fitting Information should be statistically significant ($p \leq 0.05$) (Smith & McKenna, 2013). In this case, *p-values* is less than 0.05, which suggests that the models fit the dataset well. Furthermore, for our model to be a

good fit to the dataset, chi-square results for both Pearson and Deviance under Goodness-of-Fit test should be statistically non-significant ($p > 0.05$). In this case, *p-values* for both Pearson and Deviance is greater than 0.05, suggesting a good model fitting information to the dataset (Zamanzadeh, et al., 2015; Joshi et al., 2015). On the other hand, Pseudo *R-square* (R^2) statistics is the estimation used to determine how well the variables of the model predicts the dependent variable. In this case, the higher the Pseudo *R-square* values, the better the predictions. Specifically, the researcher used Nagelkerke Pseudo *R-square* option, which compares a model with wider prediction values ranging from 0 to 1, instead of Cox & Snell's options which consider values ranges from 0 to less than 1 (Smith & McKenna, 2013). Therefore, basing on Nagelkerke Pseudo *R-square* value, $R^2 = 0.68$, suggest that 68% changes in dependent variable (SM-US) are attributed to the changes in the predictor variables - SM socio-technical information security factors (independent variables). Altogether, the results suggests that the validated SM socio-technical information security factors are good predictors of a Secure SM usage (SM-US) (Mutebi et al., 2022; Zamanzadeh, et al., 2015).

Another important assumption made before interpreting the parameter estimates for the factors was tests of proportional odds assumption, under Test of Parallel Line. The null hypothesis for tests of proportional odds assumption states that the gradient coefficients of the model are uniform throughout the response categories. Therefore, to reject null hypothesis, we would conclude that ordered logit coefficients are not the same across the levels of the outcome. Otherwise, we would conclude that the assumption holds, based on the significance chi-square values x^2 ($p > 0.05$) (Zamanzadeh, et al., 2015). In this case, the proportional odds assumption appears to be holding since the significance chi-square values x^2 ($p = 0.534$). Therefore, based on the assumptions, the researcher went ahead and interpreted Parameter estimate values as stipulated below.

Basing on the parameter estimate values in Table 15, for every unit increase in the predictor (independent variable), the dependent variable was expected to change by its corresponding regression coefficient (β) in the ordered log-odds scale, while the other variables in the model are kept constant. The coefficient explains the size of the influence of that predictor. Whereby, a low coefficient indicates that the variable has minimal influence on the response. The positive/negative (±) sign of the coefficient value indicates the direction of the relationships. The following sub sections outline the predictive strength and the type of the relationship between SM socio-technical information security factors (independent variables), and Secure SM usage (SM-US) (dependent variable) accordingly (Zamanzadeh, et al., 2015; Joshi et al., 2015).

1) *Visibility* is a significant ($p < 0.05$) and positive predictor of *intention to use SM* (ITU SM), and *user satisfaction* (US). In this case, for every one unit increase in *visibility* factor, there is a predicted increase of $\beta = 2.860$ in the log odds of being at a higher level on *intention to use,* and $\beta = 2.099$ in the log odds of being at a higher level on *user satisfaction,* (H_1 and H_2) respectively (Mutebi, et al., 2022; Joshi et al., 2015).

2) *Learnability* is a significant ($p < 0.05$) and positive predictor of *intention to use SM* (ITU SM), and *user satisfaction* (US). In this case, for every one unit increase in *learnability* factor, there is a predicted increase of $\beta = 1.603$ in the log odds of being at a higher level on *intention to use,* and $\beta = 1.771$ in the log odds of being at a higher level on *user satisfaction,* (H_3 and H_4) respectively (Mutebi, et al., 2022; Joshi et al., 2015).

3) *User language* is a significant ($p < 0.05$) and positive predictor of *intention to use SM* (ITU SM), and *user satisfaction* (US). In this case, for every one unit increase in *user language* factor, there is a predicted increase of $\beta = 2.123$ in the log odds of being at a higher level on *intention to use,* and $\beta = 2.000$ in the log odds of being at a higher level on *user satisfaction,* (H_5 and H_6) respectively (Mutebi, et al., 2022; Joshi et al., 2015).

4) *Help* and *documentations* is a significant ($p < 0.05$) and positive predictor of *intention to use SM* (ITU SM), and *user satisfaction* (US). In this case, for every one unit increase in *help and documentations* factor, there is a predicted increase of $\beta = 3.414$ in the log odds of being at a higher level on *intention to use,* and $\beta = 2.790$ in the log odds of being at a higher level on *user satisfaction,* (H_7 and H_8) respectively (Mutebi, et al., 2022; Joshi et al., 2015).

5) *Security* is a significant ($p < 0.05$) and positive predictor of *intention to use SM* (ITU SM), and *user satisfaction* (US). In this case, for every one unit increase in *security* factor, there is a predicted increase of $\beta = 1.980$ in the log odds of being at a higher level on *intention to use,* and $\beta = 1.230$ in the log odds of being at a higher level on *user satisfaction,* (H_9 and H_{10}) respectively (Mutebi, et al., 2022; Joshi et al., 2015).

6) *Privacy* and *confidentiality* is a significant ($p < 0.05$) and positive predictor of *intention to use SM* (ITU SM), and *user satisfaction* (US). In this case, for every one unit increase in *privacy and confidentiality* factor, there is a predicted increase of $\beta = 1.750$ in the log odds of being at a higher level on *intention to use,* and $\beta = 2.112$ in the log odds of being at a higher level on *user satisfaction,* (H_{11} and H_{12}) respectively (Mutebi, et al., 2022; Joshi et al., 2015).

7) *Error handling* is an insignificant ($p < 0.05$) and positive predictor of *intention to use SM* (ITU SM), and *user satisfaction* (US). In this case, for every one unit increase in *error handling* factor, there is a predicted increase of $\beta = 0.012$ in the log odds of being at a higher level on *intention to use,* and $\beta = 0.001$ in the log odds of being at a higher level on *user satisfaction*, (H_{13} and H_{14}) respectively (Mutebi, et al., 2022; Joshi et al., 2015).

8) *Process revocability* is an insignificant ($p < 0.05$) and positive predictor of *intention to use SM* (ITU SM), and *user satisfaction* (US). In this case, for every one unit increase in *revocability* factor, there is a predicted increase of $\beta = 0.101$ in the log odds of being at a higher level on *intention to use*, and $\beta = 0.008$ in the log odds of being at a higher level on *user satisfaction*, (H_{15} and H_{16}) respectively (Mutebi, et al., 2022; Joshi et al., 2015).

9) *Intention to use* is a significant ($p < 0.05$) and positive predictor of *Secure SM usage* (SM-US). In this case, for every one unit increase in *intention to use* factor, there is a predicted increase of $\beta = 2.981$ in the log odds of being at a higher level on *Secure SM usage* (SM-US), (H_{17}) (Mutebi, et al., 2022; Joshi et al., 2015).

10) *User satisfaction* is a significant ($p < 0.05$) and positive predictor of *Secure SM usage* (SM-US). In this case, for every one unit increase in *user satisfaction* factor, there is a predicted increase of $\beta = 3.752$ in the log odds of being at a higher level on *Secure SM usage* (SM-US), (H_{18}) (Mutebi, et al., 2022; Joshi et al., 2015).

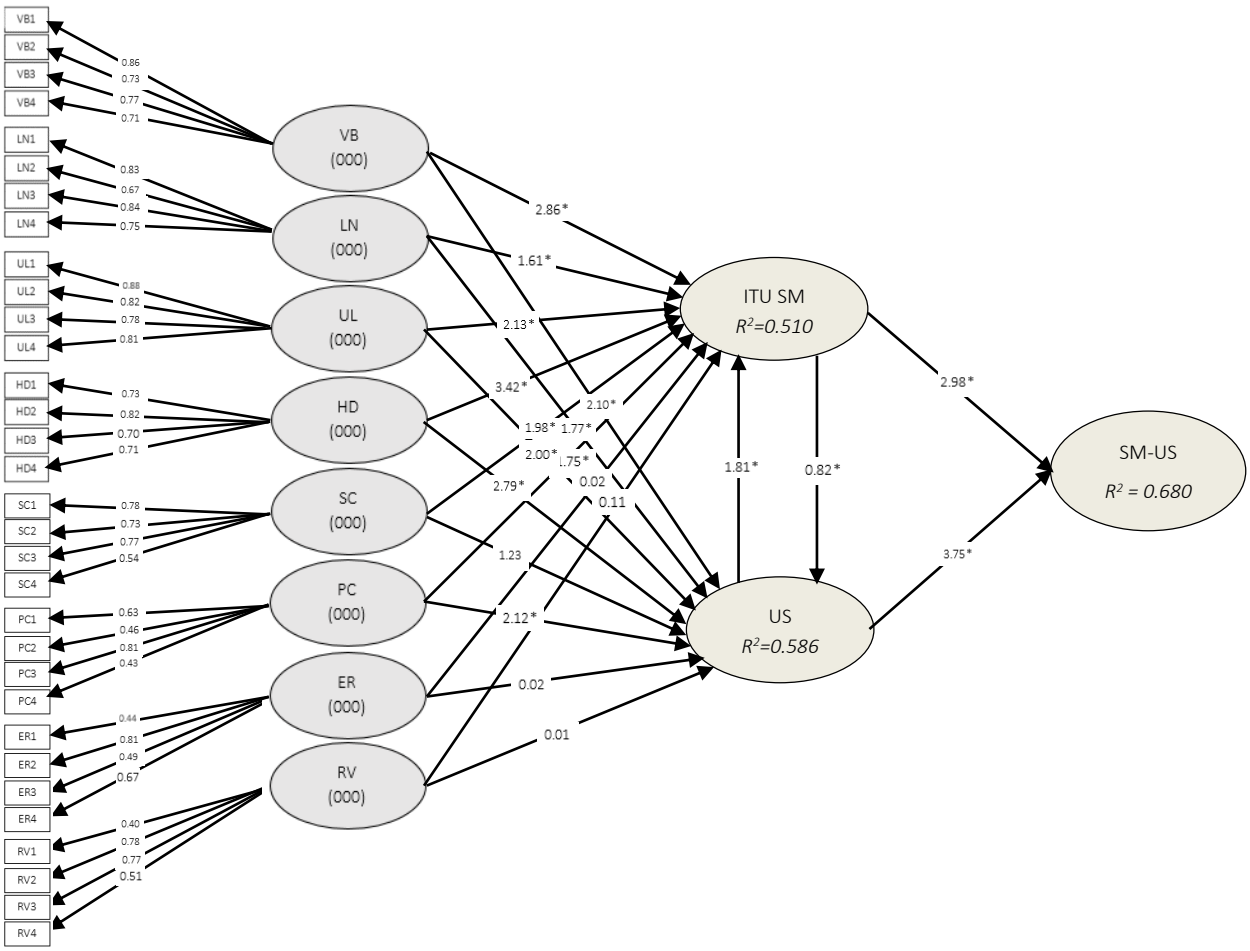
11) *User satisfaction* is a significant ($p < 0.05$) and positive predictor of *intention to use* (ITU SM). In this case, for every one unit increase in *user satisfaction* factor, there is a predicted increase of $\beta = 1.803$ in the log odds of being at a higher level on *Secure SM usage* (SM-US), (H_{19}) (Mutebi, et al., 2022; Joshi et al., 2015)

12) *Intention to use* is a significant ($p < 0.05$) and positive predictor of *User satisfaction (*US). In this case, for every one unit increase in *intention to use* factor, there is a predicted increase of $\beta = 0.812$ in the log odds of being at a higher level on *User satisfaction* (US), (H_{20}) (Mutebi, et al., 2022; Joshi et al., 2015)

Subsequently, the structural equation model was constructed based on the measurement model generated in Table 16 above. Altogether, the key SM socio-technical information security factors considered in the model include; 1) usability – *visibility* (VB), and *learnability* (LN); 2) training and education – *help* and *documentation* (HD), and *user language* (UL). While factors considered and used under technical dimension include; 3) task performed – *security* (SC), *privacy* and

confidentiality (PC). On the other hand, the key factor considered under IS success model include; 4) *intention to use SM* (ITU SM), *user satisfaction* (US), and *Secure SM usage* (SM-US). However, factors under system development with low *β-values* include *error handling*, and *process revocability*. Altogether, the key SM socio-technical information security factors considered in structural equation model include *visibility* (VB), *learnability* (LN), *user language* (UL), *help* and *documentations (*HD), *Security* (SC), *Privacy* and *Confidentiality* (PC), *error handling* (ER), *process revocability* (RV), *intention to use SM* (ITU SM), *user satisfaction* (US), and *secure SM usage* (SM-US). Figure 9 below presents the structure equation model based on the measurement values generated and interpreted in Table 16 above.

Structural Model (SM socio-technical information security factors -> Secure SM usage (SM-US))



Visibility (VB), learnability (LN), user language (UL), help and documentation (HD), security (SC), privacy and confidentiality (PC), intention to use SM (ITU-SM), user satisfaction (US), and Secure SM usage (SM-US). The other factors dropped include; error handling (ER), revocability (RV), and expressiveness (EX)

Figure 9: Structural Equation Model (SM socio-technical information security factors -> SM usage)

According to Figure 9 above, the relationships between the latent variables, and the corresponding variables are presented, and the standard coefficients are indicated in the model. Notably, all the

parameter estimates generated were significant ($p < 0.05$), except factors under system development with low *β-values*, which include *error handling*, and *process revocability*. Generally, the model shows good fitting information to the dataset, where SM-US is significantly associated with SM socio-technical information security factors, with the following path coefficient; VB -> ITU SM (*β = 2.860, p = 0.000*); VB -> US (*β = 2.099, p = 0.000*); LN -> ITU SM (*β = 1.603, p = 0.010*); LN -> US (*β = 1.771, p = 0.006*); UL -> ITU SM (*β = 2.123, p = 0.000*); UL -> US (*β = 2.000, p = 0.000*); HD -> ITU SM (*β = 3.414, p = 0.000*); HD -> US (*β = 2.790, p = 0.000*); SC -> ITU SM (*β = 1.980, p = 0.046*); SC -> US (*β = 1.230, p = 0.051*); PC -> ITU SM (*β = 1.750, p = 0.053*); PC -> US (*β = 2.112, p = 0.022*); ITU SM -> SM-US (*β = 2.981, p = 0.004*); US -> SM-US (*β = 3.752, p = 0.001*); and US -> ITU SM (*β = 1.803, p = 0.020*) respectively.

4.8 Model Validation

Notably, the key factors have demonstrated good and significant levels of parameter estimate useful for predicting US, ITU-SM, and SM-US accordingly. Pseudo $R^2 = 0.510$ for ITU-SM, and *0.586* for US imply predictive strength of 51% for ITU-SM, and 59% for US respectively. Relatively, *visibility*, *user language, help* and *documentation,* and *privacy* and *confidentiality* have better predictive strength compared to *learnability* and *security* factors. However, factors under system development with low *β-values* include *error handling,* and *process revocability*. Relatively, the social dimensional factors demonstrated better predictive estimates to US, ITU-SM, and SM-US compared to technical dimension. *User satisfaction* (US) demonstrated a better predictive estimates to *Secure SM usage* (SM-US) compared to *Intention to use SM* (ITU-SM). Overall, the pseudo $R^2 = 0.68$, suggests that 68% of the changes in dependent variable (SM-US) was as a result of the changes in independent variable (SM socio-technical information security factors). Afterwards, the model was validated for multicollinearity using SmartPLS graph, and expert evaluation. Whereby, discriminate validity of the sample model's construct were validated. This was done to measure the Average Variance Extracted (AVE) between the constructs, and their respective indicators. Table 17 below shows the Composite Reliability (CR) and Average Variance Extracted (AVE) values.

Table 17: Model validation

FACTORS	CR	AVE	MSV	ASV	VB	LN	HD	UL	SC	PC	US	ITU	SM-US
VB	**0.836**	**0.527**	0.177	0.121	1.000								
LN	**0.921**	**0.693**	0.350	0.233	0.342	1.000							
HD	**0.845**	**0.772**	0.432	0.345	0.333	0.564	1.000						
UL	**0.734**	**0.678**	0.458	0.343	0.512	0.677	0.455	1.000					

SC	**0.918**	**0.683**	0.298	0.188	0.322	0.511	0.232	0.342	1.000				
PC	**0.920**	**0.594**	0.297	0.178	0.456	0.244	0.567	0.565	0.234	1.000			
US	**0.943**	**0.737**	0.179	0.099	0.434	0.398	0.112	0.787	0.455	0.563	1.000		
ITU	**0.879**	**0.692**	0.523	0.189	0.167	0.457	0.234	0.600	0.244	0.445	0.467	1.000	
SM-US	**0.859**	**0.584**	0.540	0.233	0.388	0.565	0.213	0.323	0.347	0.245	0.238	0.578	1.000
Visibility (VB), learnability (LN), user language (UL), help and documentation (HD), security (SC), privacy and confidentiality (PC), intention to use SM (ITU SM), user satisfaction (US), and Secure SM usage (SM-US), Average Variance Extracted (AVE) and Composite Reliability (CR)No validity concern indicated. CR (≥ 0.7) and AVE (≥ 0.5)													

Notably, from Table 17 above, both the Average Variance Extracted (AVE) and Composite Reliability (CR) are necessary assumptions to validate constructs (Henseler, Ringle & Sarstedt, 2015). The general assumption requirement for validity in this case are; CR (≥ 0.70) and AVE (≥ 0.50) (Sarstedt, Ringle, & Hair, 2021). Therefore, according to Table 17, CR and AVE estimates values did not violate the assumption requirements. Hence, all the constructs of the model have achieved the minimum threshold values. Notably, multicollinearity test was performed to test the correlation between independent variables. In this case, the correlation coefficient values ranges from 0 to 0.600, which is quite below the maximum value of 1.000. With Comparative Fit Index (CFI > 95) (Zamanzadeh, et al., 2015; Joshi et al., 2015).

On the other hand, the experts were used to validate the model. The experts include information security lecturers, ICT professionals from Mbarara University of Science and Technology (MUST), Busitema University, and Kampala International University (KIU), all in Uganda. The main attributes that guided the selection of the experts were qualifications (MSc, and PhDs), area of specialty, and year of experience in academics, and research. Altogether, 10 experts were identified, and individually given evaluation forms with clear instruction to independently complete the form. More so, they were verbally briefed, and guided on the study purpose, and how to complete the form, and they all consented. Table 18 below present the demographic profiles of the experts.

Table 18: Experts demographic profiles

Experts ID	Institution	Gender	Age	Qualification	Specialization	Experience
Exp1	KIU	Male	36 – 40	MSc	Computer Engineering	11 – 15 years
Exp2	KIU	Male	41 – 45	PhD	Computer Science	11 – 15 years
Exp3	KIU	Male	Above 45	PhD	Information Systems	Above 15 years
Exp4	MUST	Male	36 – 40	MSc	Information Systems	6 – 10 years
Exp5	KIU	Female	36 – 40	MSc	Computer Science	11 – 15 years
Exp6	MUST	Male	Above 45	MSc	Information Systems	6 – 10 years
Exp7	MUST	Female	Above 45	PhD	Information Systems	11 – 15 years
Exp8	Busitema	Male	41 – 45	PhD	Biomedical Science	11 – 15 years
Exp9	MUST	Female	31 – 35	MSc	Computer Science	6 – 10 years
Exp10	KIU	Male	36 – 40	MSc	Information Systems	Above 15 years

In order to effectively validate the model, the validation form was developed with additional comment section for evaluators (experts) inputs, at both the construct and item levels. The checklist items attached to the evaluation tool were then used by experts to guide the evaluation process. Table 19 displays evaluators' feedback and comments for each construct.

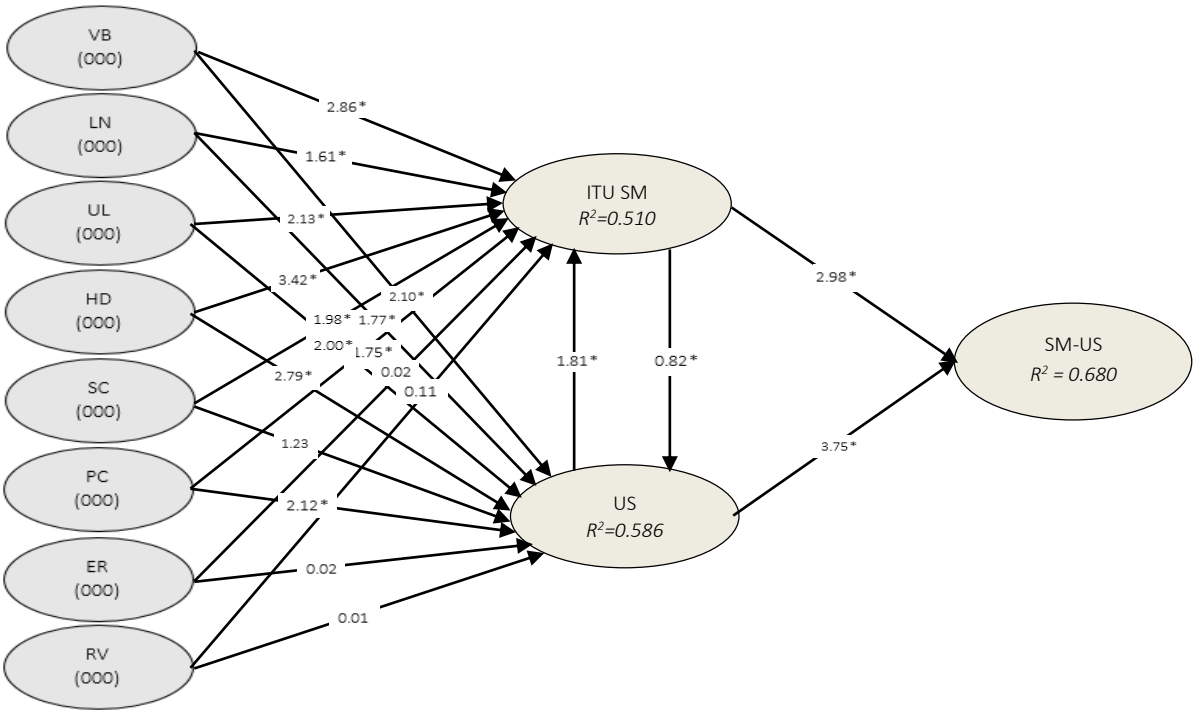
Table 19: Evaluation feedbacks and comments

FACTORS	EXP1	EXP2	EXP3	EXP4	EXP5	EXP6	EXP7	EXP8	EXP9	EXP10	AVSC	Remarks
VB	3.2	3	2.7	4	3.1	4	3.2	3.1	4	3.2	**3.35**	Important
LB	2.7	3.7	4	3.2	3	3.2	3.4	3	3.2	3.7	**3.31**	Important
HD	4	2.8	3.2	2.8	4	3.7	4	3.2	3.7	2.8	**3.42**	Important
UL	3.2	3.1	2.7	3.1	2.7	2.8	2.2	2.7	2.8	3.1	**2.84**	Moderate
SC	3.7	3	2.8	3	4	3.1	3.7	2.6	3.1	3	**3.20**	Important
PC	2.8	4	3.1	4	3.2	3	2.8	3.2	3	4	**3.31**	Important
US	3.1	3.2	3	2.8	3.7	4	3.1	3.7	2.6	2.7	**3.19**	Important
ITU SM	3	2.7	4	3.1	2.8	3.7	3	2.8	2.8	3	**3.09**	Important
SM-US	2.8	4	3.2	3	3.1	2.8	4	3.1	3.1	3.2	**3.23**	Important
AVSC	**3.17**	**3.28**	**3.19**	**3.22**	**3.29**	**3.37**	**3.27**	**3.04**	**3.14**	**3.19**		
Visibility (VB), learnability (LN), user language (UL), help and documentation (HD), security (SC), privacy and confidentiality (PC), intention to use SM (ITU SM), user satisfaction (US), and Secure SM usage (SM-US). 'less important' (1 to < 2), 'moderate' (2 to < 3), and 'important' (3 to ≥ 4)												

Table 19 above provides the average score (AVSC) for each construct as scored by each experts. The rating score guide used include; 'less important' (1 to < 2), 'moderate' (2 to < 3), and 'important' (3 to ≤ 4). Notably, each expert's evaluation of individual construct based on scores for individual checklist items were all averaged above three, except *user language* that was considered to be moderately important with an average score of 2.84. This indicates that all participants considered each construct at least important for prediction of a secure SM usage and medical information safety. In addition, the overall average for each construct across all participants also indicates that the construct was considered by all the experts to be important. While cumulatively all construct scored above three ('important'), some individual checklist items were scored 'not important' and 'moderately important' by some participants. This could be due to some reservations regarding specific checklist items in certain situations.

Therefore, based on CR values (≥ 0.70), AVE values (≥ 0.50) and AVSC values (≥ 3), the model is valid and fit the datasets well. Altogether, the key SM socio-technical information security factors considered in structural equation model include *visibility* (VB), *learnability* (LN), *user language* (UL), *help* and *documentations (*HD), *Security* (SC), *Privacy* and *Confidentiality* (PC), *error handling* (ER), *process revocability* (RV), *intention to use SM* (ITU SM), *user satisfaction* (US), and *secure SM usage* (SM-US). Figure 10 below present the final validated model for adopting a secure SM usage in Medical Institutions in Uganda.

Validated Model (SM socio-technical information security factors -> Secure SM usage)



Visibility (VB), learnability (LN), user language (UL), help and documentation (HD), security (SC), privacy and confidentiality (PC), intention to use SM (ITU SM), user satisfaction (US), and Secure SM usage (SM-US). The other factors dropped include; error handling (ER), revocability (RV), and expressiveness (EX). Based on CR values (≥ 0.70), AVE values (≥ 0.50) and AVSC values (≥ 3), the model fit the datasets well

Figure 10: Validated model (SM socio-technical information security factors -> Secure SM usage)

4.9 Chapter Four Summary

In conclusion, chapter four covered data presentations, data analysis, and brief narratives of the key analysis results and the findings. Overall, the analysis process was guided by research objectives, research questions, and the characteristics of the datasets. The main dataset used in analysis process include respondents' demographic profiles, SM usage characteristics, and medical information breaches. Both descriptive and inferential statistical tools were employed in data analysis process. Comparatively, the summary of the datasets for MUST, KIU, and related studies shows similar trends in percentage distributions among SM usage categories, (Mirembe, Lubega & Kibukamusoke, 2019). However, the leading types of SM platforms reported among students include WhatsApp, and Facebook. Overall, over 80% of the respondents across categorical divides acknowledged sharing medical data on different SM platforms. On the other hand, occurrence of medical information breaches reported within respondent categories ranges from 27% to 42% (Figure 6), while frequency in medical information breaches ranges from 33% to 46% (Figure 7), and the level of agreement in medical information breaches ranges from 39% to 42% (Figure 8). Thus, the 3 sets of percentage values complement each other, and they can all be used to explain the prevalence rate of medical information breaches in line with specific objective one.

Preliminarily, normality test was performed, and the results indicate that the datasets for SM socio-technical information security factors were not normally distributed, therefore the researcher opted for non-parametric tests; chi-square test, Spearman's Rank correlations, and Ordinal Regression analysis (Keya & Rahmatullah, 2016). Chi-square test results showed statistically significant levels of associations between selected demographic profiles and medical information breaches. On the other hand, Spearman's Rank correlation results indicate positive and significant levels of correlations between the SM socio-technical information security factors, and secure SM usage factor, but mainly negative and significant levels of correlations between the SM socio-technical information security factors, and medical information breaches. Altogether, the measurement model indicated good fitting information to the datasets, whereby, Secure SM usage is significantly influenced by SM socio-technical information security factors. Relatively, *visibility*, *user language*, *help* and *documentation,* and *privacy* and *confidentiality* have better predictive strength compared to *learnability* and *security* factors. The social dimensional factors presented a better predictive estimates to *user satisfaction*, *intention to use SM*, and *Secure SM usage* compared to technical dimension. *User satisfaction* demonstrated a better predictive estimates to *Secure SM usage* compared to *intention to use*. Overall, pseudo $R^2 = 0.68$ suggests that 68% of the changes in dependent variable (Secure SM usage) was as a result of the changes in independent variable (SM socio-technical information security factors). Nevertheless, the detailed discussion of the analysis results, including interpretation of the key findings, and recommendations are covered in chapter five and six accordingly (Keya & Rahmatullah, 2016).

CHAPTER FIVE

DISCUSSIONS OF RESULTS

5.1 Introduction

Chapter five covers discussion and interpretation of analysis results. The interpretation is based on the key findings of the study, in accordance with the research objectives, and research questions. However, the beginning section of the chapter commence with a recap of the main reference points of the study, including the research problem, research purpose, research objectives, and the methodology used. Followed by sections on discussion and interpretation of the analysis results in line with the key findings of the study, but taking into consideration the research objectives, research questions, as well as related studies accordingly.

5.2 The key Reference points of the Study

Generally, the main purpose of this study was to develop a model for adopting a secure SM usage in medical institutions in Uganda. The study problem was based on the balance of choice between SM usage and the profound need of preserving medical information safety, which seem to be a stumbling block hindering ratification and adoption of SM usage in medical institutions in Uganda (Alunyu, et al., 2021; Mirembe, Lubega & Kibukamusoke, 2019; Whyte & Hennessy, 2017; Kaddu & Mukasa, 2016; Roy et al., 2016). Relatively, existing studies often focus on information security challenges associated with mainly the technical aspects SM usage, while ignoring the social aspect. However, this study took into considerations both the social and technical dimensions of SM usage, with respect to medical information security (Mutebi, et al., 2022). Thus, the study concepts was grounded on socio-technical system theory, extended DeLone and McLean theory, and usable-security principles accordingly (Edgardo, Indira, Monica & Wenli, 2018; Ferreira, Koenig, & Lenzini, 2014). As guided by the theories, SM socio-technical information security factors were identified, validated, and used to develop the intended model, which can be used to adopt a secure SM usage in medical institutions in Uganda. To realize the study objectives, the study followed post-positivism philosophy – functionalism paradigm, abductive reasoning approach, and mixed method design. Whereby, the relevant study constructs and the measures were derived accordingly.

Specifically, data were collected using questionnaire survey (Google form), and later processed and prepared for analysis. Both descriptive and inferential statistical analysis methods were used. The key analysis results, and the findings were then generated in line with the following specific objectives; 1) to identify the key SM socio-technical information security factors with respect to SM usage and

medical information safety; 2) to establish the types of relationships existing between SM socio-technical information security factors, and SM usage, as well as medical information breaches; 3) to design a model for adopting a secure SM usage in medical institutions in Uganda; 4) to validate the developed model. In line with specific objective, the study was intended to answer the following research questions: 1) What were the key SM socio-technical information security factors influencing SM usage and medical information safety? 2) What are the types of relationships existing between SM socio-technical information security factors, SM usage and medical information breaches? 3) What is the appropriate design model necessary to adopt a secure SM usage in medical institutions in Uganda? Subsequently, the results which were expected to answer the research question were then generated and presented accordingly.

5.2.1 Prevalence of medical information breaches

With respect to medical information breaches, 3 sets of percentage values could be used to explain the prevalence rate of medical information breaches due to SM usage; occurrence of medical information breaches (27% to 42%), frequency in medical information breaches (33% to 46%), and the level of agreement in medical information breaches (39% to 42%). In line with other related studies, the percentage values include, 29% to 38% by Kaddu & Mukasa (2016), and 22% to 31% by Alunyu, et al. (2021). However, there is slight over-edge in percentage distribution between KIU compared to MUST and related studies. The over-edge could also be attributed to the population and sampling errors. However, in line with demographic profile, the prevalence rate were highly recorded among medical students (67%) compared to medical staff (33%); male students (64%) compared to female students (36%); age group < 35 years (69%) compared to others (31%). In line with SM usage engagement, the breaches were highly recorded among WhatsApp users (72%) compared to others (28%); SM user experience > 5 years (78%) compared to others (22%); frequency of SM usage: always and often (64%) compared to others (36%); number of contacts/friends connected > 150 (69%) compared to others (31%). Overall, the findings would enhance SM practitioners, medical institutions, and SM researchers with empirical basis to rationalize and comprehend the vulnerable scopes of SM usage in line with medical information safety (Mutebi et al., 2022; Lombardo, Mordonini, & Tomaiuolo, 2021; Whyte & Hennessy, 2017).

However, with respect to frequency in medical information breaches, MUST result (46%) shows slight over-edge in percentage distributions compared to KIU (43%). Within demographic profile dataset, the frequency rate were highly recorded among medical students (64%) compared to medical staff (36%); male students (68%) compared to female students (32%); age group < 35 years (66%)

compared to others (34%). In line with SM usage engagement, the frequency were highly recorded among; WhatsApp users (63%) compared to others (37%); SM user experience > 5 years (70%) compared to others (30%); frequency of SM usage: always and often (60%) compared to others (40%); number of contacts/friends connected > 150 (71%) compared to others (29%). Notably, the frequency in medical information breaches ranges from 33% to 46%. Altogether, the findings would enhance SM practitioners, medical institutions, and SM researchers with empirical basis to rationalize the vulnerable scopes of SM usage with respect to medical information safety. Hence this would support secures SM usage (Lombardo, Mordonini, & Tomaiuolo, 2021).

5.2.2 SM socio-technical information security factors

With respect to specific objective 1, the researcher's intention was to identify the key SM socio-technical information security factors associated with SM usage and medical information safety. Presumably, the key SM socio-technical information security factors were mainly identified from existing literatures, as guided by socio-technical system theory, the extended DeLone and McLean theory, and usable-security principles (Mutebi, et al., 2022; Agrawal, et al., 2022; Mujinga, Eloff & Kroeze, 2019; Edgardo, Indira, Monica & Wenli, 2018; Ferreira, Koenig, & Lenzini, 2014). In this case, the factors identified and validated under social dimension include; 1) usability factors – *visibility*, and *learnability*; 2) training and education factors – *help* and *documentation,* and *user language* (Schneiderman et al., 2016; Preece et al, 2015; Ogara, Koh, & Prybutok, 2014; Zahidi, Lim & Woods, 2014). On the other hand, the key factors identified under technical dimension include; 3) SM technology development factors – *error handling*, and *process revocability*; 4) task factors – *security, expressiveness* and, *privacy* and *confidentiality* (Mujinga, Eloff & Kroeze 2019; Schnneiderman et al., 2016; Yeratziotis et al., 2012). Altogether, 8 factors were maintained and used in the structural equation model, including *visibility*, *learnability*, *help* and *documentation, user language, security,* and *privacy* and *confidentiality*, *error handling,* and *process revocability*. Remarkably, categorizing this factors under social, and technical dimensions is a realistic and effective way of mapping the vulnerable information security areas within SM usage domain (Mutebi, et al., 2022; Mujinga, Eloff & Kroeze 2019).

5.2.3 Variable associations, and relationships

In line with specific objective 2, Chi-square (x^2) results generated ($x^2 = 7.890$, $df = 4$, $p = 0.096$) show insignificant association between medical institutions (MUST and KIU) and medical information breaches (Table 15). The results also reinforce the earlier position stated, where MUST and KIU datasets displayed similar trends in percentage distributions within medical institutions,

(Table 9). However, with respect to gender, chi-square (x^2) results ($x^2 = 17.348, df = 4, p = 0.002$) show significant association between gender and medical information breaches. Similarly, with respect to medical institutions, chi-square (x^2) results for MUST: gender ($x^2 = 17.822, df = 4, p = 0.001$) shows significant association between gender and medical information breaches, while KIU: gender ($x^2 = 6.084, df = 4, p = 0.193$) shows insignificant difference between gender and medical information breaches. With respect to age-group, chi-square (x^2) results generated ($x^2 = 23.738, df = 12, p = 0.022$) shows significant association between age-groups and medical information breaches. However, with respect to medical institutions, chi-square (x^2) results generated for MUST: age-group ($x^2 = 17.872, df = 12, p = 0.120$), and KIU: age-group ($x^2 = 15.631, df = 12, p = 0.209$) both showed insignificant association between age-groups and medical information breaches (Mutebi, et al., 2022; Whyte & Hennessy, 2017).

Further still, the researcher's intention was to examine the types of relationships between SM socio-technical information security factors, *user satisfactions* (US), *intention to use* SM (ITU-SM), and *medical information breaches* (MIBR). According to Table 15, the correlational relationships between SM socio-technical information security factors and SM-US/US/ITU are positive, strong and significant. While the correlation between SM socio-technical information security factors and MIBR are negative, strong, and significant. The negative correlations include; visibility (r = - 0.58, p = 0.000), learnability (r = - 0.62, $p = 0.000$), *user satisfaction* ($r = - 0.75, p = 0.000$), *intention to use* ($r = - 0.78, p = 0.000$), *help* and *documentation* ($r = - 0.77, p = 0.000$), *user language* ($r = - 0.68, p = 0.002$), *security* ($r = -0.76, p < 0.000$), *privacy* and *confidentiality* ($r = - 0.62, p = 0.000$). On the other hand, factors with weaker but significant associations include; *errors handling* ($r = 0.36, p = 0.041$), *process revocability* ($r = - 0.42, p < 0.029$), and *expressiveness* ($r = 0.44, p < 0.002$).

Notably, strong correlations could suggest consistency in the responses (Keya & Rahmatullah, 2016). While the negative correlations suggest that the level of medical information breaches decrease with increase in the level of compliance in SM socio-technical information security factors. Subsequently, *error handling*, *process revocability*, and *expressiveness* demonstrated weaker correlation. In line with other studies, the Spearman's Rank coefficient results showed similar and stronger correlation between the social dimensional factors, compared to the technical dimension, (Whyte & Hennessy, 2017; Albladi, & Weir, 2018; Tayouri, 2015). However, the disparity could also be explained by the difference between respondents who are more experienced in the technical aspects of SM usage, compared to the less experience social functions. However, subsequent studies would help to further substantiate the findings specified in this study.

5.2.4 Regression analysis results

With respect to objective 3, the researcher's intention was to design a model for adopting a secure SM usage in medical institutions in Uganda. Altogether, a structural equation model was developed and validated based on the measurement model generated after performing Ordinal Regression analysis (Table 16). The key SM socio-technical information security factors considered and used to develop the model include; 1) usability – *visibility* (VB), *learnability* (LN); 2) training and education – *help* and *documentation* (HD), and *user language* (UL). While factors considered under technical dimension include; 3) task performed – *security* (SC), *privacy* and *confidentiality* (PC), *expressiveness* (EX). 4) The factors considered under system development include; *error-handling* (ER), and *revocability* (RV). On the other hand, the key factor considered under ISSM include *user satisfaction* (US), *intention to use SM* (ITU-SM) and *Secure SM usage* (SM-US).

According to Figure 9 and 10, all the hypothesis and parameter estimates generated were significant ($p < 0.05$), except *error-handling* (ER), and *revocability* (RV). Thus, the model shows good fitting information to the dataset, where *Secure SM usage* (SM-US) is significantly associated with SM socio-technical information security factors. Notably, the key factors have demonstrated good and significant levels of parameter estimate useful for predicting US, ITU SM, and SM-US accordingly. Specifically, pseudo $R^2 = 0.510$ for ITU-SM, and 0.586 for US imply predictive strength of 51% for ITU-SM, and 59% for US respectively. Relatively, *visibility, user language, help* and *documentation*, and *privacy* and *confidentiality* have better predictive strength compared to *learnability* and *security* factors. The social dimensional factors demonstrated a better predictive estimates to US, ITU-SM, and SM-US compared to technical dimension. *User satisfaction* demonstrated a better predictive estimates to SM-US compared to *intention to use*. Overall, pseudo $R^2 = 0.68$, suggests that 68% of the changes in dependent variable (SM-US) was as a result of the changes in independent variable (SM socio-technical information security factors). Afterwards, the model was validated using SmartPLS graph, and subject experts. Whereby, discriminate validity of the sample model's construct were validated. This was done using Composite Reliability (CR) and Average Variance Extracted (AVE) values between the constructs and their indicators (Table 17).

5.2.5 Model validation

Generally, model validation is the procedure of evaluating the quality of model performance against the real data. In this case, the model was validated by considering the aspects and the components of the model (Table 17). In line with specific objective 4, both the Average Variance Extracted (AVE) and Composite Reliability (CR) results were considered valid in Structural Equation Modeling

(Henseler, Ringle & Sarstedt, 2015). Thus, assumptions for the requirement limitation for validity check considered in this case were CR (≥ 0.7) and AVE (≥ 0.5) (Sarstedt, Ringle, & Hair, 2021). Therefore, CR and AVE estimates values did not violate the necessary requirement limitation. Hence, all the constructs of the model have achieved the minimum threshold values, and the model would be considered a good-fit to validity test results.

Additionally, experts were used to evaluate the constructs and the items using evaluation checklist provided to them. In this case, the model was evaluated and allowed the experts to add any comments at both the construct and item levels. Notably, each expert's evaluation of individual construct based on scores for individual checklist items were all averaged above three (Table 19), except *user language* that was considered to be moderately important with an average score of 2.84. This could indicates that all participants considered each construct at least important for SM socio-technical information security design. In addition, the overall average for each construct across all participants also indicates that the construct was considered by all the experts to be important. However, while cumulatively all construct scored above three ('important'), some individual checklist items were scored 'not important' and 'moderately important' by some participants. This was due to some reservations regarding specific checklist items in certain situations

CHAPTER SIX

RECOMMENDATIONS AND CONCLUSIONS

6.1 Recommendations

Firstly, the study recommends that the validated model (Figure 10) be adopted by SM practitioners, medical institutions, SM researchers, and stakeholders. Overall, the model provides empirical and theoretical basis for rationalizing information security requirements associated with SM usage and medical information safety (Mutebi, et al., 2022). With respect to medical institutions, the model provides guidelines to stakeholders in developing SM usage strategies, including policy and curricula development (Nwankwo & Chinecherem, 2020). Thus, SM socio-technical information security approaches would effectively enhance the process of developing strategies, and policies on SM usage. For instance, the model provides key SM socio-technical information security factors to consider in ratifying SM usage in medical operations. Relatively, existing studies often focus on information security challenges associated with mainly the technical aspects SM usage (Tayouri, 2015). However, this study took into consideration both the social and technical dimensions of SM usage, with respect to usable-security principles (Agrawal, et al., 2022). Moreover, formalizing SM usage in these broader context would help medical institutions to enforce accountability in SM usage, and protect the institutions against uncensored usage of SM by stakeholders. This would protect medical institutions against negative consequences such as loss of trust and reputations, legal suit, and financial harm, (Nwankwo & Chinecherem, 2020; Jomin & Takura, 2019; Surani, et al., 2017). Nevertheless, the study also recommends subsequent researchers to explore the research areas and refine the validated factors, including the less significant factors, and use them to generate more empirical evidence to enrich the foundation of SM researches.

With respect to the study limitations, more empirical studies still need to be conducted to enrich the theoretical foundations supporting SM usage in medical education, (Roy et al., 2016). The few existing studies related to SM usage in medical education depend mainly on descriptive approaches, or practitioner experience, or literature-search, which may be context specific, (Whyte & Hennessy, 2017; Surani, et al., 2017; Roy et al., 2016). As such, their measures and findings could be limited in scopes, and prone to duplications, redundancy, or inconsistency. Formally, the subjective nature of SM concepts make it complex for existing theories and studies to have a standard definition of SM concepts (Emamjome et al., 2013). Therefore, to address the challenges, more empirical studies need to focus on generating quantitative evidence to substantiate some of the unique challenges associated

with SM usage. As such, the studies would help to guide and improve on the level of awareness on the choice of SM functions. Furthermore, to improve the research outcome without losing the quality of the time factor, the researcher recommends that further study should take into consideration a longitudinal study design, which could be time-consuming and expensive, but the outcomes could be more effective compared to cross-sectional study design. Subsequent studies would need to mitigate the effect of limitations associated with online survey by introducing data collection methods that allows research assistants to guide respondents during data collection process, and probably develop more open-ended and subjective questions, which would enhance deeper investigations and probing of research subjects, (Taherdoost, 2016).

6.2 Study Contributions

Both empirical and theoretical findings contribute to our understanding of relationship between SM socio-technical information security factors, SM usage and medical information safety. More especially, in the domain combining SM socio-technical information security concepts, the extended DeLone and McLean theory of ISSM, usable-security principles, and medical information safety. Relatively, the contribution of existing studies often focus on the descriptive roles of SM usage in medical education, while specifying the benefits and risks associated with mainly the technical aspect of SM usage, (Whyte & Hennessy, 2017; Roy et al., 2016; Wilcox, & Bhattacharya, 2015; Sherbino & Frank, 2014; Pander et al., 2014). However, in the context of medical training and medical operations, little is known about SM socio-technical information security factors associated with reported cases of medical information breaches, (Whyte & Hennessy, 2017; Roy et al., 2016). Therefore, as SM usage embracement levels keep rising amidst significant levels of medical information breaches being reported, medical institutions would require a broader empirical and theoretical basis for rationalizing and ratifying SM usage in their strategies, policy, and curricula development process, (Katz & Nandi, 2021; Nwankwo & Chinecherem, 2020; Mirembe, Lubega & Kibukamusoke, 2019; Roy et al., 2016).

With respect to practical contribution, the researcher identified and validated 9 SM socio-technical information security factors, and develop the intended model. Thus, the study outcomes provides a model, which can be used as a blueprint to guide medical institutions to formalize, ratify and adopt SM usage in medical institutions. Literally, formalizing SM usage in medical operations would help to regulate and enforce standards and accountability in SM usage, and protect medical institutions against uncensored usage of SM by stakeholders. After all, uncensored usage of SM in a formal organizational setting is a breeding ground for unscrupulous behaviors (Nwankwo & Chinecherem,

2020; Roy et al., 2015). Therefore, formalizing SM usage would protect medical institutions against negative implications such as loss of trust and reputations, legal suit, and financial harm (Nwankwo & Chinecherem, 2020; Jomin & Takura, 2019; Surani, et al., 2017; Adler et al., 2015). More so, the study outcomes would provide guidance, and help improve on the level of awareness in line with SM usage and medical information safety, with respect to medical training activities – learning, teaching, research and clinical services (Jomin & Takura, 2019). This would enhance coordination and sharing of trusted contents, knowledge and information among the medical students, medical staff including supervisors (Jomin & Takura, 2019).

Overall, addressing information security gap in SM usage in medical care is in the best interest of every SM user in healthcare fraternity. With better information security mechanism on SM usage, patients and community confidence, and trust in healthcare systems will improve. When patients and community are assured of the safety of their private information, they would be more willing to disclose sensitive information to physicians, and this will improve on the quality of medical care and services provided (Jomin & Takura, 2019). According to Liaw & Hannan (2011), 49.1% of patients in Australia confirmed withholding information from clinicians based on privacy and confidentiality concerns (Usher et al., 2014). Recently, among the global IT related breaches reported, SM incidents accounted for over 56% of the 4.5 billion data records compromised in 2018 (Katz & Nandi, 2021; Seh et al., 2020; HIPAA 2020). In Uganda, Alunyu, et al. (2021) study indicates that 22% to 31% of respondents reported IT related breaches in medical data in healthcare sites in Uganda. Therefore, this study contribute to the existing body of knowledge by identifying and validating the key factors, and developing a model based on validated SM socio-technical information security factors, in line with SM usage and medical information safety.

6.3 Limitation of the Study

As with several researches, the design of this study was subject to limitations. However, the researcher anticipated some of the limitations of the research outcomes and catered for them in the study design process. Nevertheless, the key study limitations encountered included time constraint limitation, self-reported data limitation, lack of prior research studies in the study topic (Nwankwo & Chinecherem, 2020; Whyte & Hennessy, 2017; Roy et al., 2015), and lack of institutional policy on SM usage. Altogether, the impact of the limitations are discussed in the following sections below, and recommendations made accordingly.

6.3.1 Time-constraint limitation

The time available to execute the research processes were constrained by practical issues such as restricted academic calendar, limited funding, and predefined datelines to complete the research activities. Nevertheless, the researcher overcame the time-constraint by adopting to realistic and time-efficient methods such as online survey methods, and automated data analysis process. Online survey enabled the researcher to collect enormous, affordable and reliable data within short period of time. Additionally, the Google form platform used had automated functions, which helped to ease the time constraint imposed on the analysis processes. However, to improve the research outcome without losing the quality of the time factor, the researcher recommends that subsequent study should take into consideration a longitudinal study design, which could be time-consuming and expensive, but the research outcomes could be more effective compared to the other time-constrained design methods such as cross-sectional study design.

6.3.2 Self-reported data

On the other hand, COVID-19 pandemic imposed restrictions on the choice of data collection processes. Thus, the researcher opted for online survey to minimize social contact among research participants. However, an online survey is often limited to close-ended questions and self-reported data (Taherdoost, 2016). In this case, there were cases of low response rate, and respondent bias. For instance, some respondents would just tick through the questionnaire without paying much attention to the questions. However, the researcher anticipated and cater for some of the limitation in the study design. Whereby, the structure of the questions and corresponding answers were simple, brief and precise. More so, the exact sample size computed in Table 7 were exaggerated to compensate for errors that could arise due to low response rate, or elimination due to data cleaning process (Taherdoost, 2016). Therefore, datasets collected were processed, cleaned and sorted before performing final analysis process. For instance, questionnaire were checked to eliminate inadequate and incomplete questionnaires. Nevertheless, subsequent studies would mitigate the effect of the limitation by including open-ended questions, and introduce data collection methods that allows research assistants to guide respondents during data collection process onsite.

6.3.3 Literature limitation

At the precept of literature review, the main keywords that guided the literature search process included “Social Media usage”, and “Information Security”. Thus, the literature search process generated 170 literatures. However, after resetting and applying significant literature search criteria,

the results were reduced to 99 literatures. Afterwards, the literatures were scrutinized using citation guides, and 25 literatures were found relevant to the study. However, in line with study gap, only 1 literature was retrieved (Mutebi, et al., 2022; Lombardo, & Tomaiuolo, 2021). And with respect to the study topic, no literature was returned after applying combination of Boolean keywords; "Social Media information security factors AND socio-technical factors AND usable-security factors". Therefore, the literature limitations with respect to the study topic highlight research gaps that needed to be filled. Hence, with respect to the study limitations, more empirical studies still need to be conducted to enrich the theoretical foundations supporting SM usage in medical education and other related settings (Mutebi, et al., 2022; Roy et al., 2016).

6.3.4 Lack of institutional policy

Despite the high level of SM embracement in medical operations, medical institutions in Uganda are still conservative in ratifying and adopting SM usage in their policies and curricula (Katz & Nandi, 2021; Olum & Bongomin 2020; Mirembe, Lubega & Kibukamusoke, 2019; Roy et al., 2015). As such, the study found it challenging to establish the formal scope of SM usage in medical training, and clinical operations. However, the study relied on the previous related researches done and published in a similar circumstances. The study also relied on the facts gathered through primary data, using respondent's experience, as well as literature search (Nwankwo & Chinecherem, 2020; Mirembe, Lubega & Kibukamusoke, 2019). Nevertheless, all these limitations highlights significant research gaps yet to be covered in the area of SM usage and medical education in Uganda.

6.4 Conclusion

The main purpose of this study was to develop a model for adopting a secure SM usage in medical institutions in Uganda. Overall, the study purpose was achieved with an intended model developed, and the key results obtained accordingly. With respect to specific objective 1, the key SM socio-technical information security factors were identified, while 27% to 42% of the respondents within categorical divides acknowledged occurrence of medical information breaches due to SM usage. Relatively, the percentage of prevalence rate of medical information breaches shows similar trend with related literatures (Alunyu, et al., 2021; Mirembe, Lubega & Kibukamusoke, 2019; Whyte & Hennessy, 2017; Kaddu & Mukasa, 2016; Roy et al., 2016). However, the trend shows slightly increasing levels of percentage prevalence among related studies done overtime, (Alunyu, et al., 2021; Kaddu & Mukasa, 2016). Overall, 9 SM socio-technical information security factors were identified, verified and validated, accordingly. The key factors include; *visibility, learnability, errors handling, process revocability, expressiveness, help* and *documentations, user language, security,*

and *privacy* and *confidentiality*. These factors were the common denominators cited across the main domain of the study concepts; SM usage and information security factors, socio-technical information system factors, usable-security factors, and IS success factors accordingly (Agrawal, et al., 2022; Jain, Sahoo, & Kaubiyal, 2021; Obrain et al., 2021; Ma, Zhang, Li, & Wu, 2019; Albladi, & Weir, 2018; Tayouri, 2015; Wilcox, & Bhattacharya, 2015). Subsequently, the outputs of objective 1 were used to provide data inputs for subsequent objectives accordingly.

From preliminary assessment, normality test was performed and the results indicated that the datasets were not normally distributed. Therefore, the researcher opted for non-parametric tests. Hence, with respect to specific objective 2, the appropriate statistical tools opted were Chi-square (x^2) test, and Spearman's Rank correlations. Chi-square (x^2) test results showed statistically significant levels of associations between selected demographic datasets, SM usage, and medical information breaches. On the other hand, Spearman's Rank correlation results indicated significant levels of correlations between SM socio-technical information security factors, user satisfaction, intention to use SM, Secure SM usage and medical information breaches. Subsequently, specific objective 3 was attained by performing ordinal regression analysis. The results of the measurement model displayed good fitting information to the datasets, whereby *secure SM usage* (SM-US) was significantly associated with user satisfaction, intention to use SM, and SM socio-technical information security factors. Overall pseudo $R^2 = 0.68$, suggests that 68% of the changes in Secure SM usage was as a result of the changes in SM socio-technical information security factors. The significance of this study outcomes provide SM practitioners, medical institutions, SM researchers, and stakeholders with theoretical and empirical basis to rationalize, and comprehend information security challenges associated with SM usage and medical information safety. Thus, the model can be used as a blueprint to enhance medical institutions in ratifying SM usage in operations (Mutebi et al., 2022; Nwankwo & Chinecherem, 2020; Whyte & Hennessy, 2017).

REFERENCES

Abraham, R.R., Velladath, S.U., Elman, B.E., Ezreen, Z.E., Sobri, L., Saha, M.D.S., Ghazali, M.S., Bakar, A.A., & Hussain, A.M. (2018). Exploring Time Management Skills of First Year Undergraduate Medical and Allied Health Science Students. *Journal of Clinical and Diagnostic Research*, 12(10): 07-10.

Abuhashesh, M.Y. (2014). 'Integration of Social Media in Businesses', *International Journal of Business Environment*, 5 (8): 202-209.

Adler, J., Demicco, M., & Neiditz, J. (2015). Critical privacy and data security risk management issues for the franchisor. *Franchise Law Journal*, 35, 79-92

Agrawal, Alenezi, M., Khan, S. A., Kumar, R., & Khan, R. A. (2022). Multi-level Fuzzy system for usable-security assessment. *Journal of King Saud University. Computer and Information Sciences*, 34(3), 657–665. https://doi.org/10.1016/j.jksuci.2019.04.007

AHIMA (2011). American Health Information Management Association Code of Ethics.

Alenezi, A.N., & Yaiesh, S.M. (2018). The ubiquitous invasion of social media in lifelong learning in medical education. *Review Article Kuwait Medical Journal,* 50(3): 271-277.

Al-Rahmi, Othman, M. S., & Yusuf, L. M. (2015). The Role of Social Media for Collaborative Learning to Improve Academic Performance of Students and Researchers in Malaysian Higher Education. *International Review of Research in Open and Distance Learning*, 16(4), 177–204. https://doi.org/10.19173/irrodl.v16i4.2326

Albladi, & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*, 8(1). https://doi.org/10.1186/s13673-018-0128-7

Alunyu, E., A., et al., (2021). Investigating the Impediments to Accessing Reliable, Timely and Integrated Electronic Patient Data in Healthcare Sites in Uganda. 522-532. 10.5220/0010266705220532.

Amgad, M. and AlFaar, A.S. (2014). Integrating web 2.0 in clinical research education in a developing country, Journal of Cancer Education, 29(3): 536–540

Amin, M. E. (2005). *Foundations of Statistical Inference for Social Science Research*. Kampala, Makerere University Printery.

Andrew Swinney. (2019). CREATING A SOCIAL MEDIA RISK ASSESSMENT. *Bank News*, *119*(2), 10–13

Andriole, K.P. (2014). "Security of Electronic Medical Information and Patient Privacy: What You Need to Know". *Journal of the American College of Radiology*. 11(12): 1212-1216.

Belanger, F., Watson-Manheim, M.B., & Swan, B.R. (2013). A multi-level socio-technical systems telecommuting framework. *Behavior and Information Technology*, 32(12), 1257-1279.

Bell, D. E., (2015) "Looking back at the Bell-La Padula model," in Proc. 21st Annu. Comput. Secur. Appl. Conf., Tucson, AZ, USA, pp. 1–15.

Beltran-Aroca, C.M., Girela-Lopez, E., Collazo-Chao, E., Montero-Perez-barquero, M., & Munoz-Villanueva, M.C. (2016). Confidentiality breaches in clinical practice: what happens in hospitals? *BMC Medical Ethics* 17, 52.

Benetoli, A., Chen, T. F., & Aslani, P. (2015). The use of social media in pharmacy practice and education. *Res Social Adm Pharm*, 11(1): 01- 46.

Bhattacherjee, A. (2012). Social Science Research: "*Principles, Methods and Practices*". 2nd edition, ISBN: 13:978-1475146127, University of South Florida, USA – Florida

Birkhauer, J., Gaab, J., Kossowsky, J., et al. (2017). Trust in Health care professional and health outcome: A meat-analysis. *PLoS One*. 12(2): eCD004134.

Bongomin, F., et al., (2021). Internal Medicine Clerkship amidst COVID-19 Pandemic: A Cross-sectional Study of the Clinical Learning Experience of Undergraduate Medical Students at Makerere University, Uganda. *Advances in Medical Education and Practices,* 12: 253-262.

Boucher, S.C. (2015). "Functionalism and structuralism as philosophical stances: van Fraassen meets the Philosophy of Biology". *Biol Philos*, 30(3), 383-403.

Bowman MA, Maxwell RA. A beginner's guide to avoiding Protected Health Information (PHI) issues in clinical research - With how-to's in REDCap Data Management Software. J Biomed Inform. 2018 Sep;85:49-55.

Boyd, M., & Ellison, B. (2007). "Social Network Sites: Definition, History, and Scholarship". *Journal of Computer-Mediated Communication*. 13(1): 210-230.

Bramer, Rethlefsen, M., Kleijnen, J., & Franco Duran, O. (2017). Optimal database combinations for literature searches in systematic reviews: a prospective exploratory study. *Systematic Reviews*, *6*(1), 245–245. https://doi.org/10.1186/s13643-017-0644-y

Brodnik, M., Rinehart-Thompson, L.A., & Reynolds R.B. (2012). *Fundamental of Law for Health Informatics and Information Management Professionals* (2nd ed.) Chicago, IL: American Health Information Management Association.

Cartledge, P., Miller, M., & Phillips, B. (2013). "The use of social-networking sites in medical education", *Medical Teacher Journal*, 35(10): 847 – 857.

Casteel, A., & Bridier, N. L. (2021). Describing populations and samples in doctoral student research. *International Journal of Doctoral Studies*, 16, 339-362.

Chai, Das, S., & Rao, H. R. (2011). Factors Affecting Bloggers' Knowledge Sharing: An Investigation Across Gender. *Journal of Management Information Systems*, *28*(3), 309–342. https://doi.org/10.2753/MIS0742-1222280309

Chan, W.S., & Leung, A.Y. (2018). Use of social network sites for communication among health professionals: systematic review, *Journal of Med Internet Res*. 20(3):e117

Chibita, M.B. (2016). Digital activism in Uganda: Critical Reflection on Emerging Trends in Sub-Saharan Africa. Cham: Palgrave Macmillan, 69-93

Chen, J. Mishler, S. Hu B., Li N. & Proctor, R. W. (2018). The description experience gap in the effect of warning reliability on user trust and performance in a phishing detection context. *International Journal of Human Computers Studies*, 119: 35–47

Cheston, C. C., Flickinger, T. E., & Chisolm, M. S. (2013). "Social media use in medical education", *Academic Medicine Journal*, 88(6): 893-901.

Cheung, C.M.K., & Lee, M.K.O. (2010) "A Theoretical Model of Intentional Social Action in Online Social Networks," Decision Support Systems, 49(1): 24-30.

Chibita, M. B. (2016), 'Digital activism in Uganda', in B. Mutsvairo (ed.), Digital Activism in the Social Media Era: Critical Reflections on Emerging Trends in Sub Saharan Africa, Cham: Palgrave Macmillan, pp. 69–93.

Chretien, K., & Kind, T. (2013). Social media and clinical care: Ethical, professional, and social implications. *Circulation Journal*, 127(13):1413–1421.

Chui, M., Manyika, J., Dobbs, R., et al. (2012). The social economy: Unlocking value and productivity through social technologies: Mc kinsye Global Institute.

Chugh, R., & Ruhi, U. (2018). Social Media in Higher Education: A Literature Review of Facebook. *Journal of Education and Information Technologies*, 23 (2): 604-616.

CIPESA (2020). The State of Internet Freedom in Africa**:** *Promoting Effective and Inclusive ICT Policy in Africa***.** https://cipesa.org/2020/09/report-the-state-of-internet-freedom-in-africa-2020.

Coventry L. & Branley D., (2018) Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113:48 – 52. ISSN 0378-5122.

Cristia, M., Rossi, G. (2021) Automated Proof of Bell–LaPadula Security Properties. *J Autom Reasoning* 65, 463–478.

Decuypere, M. & Bruneel, S. (2012). Social Learning Sites? In Kathryn Moyle & Guus Wijngaards. Student Reactions to Learning with Technologies: Perceptions and Outcomes: (249-268). Hershey: IGI Global.

Di Gangi, Johnston, A. C., Worrell, J. L., & Thompson, S. C. (2017). What could possibly go wrong? A multi-panel Delphi study of organizational social media risk. *Information Systems Frontiers*, *20*(5), 1097–1116. https://doi.org/10.1007/s10796-016-9714-2

Edgardo D., Indira R. G., & Monica A. & Wenli W., (2018). A cloud update of the DeLone and McLean model of information systems success. *Journal of Information Technology Management*, Vol 29 (3): 23 – 34.

Edosomwan, S., Prakasan, S.K., Kouame, D., Watson, J., & Seymour, T. (2011). The history of social media and its impact on business. *Journal of Applied Management and Entrepreneurship*. 16(3): 79-91.

Emamjome, F.F., Rabaai, A.A., Gable, G.G., & Bandara, W. (2013). Information quality in SM: a conceptual model. *Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2013)*, AIS Electronic Library (AIsel), Jeju Island, Korea, 72.

Fenwick, T. (2016). Social media, professionalism and higher education: a sociomaterial consideration. *Studies in Higher Education*, 41(4): 664-677.

Ferreira, Huynen, J.-L., Koenig, V., & Lenzini, G. (2014). A Conceptual Framework to Study Socio-Technical Security. In *Human Aspects of Information Security, Privacy, and Trust* (pp. 318–329). Springer International Publishing. https://doi.org/10.1007/978-3-319-07620-1_28

Fire, M., Goldschmidt, R., Elovici, Y. (2014). Online social net-works: threats and solutions. *IEEE Commun Surv Tutorials*, 16 (4): 2019-2036

Ford, L.A. (2017), "Selection issues of formative models", *Journal of Management Development*, 36 (5): 660-670.

Gartzke, Eric & Lindsay, Jon R. (2019). *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press. doi:10.1093/oso/9780190908645.001.0001. ISBN 978-0-19-090960-4.

GDPR, (2021). Guidelines 8/2020 on the targeting of social media users. Version 2.0

Gray, K., Annabell L., & Kennedy, G. (2010). Medical student's use of Facebook to support learning: Insights from four case studies. *Med. Tech*. 32: 971 – 976.

Greenhow, C., & Lewin, C. (2016). Social Media and Education: Reconceptualizing the Boundaries of Formal and Informal Learning. *Journal of Learning, Media and Technology*, 41 (1): 6-30

Hair, J.F., William, C.B., Barry, J.B., & Rolph, E.A. (2010). *Multivariate Data Analysis*, Englewood Cliffs, NJ: Prentice Hall.

Hamid, S., Waycott, J., Kurnia, S., & Chang, S. (2015). Understanding Student's Perceptions on the Benefits of Online Social Networking Use for Teaching and Learning. *The Internet and Higher Education Journal*. 26: 1-9

Hamm, A. et al, (2013). Social media use by health care professionals and trainees: A scoping review. *Academic medicine? Journal of the Association of American Medical Colleges*, 88(8), 1376-1383

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135.

Hillman, T., & Sherbino, J. (2015). "Social media in medical education: A new pedagogical paradigm?" *Postgraduate Medical Journal*, 9(1080): 544-545.

HIPPA, (2018). De-identification of Protected Health Information. *HPPA Journal.* https://www.hipaajournal.com/de-identification-protected-health-information.

Hollinderbaumer, A., Hartz, T., & Uckert, F. (2013). Education 2.0 – How has social media and Web 2.0 been integrated into medical education? A systematical literature review. *GMS Zeitschrift fur Medizinische Ausbildung,* 30 (1).

Househ M, Grainger R, Petersen C, Bamidis P, Merolli M. (2018) Balancing Between Privacy and Patient Needs for Health Information in the Age of Participatory Health and Social Media: A Scoping Review. Yearb Med Inform; 27(1): 29-36

Hu, T., & Zhang, P. (2016). Social media usage as a formative construct: Conceptualization, validation, and implication. *Journal of Information Technology Management*, 27(4), 151-168.

Hu, T., Kettinger, W., & Poston, R. (2015). "The Effect of Online Social Value on Satisfaction and Continued Use of Social Media," *European Journal of Information Systems*, 24 (4): 391-410.

Jain, A. K., Sahoo, S. R. & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex Intell. Syst*. https://doi.org/10.1007/s40747-021-00409-7

Jayakrishna NAIR, Moneer ALSHAIKH and Christopher CULNANE (2020)," A Comparative Study of Security and Privacy in Electronic Health Records", Journal of e-health Management, Vol. 2020 (2020), Article ID 557564, DOI:10.5171/2020.557564

Jomin, G., & Takura, B., (2019). Security, Confidentiality, and Privacy in Health of Healthcare Data. International Journal of Trends in Scientific Research and Development, 3(4): 2456-6470.

Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. *Current Journal of Applied Science and Technology*, 7(4): 396-403.

Kabir, S. M. (2016). *Basic Guidelines for Research: An Introductory Approach for all Disciplines, First Edition*. Bangladesh: Book Zone.

Kaddu, S., & Mukasa, G. (2016). Social media and Social Transformation in Uganda's families. *African Research & Documentations*, (128): 70-80

Kagoya, H.R., et al. (2013). Awareness of, responsiveness to and practice of patient's rights at Uganda's national referral hospital. *African Journal of primary Health care and Family Medicine*, 5 (1): 491.

Kaplan, M. (2012). If you love something, let it go mobile: Mobile marketing and mobile SM 4x4. *Business Horizons*, 55 (2): 129-139.

Katarahweire, M., Bainomugisha & Khalid A. (2020). Data Classification for Secure Mobile Health Data Collection Systems. *Journal of Development Engineering*, 5, 100054.

Katz M., Nandi N., (2021). Social Media and medical Education in the Context of the COVID-19 Pandemics: Scoping Review *JMIR Med Educ,* 7(2): e25892

Kesselheim, J.C., et al. (2014). New professionalism challenges in medical training: an exploration of social networking. *Journal of Medical Education,* 6(1): 100-105.

Keya Rani Das, A. H. M. Rahmatullah Imon (2016). A Brief Review of Tests for Normality. *American Journal of Theoretical and Applied Statistics*. Vol. 5, No. 1, pp. 5-12. doi: 10.11648/j.ajtas.20160501.12

Khamala, D.F., Makori, O., & Njiraine, M. (2018). "Webometrics Ranking and its Relationship to Quality Education and Research in Academic Institutions in Kenya." *Library Philosophy and Practice (e-journal).*

Kietzmann, et al., (2011). Social Media? Get serious! Understanding the functional building blocks of social media. *Bus Horizon*. 54(3): 241-251.

Kim, H., Chan, H.C., & Kankanhalli, A. (2012) "What Motivates People to Purchase Digital Items on Virtual Community Websites? The Desire for Online Self-Presentation," *Information Systems Research,* 23 (4): 1232-1245.

Kind, T. & Evans, Y. (2015). Social media for lifelong learning. International Review ofPsychiatry, 27(2), 124-132

Kirkpatrick, D. (2010). *The Facebook Effect: The Inside Story of the Company that is connecting the World*. Simon & Schuster. ISBN 978-1439102121.

Kuteesa, J., Musiime, V., Munabi, G., et al. (2021). Specialty career preferences among final year medical students at Makerere University College of health science, Uganda: a mixed methods study. *BMC Med Education Journal*, 21, 215

Liaw, S. T. & Hannan, T. (2011). Can we trust the PCEHR not to leak? *Medical Journal of Australia*. 195, 222.

Lie, D.A., Trial J., Schaff, P., Wallace, R., & Elliott, D. (2013) "Being the best we can be": medical students' reflections on physician responsibility in the social media era". *Academic Medical Journal*, 88(2): 240–245.

Lockhat R., (2021). Social media and the Protection of Personal Information Act. *Southern African Journal of Anaesthesia and Analgesia*. 27(6): 69-72 https://doi.org/10.36303/SAJAA. 2021.27.6.S1.2702

Lombardo, Mordonini, M., & Tomaiuolo, M. (2021). Adoption of Social Media in Socio-Technical Systems: A Survey. *Information (Basel), 12*(3), 132. https://doi.org/ 10.3390/info12030132

Madanick, R.D. (2015). 'Education becomes social: The intersection of social media and medical education', Gastroenterology, 149(4): 844–847

Ma, Zhang, S., Li, G., & Wu, Y. (2019). Exploring information security education on social media use: Perspective of uses and gratifications theory. *Aslib Journal of Information Management*, *71*(5), 618–636. https://doi.org/10.1108/AJIM-09-2018-0213

Maloney, S., Moses, A., & Ilic, D. (2014). Social media in health professional education: a student perspective on user levels and perspective applications. *Adv Health Science Education theory practice*, 19(5): 687-697.

Mare, A. (2014). Social Media: The New Protest Drums in Southern Africa? In B. Pătruț & M. Pătruț (Eds.), Social Media in Politics: Case Studies on the Political Power of Social Media (pp. 315–335). Springer International Publishing. https://doi.org/10.1007/978-3-319-04666-2_17

McWay, D. (2010). *Legal and Ethical Aspects of Health Information, Third Edition*. New York: Cengage Learning. Chapter 9.

Melissa, B. (2012). "10". Social Media Marketing: A Strategic Approach (1st ed.). Cengage Learning.

Mirembe, D.P., Lubega, J.T., & Kibukamusoke, M. (2019). Leveraging Social Media in Higher Education: A case of Universities in Uganda. *European Journal of Open, Distance and eLearning*, 22(1), 70-84.

Mujinga, Eloff, M. M., & Kroeze, J. H. (2019). Towards a framework for online information security applications development: A socio-technical approach. *South African Computer Journal*, 31(1), 24–50. https://doi.org/10.18489/sacj.v31i1.587

Mujinga, M., Eloff, M., & Kroeze, J. (2017). A socio-technical approach to information security. In *Proceedings of the 23rd Americas Conference on Information Systems (AMCIS), Boston, MA*, 10-12 August 2017 (1–10).

Mukassa, S. P. (2012). An instrument to assess information systems success in developing countries. [Thesis fully internal (DIV), University of Groningen]. University of Groningen, SOM research school.

Musah, A. (2015). *Social Media Network Participation and Academic Performance in Senior High School in Ghana.* Jeffrey Mingle Lancaster University Ghana

Mutebi, J., Kareyo, M., Chinecherem, U., & Paul, A. (2022). Identification and Validation of Social Media Socio-Technical Information Security Factors with Respect to Usable-Security Principles. *Journal of Computer and Communications*, 10 (8), 41-63.

Nabimanya, D., Sembatya, R., Atuhaire, A., & Mbabazi, P. (2020). Patient's Health Records Management in Ugandan Hospitals: A Case of Kabale Regional Referral Hospital. *International Journal for e-Learning Security (IJeLS)*, Vol 9 (1).

Najjuma, J.N., Ruzaaza, G., Groves, S., Maling, S., & Mugenyi, G. (2016). Multidisciplinary leadership training for undergraduate health science students may improve Uganda healthcare. *African Journal of Health Professions Education*, 8(2): 184-8

Nielsen, J. (2010). What is usability? In C. Wilson (Ed.), User experience re-mastered: Your guide to getting the right design (3–22). Morgan Kaufmann.

Nwankwo, W. & Chinecherem, U. (2020). Institunalising Social Network Solution in Tertiary Educational Institutions. *Journal of Applied Sciences, Information and Computing*, 1(1).

Nysveen, H., & Pedersen, P. E. (2014). Influences of co-creation on brand experience. The role of brand engagement. *International Journal of Market Research*, 56(6), 807-832.

Obar, J.A., & Wildman, S. (2015). Social media definition and the governance challenge: An introduction to the special issue. *Telecomm Policy*, 39(9): 745-750.

Obrain T. Murire, Stephen Flowerday, Kariena Strydom, & Christoffel J.S. Fourie. (2021). Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa. *The Journal for Transdisciplinary Research in Southern Africa, 17*(1), e1–e10. https://doi.org/10.4102/td.v17i1.909

Ogara, S.O., Koh, C.E., & Prybutok, V.R. (2014). Investigating factors affecting social presence and user satisfaction with mobile instant messaging. *Computers in Human Behavior*, 36: 453-459.

Olum, R., Kajjimu, J., Kanyike, A.M., et al. (2020). Perspective of medical students on the COVID - 19 pandemic: survey of nine medical schools in Uganda. *JMIR Public Health Surveill*. 6:e19847.

Paja, E., Dalpiaz, F. & Giorgini, P. (2013). Managing security requirements conflicts in Socio-technical Systems. In: Ng W., Story V. C., Trujillo J. C. (eds) Conceptual Modelling ER 2013. Lecture Notes in Computer Science, 8217. Springer, Berlin, Heidelberg.

Panahi, S., Watson, J., & Partridge, H. (2014). Social media physicians: Exploring the benefits and challenges. *Health Informatics Journal*. 22 (2): 99-112.

Pander, T., Pinilla, S., Dimitriadis, K., & Fischer, M.R., (2014). The use of Facebook in medical education – A literature review. GMS Z Med Ausbild, 31(3):33.

Petersen, C., & Lehmann, U. (2018). Social Media in Health Care: Time for Transparent Privacy Policies and Consent for Data use and Disclosure. *Applied Clinical Informatics*, 9(4): 856-859.

Petronilla Muriithi, David Horner & Lyn Pemberton (2016) Factors contributing to adoption and use of information and communication technologies within research collaborations in Kenya, Information Technology for Development, 22:sup1, 84-100

Philip Nyblom, Gaute Wangen, & Vasileios Gkioulos. (2020). Risk Perceptions on Social Media Use in Norway. *Future Internet*, *12*(12), 211–. https://doi.org/10.3390/fi12120211

Pointer, R., Bosch, T., Chuma, W., & Wasserman, H. (2016, September). *Comparative analysis of civil society, media and conflict*. Media Conflict and Democratization.

Preece, J., Rogers, Y. & Sharp, H. (2015). Interaction design: Beyond Human Computer Interaction. Wiley and Sons.

Qasem, N., Ali, M., Gul, A., & Bilal, S. (2014). Effect of Items Direction (Positive or Negative) on the 797 Factorial Construction and Criterion Related Validity in Likert Scale. Khazar Journal of 798 Humanities and Social Sciences, 17(3), 77-84.

Ralph, M., & Ralph, L. (2010). Weapons of Mass Instruction: The Creative use of Social Media in Improving Pedagogy. *Issues Informing Science Information Technology*. 10(1): 449-460.

Roy, Taylor, J., Cheston, C., Flickinger, T.E., & Chisolm, M.S., (2016). Social Media: Portrait of an Emerging Tool in Medical Education, *Academic Psychiatry Journal*, 40(1):136-140

Sangoseni O, Hellman M, Hill C. (2013) Development and validation of a questionnaire to assess the effect of online learning on behaviors, attitude and clinical practices of physical therapists in United States regarding of evidence-based practice. *Internet J Allied Health Science Practice*; 11:1-12.

Sarstedt, M., Ringle, C. M., & Hair, J. F. (2021). Partial Least Squares Structural Equation Modeling. Springer.

Schneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N. & Diakopoulos, N. (2016). Designing the user interface: Strategies for effective human-computer interaction. Pearson Education.

Seh A. H., et al., (2020). Healthcare data breaches: insights and implications. *Healthcare* 8(2): 133

Shenoy A, & Appel J M, (2017). Safeguarding Confidentiality in Electronic Health Records. Camb Q Healthc Ethics. 26(2): 337-341.

Sherbino, J. and Frank, J.R. (2014). '@SirBill: The power of social media to transform medical education', Postgraduate Medical Journal, 90(1068): 545–546

Simon, M.K., & Goes, J. (2013). *Scope, limitation, and delimitation*. Retrieved from http://dissertationrecipes.com

Surani, Z., et al., (2017). Social media usage among health care providers. BMC Res Notes 10, 654.

Taherdoost, H. 2016. Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. International Journal of Advance Research in Management, 5(2), 18-27

Tamarah, S., & Samantha, S., (2018). Reliability and Validity of the Research Methods Skills Assessment, *International Journal of Teaching and Learning in Higher Education,* Volume 30 (1) 80-90.

Tang, Z., Ding, X., Zhong, Y., Yang, L., & Li, K. (2018). A Self-Adaptive Bell–LaPadula Model Based on Model Training With Historical Access Logs. IEEE Transactions on Information Forensics and Security, 13(8), 2047-2061.

Taitsman, J. K., Grimm, C. M. & Agrawal, S. (2013). Protecting patient privacy and data security. *New England Journal of Medicine*. 368 (11): 977-9.

Tamarah S., & Samantha S., (2018). Reliability and Validity of the Research Methods Skills Assessment. *International Journal of Teaching and Learning in Higher Education*, Volume 30, Number 1, 80-90.

Taylor, Derrick Bryson (2020). "George Floyd Protests: A Timeline". The New York Times. Archived from the original.

Tayouri. (2015). The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Procedia Manufacturing*, *3*, 1096–1100. https://doi.org/10.1016/j.promfg.2015.07.181

Thilini B G Herath, Prashant Khanna, & Monjur Ahmed. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*, *2*(1), 1–18. https://doi.org/10.3390/jcp2010001

Turel, O., & Serenko, A. (2012) "The benefit and danger of Enjoyment with Social Networking Websites," *European Journal of Information Systems*, 21: 512-528.

UMDPC (2017). "Resources: Medical Schools". Kampala: Uganda Medical and Dental Practitioners Council.

UNCST, (2014). National Guidelines for Research involving Humans as Research Participants, Kampala – Uganda.

Usher, K., Woods, C., Casella, E., Glass, N., Wilson, R., Mayner, L., Jackson, D., Brown, J., Duffy, E., Mather, C., Cummings, E. and Irwin, P. (2014). 'Australian health professions student use of social media', Collegian, 21(2): 95–101

Yee, K. (2004). Secure interaction design. *In Proceedings of the 8th International Conference on Financial Cryptography*, (114–115).

Walji, M. & Stanbrook, M.B. (2015). 'Health professionalism must be ensured online and offline', Canadian Medical Association Journal, 187(8): 547–547.

Warboys, I., Mok, W.Y., & Frith, K.H. (2014). Electronic medical records in clinical teaching. *Nurse Educ Journal*. 39(6): 298-301.

Wendy, M., Kendall, H., & Jason, L. (2015). Advancing social media in medical education. *Canadian Medical Association Journal*, Ottawa, 187(8): 549-550.

Whyte, W., & Hennessy C. (2017). Social Media use within medical education: a systematic review to develop a pilot questionnaire on how social media can be best used at BSMS. *Med Educ Publish*, 6(2): 01-36

Wilcox, & Bhattacharya, M. (2015). Countering Social Engineering through Social Media: An Enterprise Security Perspective. In *Computational Collective Intelligence* (pp. 54–64). Springer International Publishing. https://doi.org/10.1007/978-3-319-24306-1_6

Yasnitsky, A. (2018). Vygotsky: An Intellectual Biography. London and New York: Routledge BOOK PREVIEW

Yeratziotis, Pottas, D., & Van Greunen, D. (2017). A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm. *International Journal of Human-Computer Interaction*, *28*(10), 678–694. https://doi.org/10.1080/10447318.2011.654202

Yigzaw Samuel, T., Jormanainen I., & Tukiainen M., (2018). Information Systems in Developing Countries: Opportunities and Challenges. TEEM'21: Ninth International Conference on Technological Ecosystems for Enhancing Multiculturality (TEEM'21), Pages 812–818 https://doi.org/10.1145/3486011.3486563

Zahidi, Yan Peng Lim, & Woods, P. C. (2014). Understanding the user experience (UX) factors that influence user satisfaction in digital culture heritage online collections for non-expert users. *2014 Science and Information Conference*, 57–63. https://doi.org/10.1109/SAI.2014.6918172

Zamanzadeh V, Ghahramanian A, Rassouli M, Abbaszadeh A, & Alavi, H. (2015). Design and implementation content validity Study: development of an instrument for measuring patient-centered communication. *Journal of Caring Science*; 4(5): 165-178.

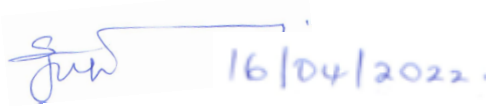
APPENDIX A

TRANSMITTAL LETTER TO RESPONDENTS

Dear Sir/Madam,

I am a postgraduate candidate for the award of Doctor of Philosophy (PhD) in Management Information Systems at Kampala International University, and currently conducting a research study titled; “A Model for adopting a secure Social Media (SM) usage in Medical Institutions in Uganda”: focusing on the training of medical students in Universities. In view of this empirical investigation, I request you to be part of this study by answering my questionnaire. Rest assured that the information you provide shall be kept with utmost confidentiality and will be used for academic purposes only. Please respond to all the items in the questionnaire and do not leave any item unanswered.

Thank you very much in advance,



_____

Mutebi Joe

PhD Candidate

School of Computing and Mathematics,

Kampala International University, Kampala, Uganda.

APPENDIX B

INFORMED CONSENT

I am giving my consent to be part of the research study of Mr Mutebi Joe, who is a PhD candidate at Kampala International University. He is currently conducting a research study titled; “A Model for adopting a secure Social Media (SM) usage in Medical Institutions in Uganda”: focusing on the training of medical students in Universities. I have been assured of privacy, anonymity and confidentiality, and given the option to turndown or withdraw my right of participation anytime. I have also been informed that the research is voluntary and that the results will be given to me if I ask for it.

Initial:_____

Date:_____

APPENDIX C

STUDENT QUESTIONNAIRE

A. INTRODUCTION

Hello, I am a postgraduate student at Kampala International University (KIU). I am conducting a study on Social Media (SM) usage in medical institutions in Uganda, and would like to know your experience of medical information breaches, due to SM usage. The study is intended to develop a model for adopting a secure SM usage in medical institutions in Uganda. This will help medical institutions to ratify and adopt SM usage in their operations. Please, feel free to complete this 15-minutes questionnaire survey. Your responses are confidential and anonymous.

Thank you very much for your honesty, time and effort in responding to this questionnaire.

B. DEMOGRAPHIC DATA

This section asks questions about you. The information is necessary to help in understanding the demographic profiles of Social Media users in medical institutions. The data you share with us will not be used to personally identify you, and will not be passed onto anyone else.

1. Gender
    a) Male
    b) Female
2. Age group
    a) 18 – 25
    b) 26 – 35
    c) 36 – 45
    d) 46 years and above
3. Nationality
    a) Ugandan
    b) International
4. Denomination
    a) Catholic
    b) Protestants
    c) Muslim
    d) Others
5. Medical institution
    a) MUST

b) KIU

6. Year of study
   a) Year 3
   b) Year 4
   c) Year 5
7. Medical Departments
   d) Internal Medicine
   e) Pathology
   f) Anesthesia
   g) Dermatology
   h) Obstetrics and Gynecology
   i) Pediatrics
   j) Psychiatry
   k) Others, specify _____

C. SOCIAL MEDIA USAGE

This section asks questions about Social Media usage. The information is necessary to help in understanding the type and engagement levels of Social Media usage in medical institutions in Uganda. The data you share with us will not be used to personally identify you, and will not be passed onto anyone else.

8. Which Social Media platforms are you subscribed to? (you may tick more than 1)
   a) WhatsApp
   b) YouTube
   c) Twitter
   d) Facebook
   e) Others, specify_____
9. For how long have you been using Social Media in your institution?
   a) Less than a year
   b) 1 – 2 years
   c) 3 – 4 years
   d) 5 – 6 years
   e) More than 6 years
10. How frequently do you use Social Media?
    a) Never use Social Media
    b) Rarely
    c) Sometimes

d) Often

e) Always

11. How many contacts/friends do you have on your Social Media account?

a) Less than 50

b) 51 – 100

c) 101 – 150

d) 151 - 200

e) More than 200

12. Do you normally share or post medical data on Social Media? (during learning, teaching, research or clinical sessions)

a) Yes

b) No

13. Have you ever encountered any form of medical information breaches on Social Media, during clinical session or interaction with your colleagues or supervisors or patients or students?

a) Yes

b) No

14. How frequently do you encounter medical information breaches on Social Media, during clinical session or interaction with your colleagues or supervisors or patients or students?

a) Never

b) Rarely

c) Sometimes

d) Often

e) Always

D. USABLE SECURITY

The following assessment is based on the importance of 10 factors and their respective items in addressing usability-security, communications, training and education aspects of Social Media usage in medical education, with respect to medical information safety.

Please, read each item and indicate your choice by ticking in the box one of the provided options as follows: **1** = Strongly Disagree, **2** = Disagree, **3** = Neutral, **4** = Agree, and **5** = Strongly Agree.

1	**Visibility**: Social Media system should visibly keep users informed about their security status:	**1**	**2**	**3**	**4**	**5**
1.1	Social Media system show the user the progress status during a visible delay in response time					
1.2	Social Media system visibly shows the current selection/data input field					
1.3	Social Media system clearly highlight the problem field with regard to error					

	messages					
1.4	Social Media system give feedback for every security-related action					
1.5	Social Media system visibly show the location of security-related options					
2	**Learnability**: Social Media system should ensure that security actions are easy to learn and remember:	**1**	**2**	**3**	**4**	**5**
2.1	Social Media provide easy-to-learn training material					
2.2	Social Media system have a quick-start guide to assist the user					
2.3	Social Media security options are selected by default					
2.4	Social Media user interface make it obvious which security items are currently selected					
2.5	Social Media system protect users against making severe errors					
3	**Satisfaction**: Social Media system should ensure that users have a good experience when using the system and its security features	**1**	**2**	**3**	**4**	**5**
3.1	The actual process of using Social Media system is fun and enjoyable					
3.2	Most frequently used function keys on Social Media are placed in the most accessible positions					
3.3	Social Media security-related prompts imply that the user is in control					
3.4	Social Media security mechanisms of the system provide a sense of protection to the user					
3.5	Social Media system fulfil its claimed capabilities					
4	**Error handling**: Social Media system should provide users with detailed security error messages that they can understand and act on	**1**	**2**	**3**	**4**	**5**
4.1	Social Media security-related error messages inform the user of the severity of the errors					
4.2	Social Media system warn users if they are about to make a potentially serious error					
4.3	Social Media system allow users to recover from errors quickly and easily					
4.4	Social Media error messages of the system not interfere with the users' work, whenever possible					
4.5	Social Media system clearly ask for users' confirmation of serious and possibly irrevocable actions					
5	**Process revocability**: Social media system should allow users to revoke any of their security actions	**1**	**2**	**3**	**4**	**5**
5.1	Social Media users can easily reverse their security and non-security actions					
5.2	Social Media users can cancel operations in progress					
5.3	Social Media system have 'undo' and 'redo' functions at the level of a single security action or for a complete group of security actions					
5.4	Social Media system provide confirmation for actions that have drastic, possibly destructive consequences					
5.5	Social Media system have a clearly marked exit					
6	**Help and documentation**: Social Media system should make security help apparent and easy to find for users	**1**	**2**	**3**	**4**	**5**
6.1	Social Media help function visible, for example, a key labelled HELP or a special menu					
6.2	Social Media help function cover security and non-security related information					
6.3	Social Media system provide an up-to-date security center, with security training and awareness information					
6.4	Social Media system provide complete and accurate help and a FAQs section					
6.5	Social Media language selection is possible, the translation accurate, without errors					

7	**Security**: Social Media system should provide trusted communication channels between the user and the data Servers	**1**	**2**	**3**	**4**	**5**
7.1	Social Media system initiate a session lock after a period of inactivity or on user request					
7.2	Social Media system enforces a limit on consecutive invalid access attempts by a user during a period of time.					
7.3	Social Media system implement an appropriate time-out logoff period					
7.4	Social Media system encrypt passwords in storage and in transmission					
7.5	Social Media system enforce password restrictions, such as complexity, length, expiry period, reuse, etc.					
8	**Privacy and Confidentiality**: Social Media system should protect user information against unauthorized access by third parties	**1**	**2**	**3**	**4**	**5**
8.1	Social Media system clearly state what personal information is collected and for what purposes it will be used					
8.2	Social Media system require users to confirm statements indicating that they understand the conditions of access					
8.3	Social Media system ask for permission before distributing personal information to third parties					
8.4	Social Media personal information collection and storage mechanisms comply with the data protection regulation of the institution					
8.5	Social Media private or confidential contents are accessed with passwords					
9	**Expressiveness**: Social Media system should guide users on security in a manner that still gives them freedom of expression	**1**	**2**	**3**	**4**	**5**
9.1	Social Media users are initiators of security actions rather than respondents					
9.2	Social Media system correctly anticipate, and prompt for, the user's probable next security-related activity					
9.3	Social Media user can tell the security state of the system and the alternatives for security-related actions if needed					
9.4	Social Media system clearly state its security capabilities					
9.5	Social Media system clearly state the users' responsibilities in terms of security actions					

You can add any other comments below:

_____

_____

_____

Thank you very much for your response, all the information you have provided will be treated with outermost confidentiality and anonymity.

You can reach me on:
0781523424
Mutebi.joe@kiu.ac.ug
WhatsApp No: 0781523424

APPENDIX D

STAFF QUESTIONNAIRE

A. INTRODUCTION

Hello, I am a postgraduate student at Kampala International University (KIU). I am conducting a study on Social Media (SM) usage in medical institutions in Uganda, and would like to know your experience of medical information breaches, due to SM usage. The study is intended to develop a model for adopting a secure SM usage in medical institutions in Uganda. This will help medical institutions to ratify and adopt SM usage in their operations. Please, feel free to complete this 15-minutes questionnaire survey. Your responses are confidential and anonymous.

Thank you very much for your honesty, time and effort in responding to this questionnaire.

B. DEMOGRAPHIC PROFILES

This section asks questions about you. The information is necessary to help in understanding the demographic profiles of Social Media users in medical institutions. The data you share with us will not be used to personally identify you, and will not be passed onto anyone else.

1. Gender
    a) Male
    b) Female
2. Age group
    a) 18 – 25
    b) 26 – 35
    c) 36 – 45
    d) 46 years and above
3. Nationality
    a) Ugandan
    b) International
4. Denomination
    a) Catholic
    b) Protestants
    c) Muslim
    d) Others
5. Medical institution
    a) MUST
    b) KIU
6. Class taught
    a) Year 3
    b) Year 4

c) Year 5

7. Medical Departments
   a) Internal Medicine
   b) Pathology
   c) Anesthesia
   d) Dermatology
   e) Obstetrics and Gynecology
   f) Pediatrics
   g) Psychiatry
   h) Others, specify _____

C. SOCIAL MEDIA USAGE

This section asks questions about Social Media usage. The information is necessary to help in understanding the type and engagement levels of Social Media usage in medical institutions in Uganda. The data you share with us will not be used to personally identify you, and will not be passed onto anyone else.

8. Which Social Media platforms are you subscribed to? (you may tick more than 1)
   a) WhatsApp
   b) YouTube
   c) Twitter
   d) Facebook
   e) Others, specify_____
9. For how long have you been using Social Media in your institution?
   a) Less than a year
   b) 1 – 2 years
   a) 3 – 4 years
   b) 5 – 6 years
   c) More than 6 years
10. How frequently do you use Social Media?
   a) Never use Social Media
   b) Rarely
   c) Sometimes
   d) Often
   e) Always
11. How many contacts/friends do you have on your Social Media account?
   a) Less than 50
   b) 51 – 100
   c) 101 – 150
   d) 151 - 200

e) More than 200

12. Do you normally share or post medical data on Social Media? (during learning, teaching, research or clinical sessions)
    a) Yes
    b) No
13. Have you ever encountered any form of medical information breaches on Social Media, during clinical session or interaction with your colleagues or supervisors or patients or students?
    a) Yes
    b) No
14. How frequently do you encounter medical information breaches on Social Media, during clinical session or interaction with your colleagues or supervisors or patients or students?
    a) Never
    b) Rarely
    c) Sometimes
    d) Often
    e) Always

D. USABLE SECURITY

The following assessment is based on the importance of 10 factors and their respective items in addressing usability-security, communications, training and education aspects of Social Media usage in medical education, with respect to medical information safety.

Please, read each item and indicate your choice by ticking in the box one of the provided options as follows: **1** = Strongly Disagree, **2** = Disagree, **3** = Neutral, **4** = Agree, and **5** = Strongly Agree.

1	**Visibility**: Social Media system should visibly keep users informed about their security status:	**1**	**2**	**3**	**4**	**5**
1.1	Social Media system show the user the progress status during a visible delay in response time					
1.2	Social Media system visibly shows the current selection/data input field					
1.3	Social Media system clearly highlight the problem field with regard to error messages					
1.4	Social Media system give feedback for every security-related action					
1.5	Social Media system visibly show the location of security-related options					
2	**Learnability**: Social Media system should ensure that security actions are easy to learn and remember:	**1**	**2**	**3**	**4**	**5**
2.1	Social Media provide easy-to-learn training material					
2.2	Social Media system have a quick-start guide to assist the user					
2.3	Social Media security options are selected by default					
2.4	Social Media user interface make it obvious which security items are currently selected					
2.5	Social Media system protect users against making severe errors					
3	**Satisfaction**: Social Media system should ensure that users have a good experience when using the system and its security features	**1**	**2**	**3**	**4**	**5**
3.1	The actual process of using Social Media system is fun and enjoyable					

3.2	Most frequently used function keys on Social Media are placed in the most accessible positions					
3.3	Social Media security-related prompts imply that the user is in control					
3.4	Social Media security mechanisms of the system provide a sense of protection to the user					
3.5	Social Media system fulfil its claimed capabilities					
4	**Error handling**: Social Media system should provide users with detailed security error messages that they can understand and act on	**1**	**2**	**3**	**4**	**5**
4.1	Social Media security-related error messages inform the user of the severity of the errors					
4.2	Social Media system warn users if they are about to make a potentially serious error					
4.3	Social Media system allow users to recover from errors quickly and easily					
4.4	Social Media error messages of the system not interfere with the users' work, whenever possible					
4.5	Social Media system clearly ask for users' confirmation of serious and possibly irrevocable actions					
5	**Process revocability**: Social media system should allow users to revoke any of their security actions	**1**	**2**	**3**	**4**	**5**
5.1	Social Media users can easily reverse their security and non-security actions					
5.2	Social Media users can cancel operations in progress					
5.3	Social Media system have 'undo' and 'redo' functions at the level of a single security action or for a complete group of security actions					
5.4	Social Media system provide confirmation for actions that have drastic, possibly destructive consequences					
5.5	Social Media system have a clearly marked exit					
6	**Help and documentation**: Social Media system should make security help apparent and easy to find for users	**1**	**2**	**3**	**4**	**5**
6.1	Social Media help function visible, for example, a key labelled HELP or a special menu					
6.2	Social Media help function cover security and non-security related information					
6.3	Social Media system provide an up-to-date security center, with security training and awareness information					
6.4	Social Media system provide complete and accurate help and a FAQs section					
6.5	Social Media language selection is possible, the translation accurate, without errors					
7	**Security**: Social Media system should provide trusted communication channels between the user and the data Servers	**1**	**2**	**3**	**4**	**5**
7.1	Social Media system initiate a session lock after a period of inactivity or on user request					
7.2	Social Media system enforces a limit on consecutive invalid access attempts by a user during a period of time.					
7.3	Social Media system implement an appropriate time-out logoff period					
7.4	Social Media system encrypt passwords in storage and in transmission					
7.5	Social Media system enforce password restrictions, such as complexity, length, expiry period, reuse, etc.					
8	**Privacy and Confidentiality**: Social Media system should protect user information against unauthorized access by third parties	**1**	**2**	**3**	**4**	**5**
8.1	Social Media system clearly state what personal information is collected and for what purposes it will be used					

8.2	Social Media system require users to confirm statements indicating that they understand the conditions of access					
8.3	Social Media system ask for permission before distributing personal information to third parties					
8.4	Social Media personal information collection and storage mechanisms comply with the data protection regulation of the institution					
8.5	Social Media private or confidential contents are accessed with passwords					
9	**Expressiveness**: Social Media system should guide users on security in a manner that still gives them freedom of expression	**1**	**2**	**3**	**4**	**5**
9.1	Social Media users are initiators of security actions rather than respondents					
9.2	Social Media system correctly anticipate, and prompt for, the user's probable next security-related activity					
9.3	Social Media user can tell the security state of the system and the alternatives for security-related actions if needed					
9.4	Social Media system clearly state its security capabilities					
9.5	Social Media system clearly state the users' responsibilities in terms of security actions					
10	**Medical Information Breaches:** acquiring, accessing, disclosing and sharing of identifiable medical information on SM illegally.	**1**	**2**	**3**	**4**	**5**
10.1	Identifiable medical information are captured on Social Media without informed consent					
10.2	Private medical information are disclosed on Social Media without informed consent					
10.3	Confidential medical information are shared on Social Media against institutional policy					
10.4	Confidential medical information are access on Social Media against institutional policy					

You can add any other comments below:

_____

_____

Thank you very much for your response, all the information you have provided will be treated with outermost confidentiality and anonymity.

You can reach me on:
0781523424
Mutebi.joe@kiu.ac.ug
WhatsApp No: 0781523424

APPENDIX E

INTERVIEW GUIDE FOR INSTITUTION/FACULTY HEADS

	AREA	**INTERVIEW GUIDE FOR INSTITUTION/FACULTY HEADS**
1	Social Media usage	Do you allow Social Media usage in your institution/department? If yes or no, Why?
		Have you ever considered formalizing Social Media usage in your institution/department? If yes or no, why?
		What do you consider to be some of the benefits and risks of formally adopting Social Media usage in your operations?
		What do you think could be some of the solutions to Social Media risks in your area of operations? Manage the risks or avoid Social Media?
		Have you had any Social Media training as an institution/department?
		Do you have any documents or procedures regulating Social Media usage in teaching/learning, or research?
		Do you normally use Social Media in communicating and sharing of medical information to staff and student?
2	Medical privacy and confidentiality	Do your staff and students understand the legal or ethical requirements governing medical privacy and confidentiality in your institution/department?
		Have you ever been a victim of breaches related medical privacy and confidentiality on Social Media? If yes, what do you attribute the breaches to?
		How many breaches have you witnessed in medical privacy and confidentiality, due to Social Media usage in the last one year in your institution?
		How do you often safeguard medical privacy and confidentiality on Social Media?
		Do you believe Social Media usage is important in medical education, irrespective of the associated risks?
3	Any other comment you may need to add	**Thank you very much for your time**

APPENDIX F

VALIDITY ASSESSMENT FORM

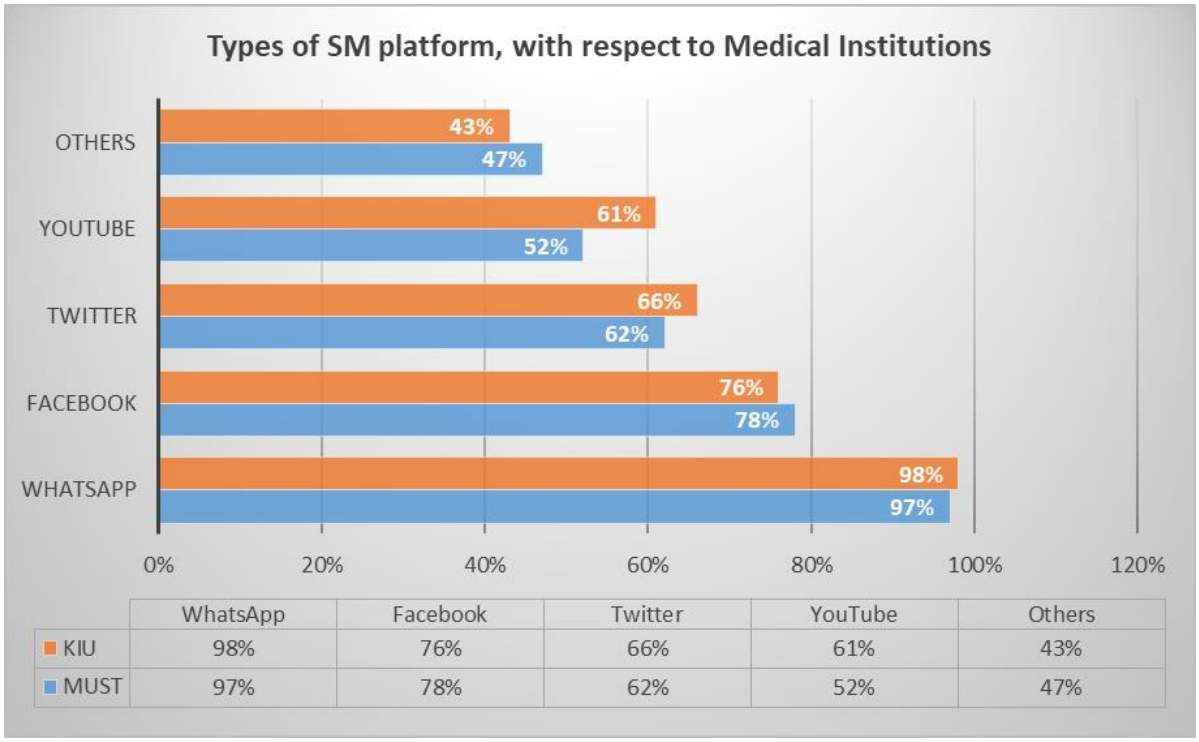
	CONTENT VALIDITY INDEX (**CVI**) ASSESSMENT FORM									COMMENTS
	1 = not relevant/clear, 2 = less relevant/clear, 3 = relevant/clear, 4 = very relevant/clear									
		Your assessment, kindly tick appropriately								
	ITEMS	RELEVANCE				CLARITY				
1	**Visibility**: Social Media system should visibly keep users informed about their security status:	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
1.1	Social Media system show the user the progress status during a visible delay in response time									
1.2	Social Media system visibly shows the current selection/data input field									
1.3	Social Media system clearly highlight the problem field with regard to error messages									
1.4	Social Media system give feedback for every security-related action									
1.5	Social Media system visibly show the location of security-related options									
2	**Learnability**: Social Media system should ensure that security actions are easy to learn and remember:	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
2.1	Social Media provide easy-to-learn training material									
2.2	Social Media system have a quick-start guide to assist the user									
2.3	Social Media security options are selected by default									
2.4	Social Media user interface make it obvious which security items are currently selected									
2.5	Social Media system protect users against making severe errors	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
3	**Satisfaction**: Social Media system should ensure that users have a good experience when using the system and its security features									
3.1	The actual process of using Social Media system is fun and enjoyable									
3.2	Most frequently used function keys on Social Media are placed in the most accessible positions									
3.3	Social Media security-related prompts imply that the user is in control									
3.4	Social Media security mechanisms of the system provide a sense of protection to the user									
3.5	Social Media system fulfil its claimed capabilities									
4	**Error handling**: Social Media system should provide users with detailed security error messages that they can understand and act on	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
4.1	Social Media security-related error messages inform the user of the severity of the errors									
4.2	Social Media system warn users if they are about to make a potentially serious error									
4.3	Social Media system allow users to recover from									

	errors quickly and easily									
4.4	Social Media error messages of the system not interfere with the users' work, whenever possible									
4.5	Social Media system clearly ask for users' confirmation of serious and possibly irrevocable actions	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
5	**Process revocability**: Social media system should allow users to revoke any of their security actions									
5.1	Social Media users can easily reverse their security and non-security actions									
5.2	Social Media users can cancel operations in progress									
5.3	Social Media system have 'undo' and 'redo' functions at the level of a single security action or for a complete group of security actions									
5.4	Social Media system provide confirmation for actions that have drastic, possibly destructive consequences									
5.5	Social Media system have a clearly marked exit									
6	**Help and documentation**: Social Media system should make security help apparent and easy to find for users	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
6.1	Social Media help function visible, for example, a key labelled HELP or a special menu									
6.2	Social Media help function cover security and non-security related information									
6.3	Social Media system provide an up-to-date security center, with security training and awareness information									
6.4	Social Media system provide complete and accurate help and a FAQs section									
6.5	Social Media language selection is possible, the translation accurate, without errors									
7	**Security**: Social Media system should provide trusted communication channels between the user and the data Servers	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
7.1	Social Media system initiate a session lock after a period of inactivity or on user request									
7.2	Social Media system enforces a limit on consecutive invalid access attempts by a user during a period of time.									
7.3	Social Media system implement an appropriate time-out logoff period									
7.4	Social Media system encrypt passwords in storage and in transmission									
7.5	Social Media system enforce password restrictions, such as complexity, length, expiry period, reuse, etc.									
8	**Privacy and Confidentiality**: Social Media system should protect user information against unauthorized access by third parties	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
8.1	Social Media system clearly state what personal information is collected and for what purposes it will be used									
8.2	Social Media system require users to confirm statements indicating that they understand the conditions of access									
8.3	Social Media system ask for permission before distributing personal information to third parties									
8.4	Social Media personal information collection and storage mechanisms comply with the data protection regulation of the institution									

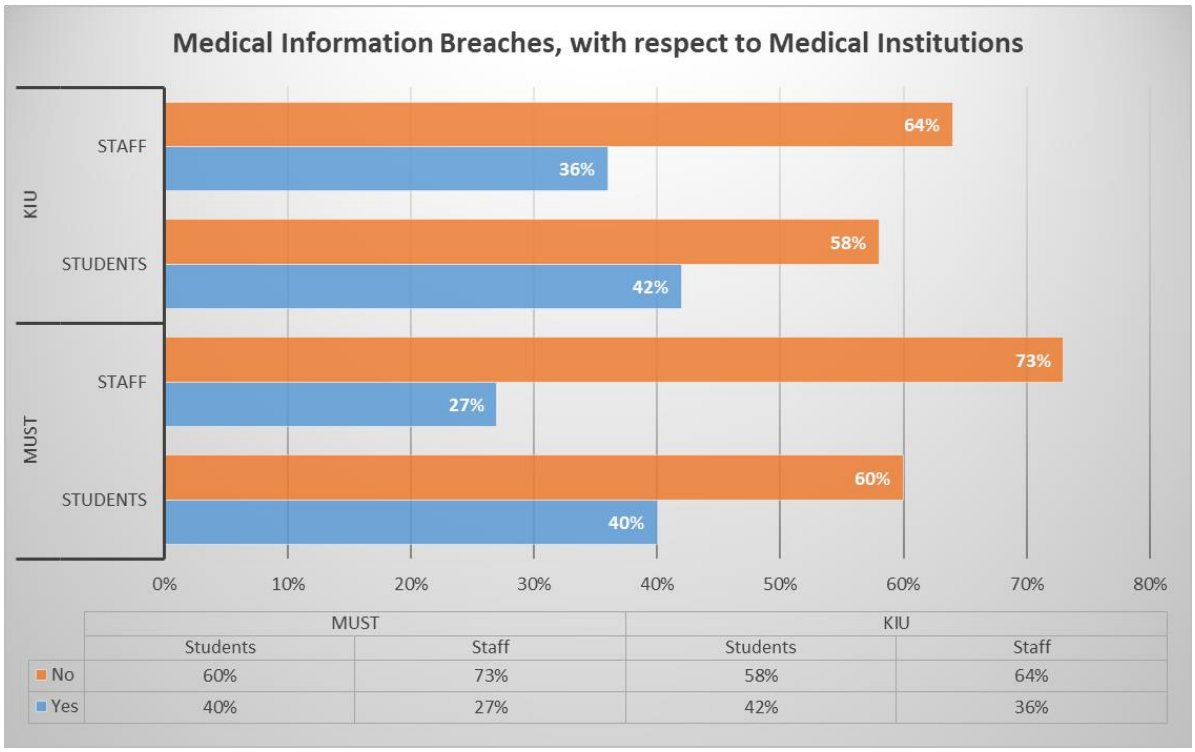
8.5	Social Media private or confidential contents are accessed with passwords									
9	**Expressiveness**: Social Media system should guide users on security in a manner that still gives them freedom of expression	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
9.1	Social Media users are initiators of security actions rather than respondents									
9.2	Social Media system correctly anticipate, and prompt for, the user's probable next security-related activity									
9.3	Social Media user can tell the security state of the system and the alternatives for security-related actions if needed									
9.4	Social Media system clearly state its security capabilities									
9.5	Social Media system clearly state the users' responsibilities in terms of security actions									
10	**Medical Information Breaches:** acquiring, accessing, disclosing and sharing of identifiable medical information on SM illegally.	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
10.1	Identifiable medical information are captured on Social Media without informed consent									
10.2	Private medical information are disclosed on Social Media without informed consent									
10.3	Confidential medical information are shared on Social Media against institutional policy									
10.4	Confidential medical information are access on Social Media against institutional policy									

APPENDIX G

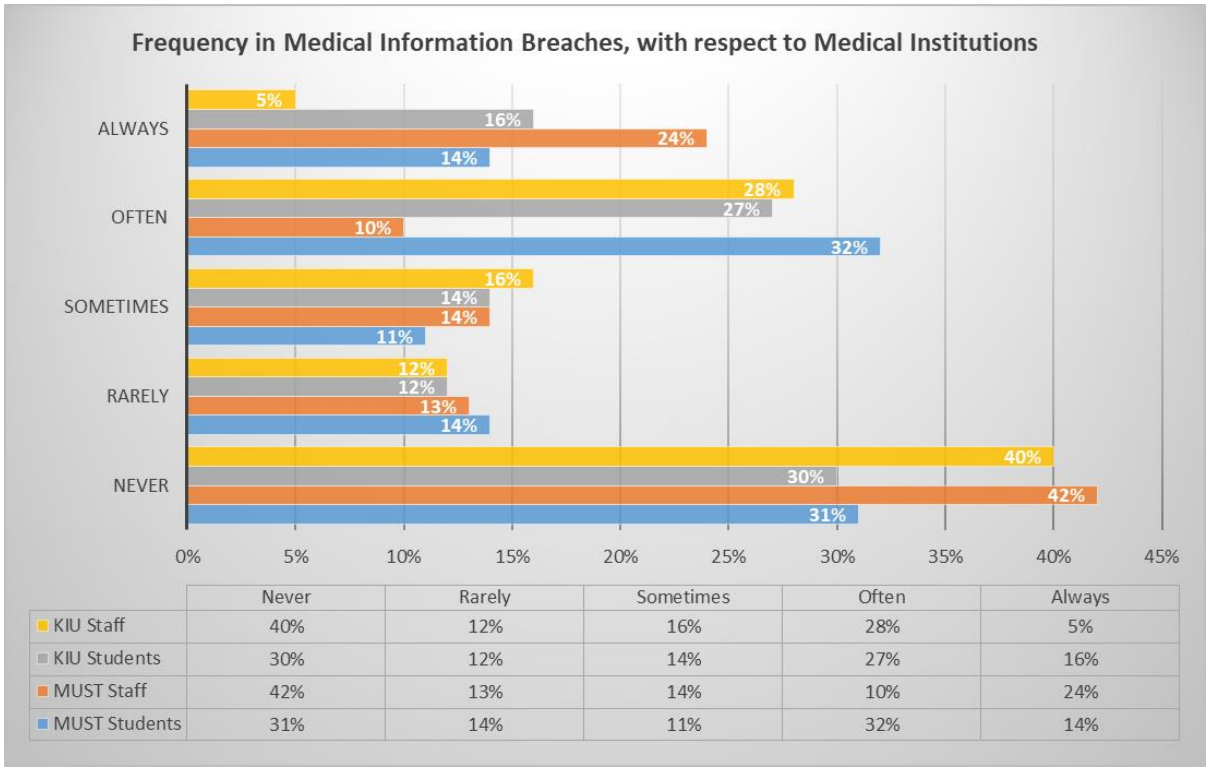
ANALYSIS OUTPUTS AND GLOSSARY



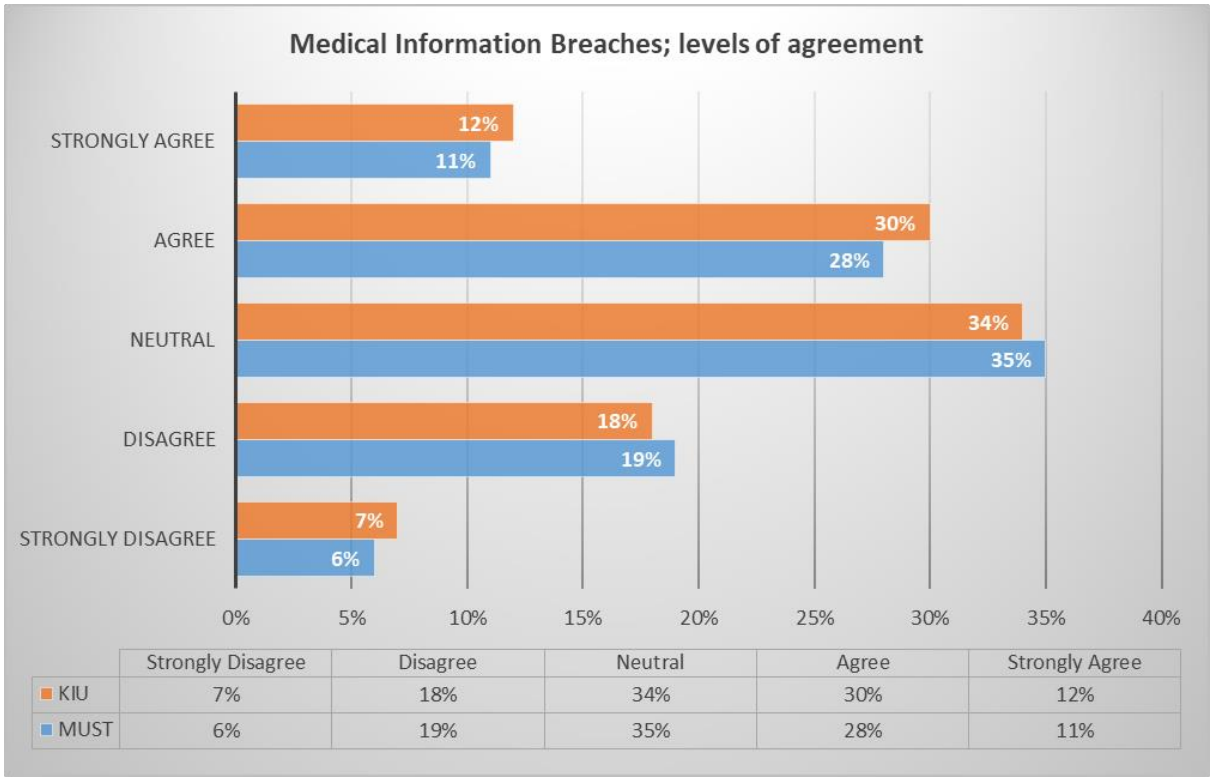
	WhatsApp	Facebook	Twitter	YouTube	Others
KIU	98%	76%	66%	61%	43%
MUST	97%	78%	62%	52%	47%



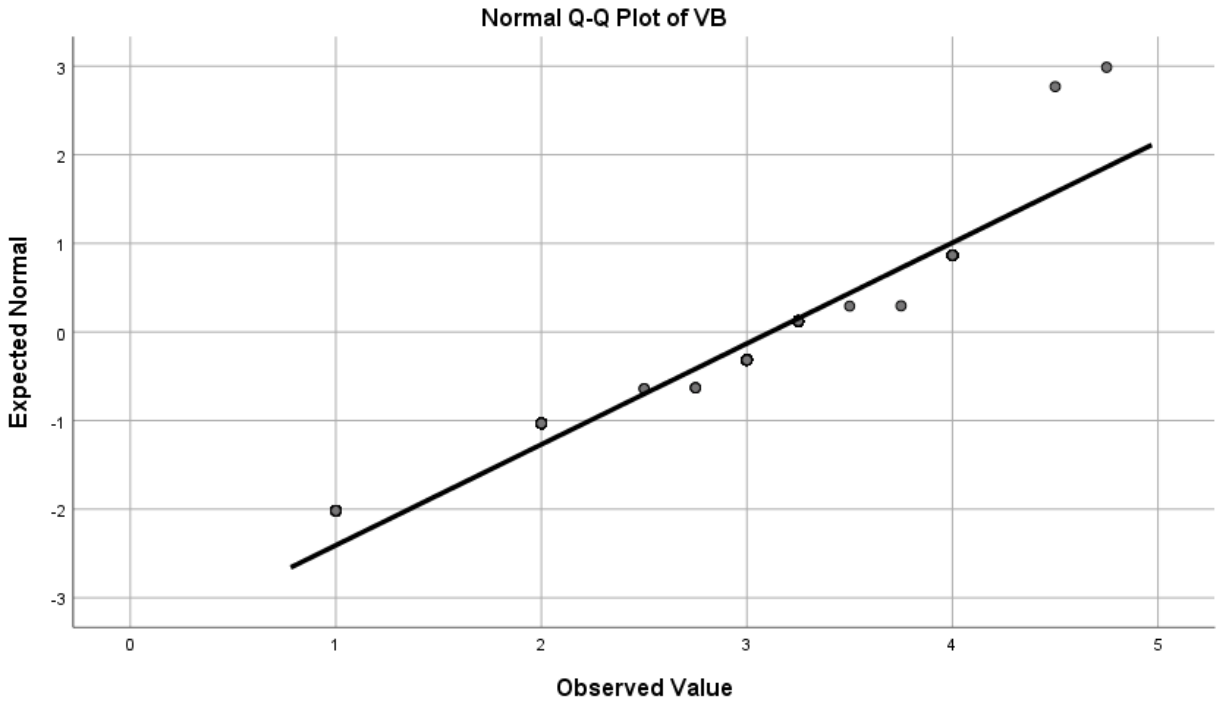
	MUST		KIU	
	Students	Staff	Students	Staff
No	60%	73%	58%	64%
Yes	40%	27%	42%	36%

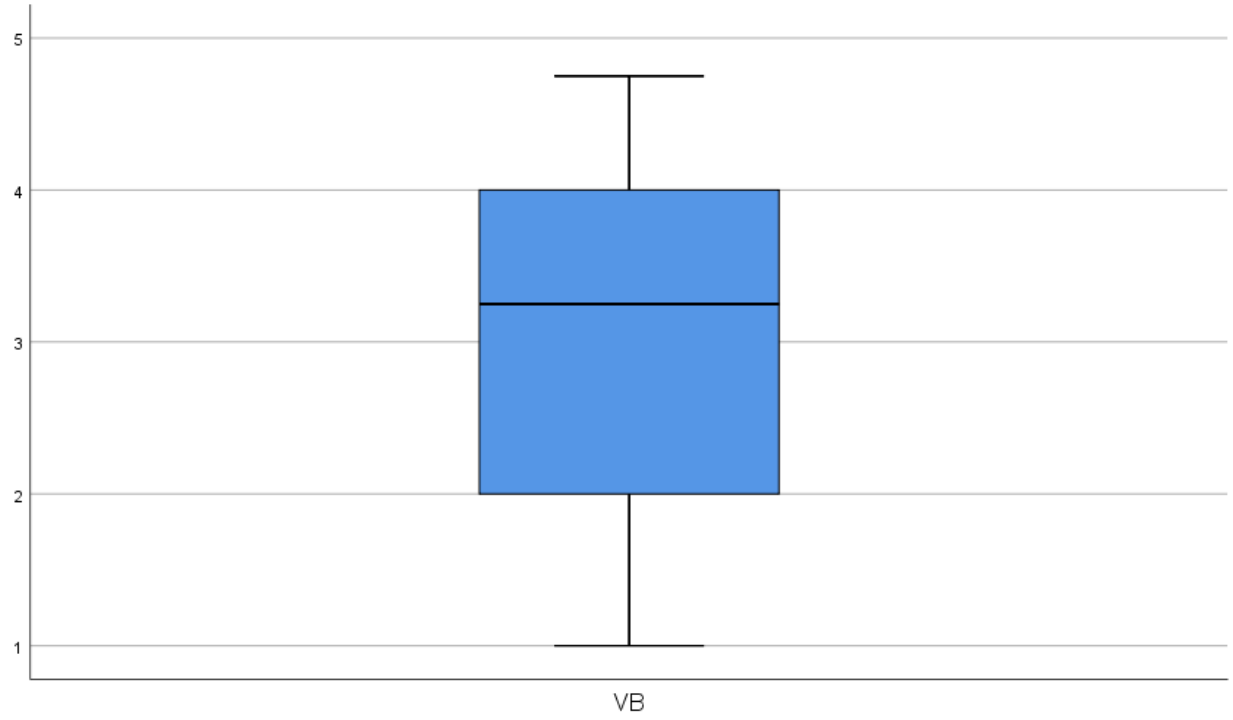


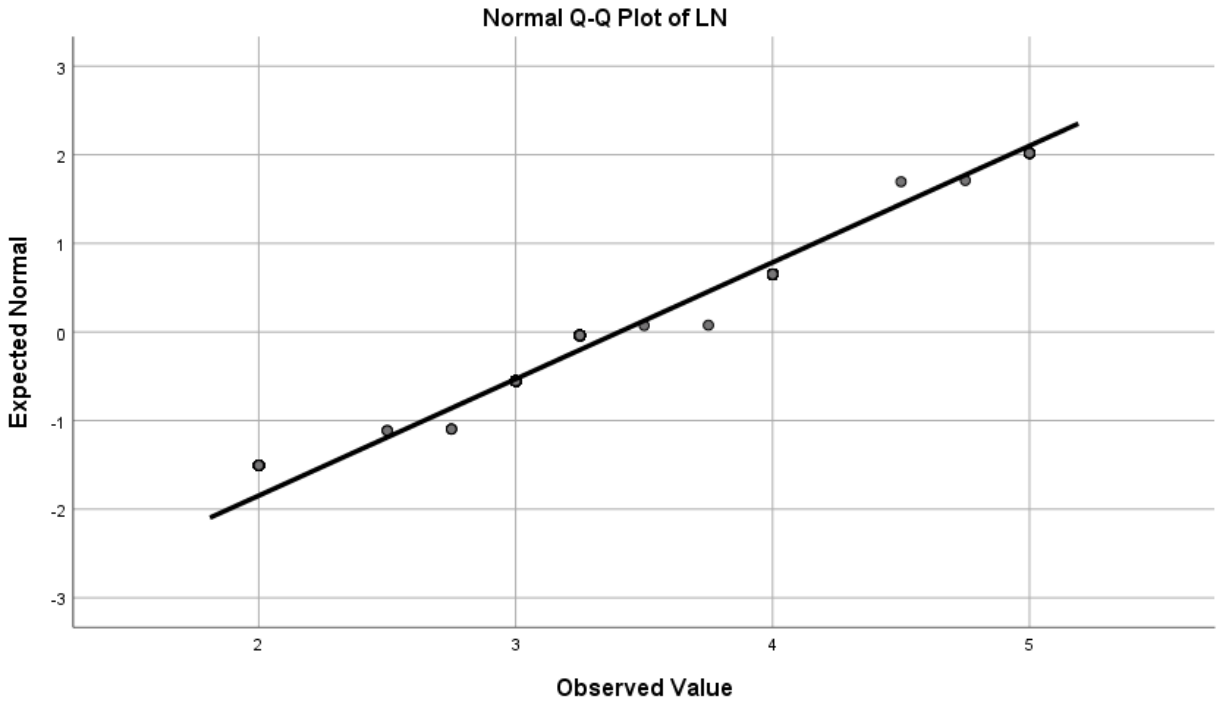
	Never	Rarely	Sometimes	Often	Always
KIU Staff	40%	12%	16%	28%	5%
KIU Students	30%	12%	14%	27%	16%
MUST Staff	42%	13%	14%	10%	24%
MUST Students	31%	14%	11%	32%	14%

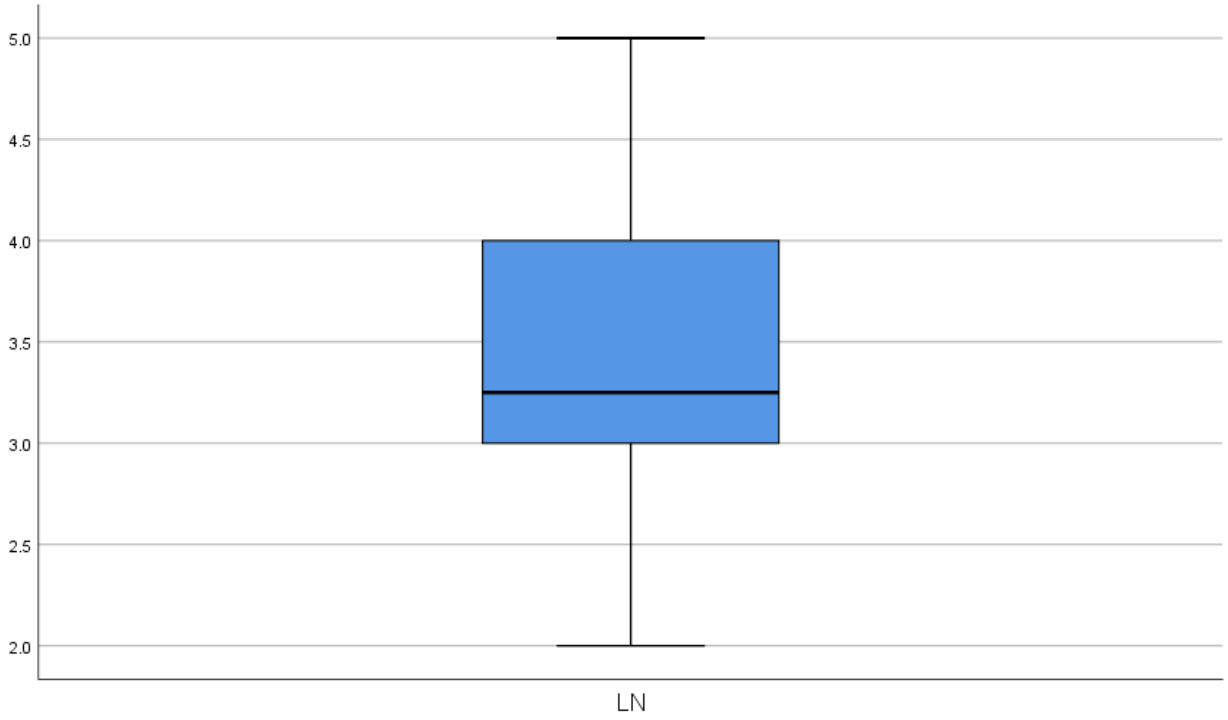


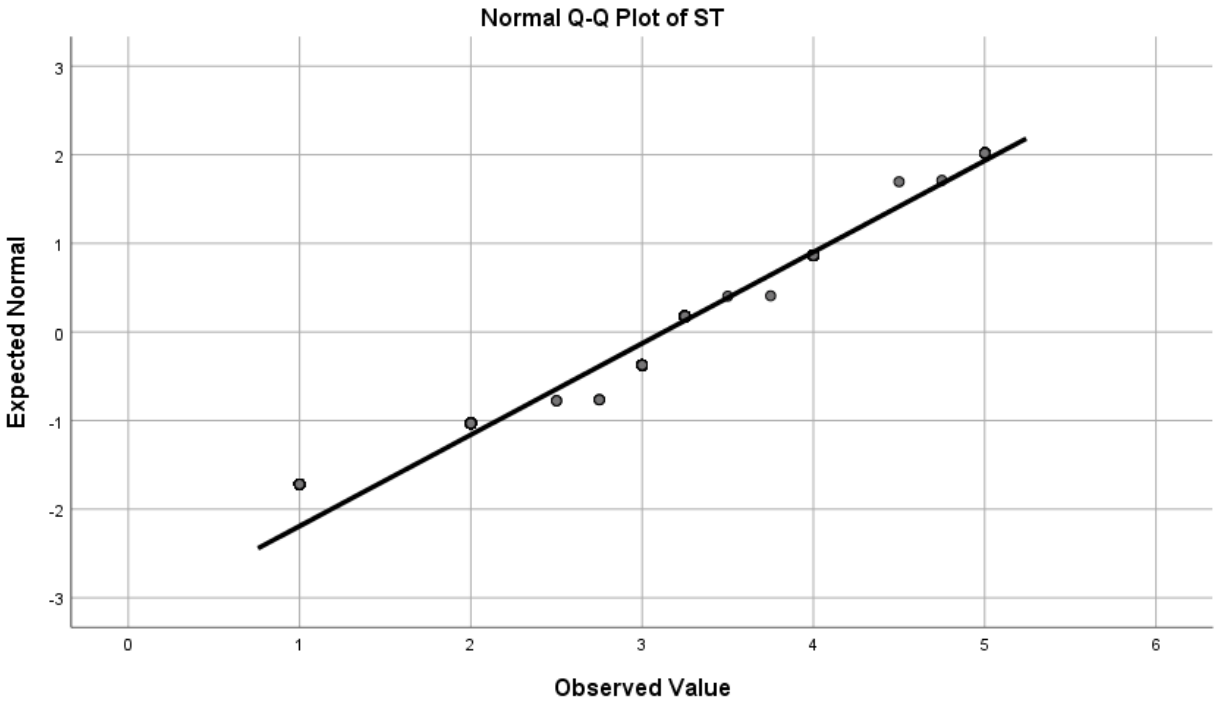
	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
KIU	7%	18%	34%	30%	12%
MUST	6%	19%	35%	28%	11%

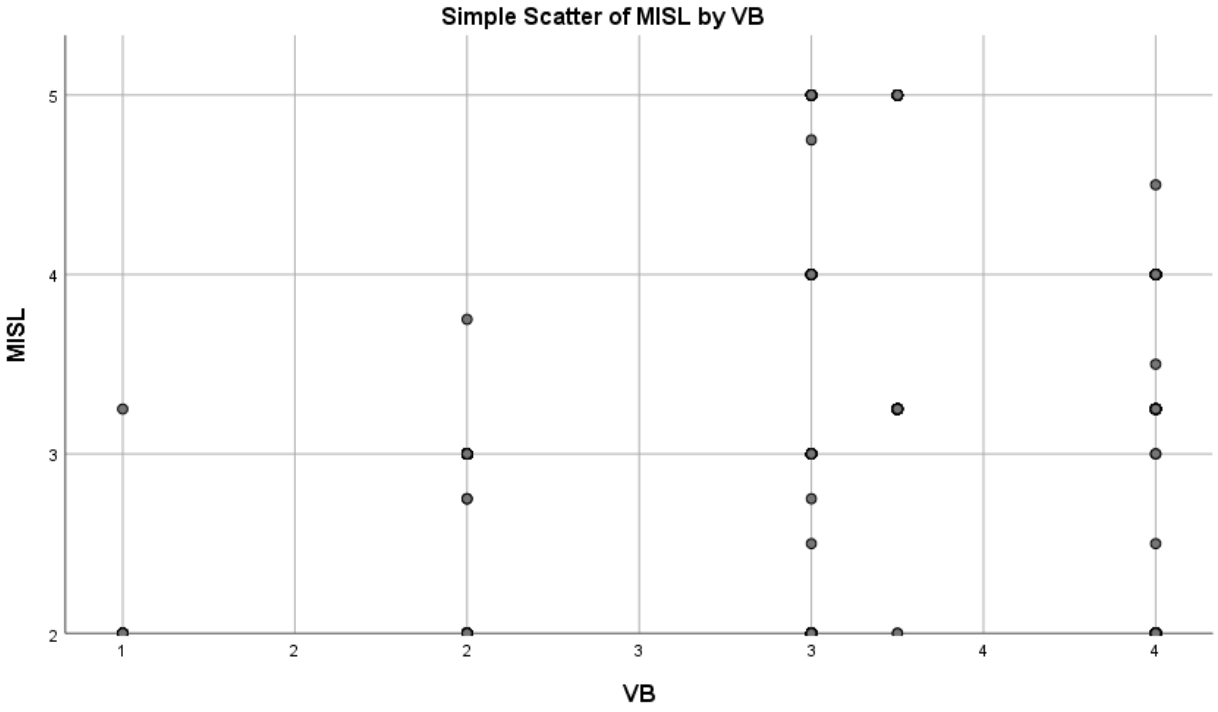

Normal Q-Q Plot of VB
Expected Normal
Observed Value
3
2
1
0
-1
-2
-3
0
1
2
3
4
5

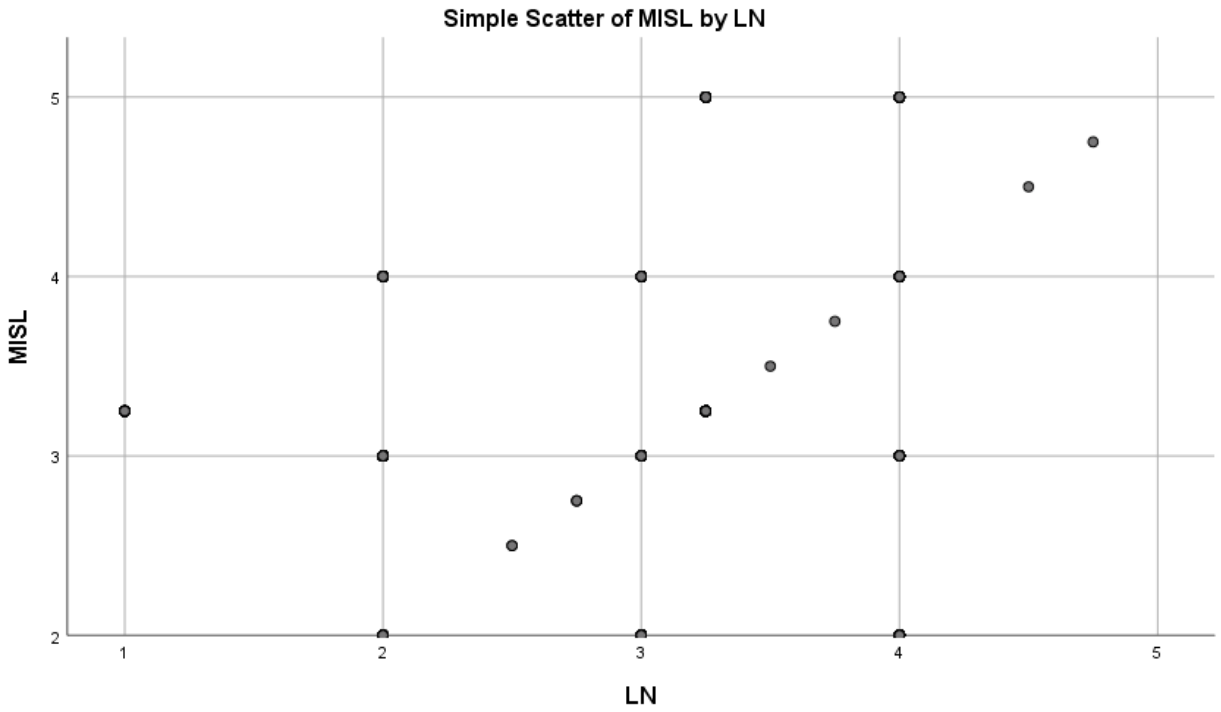

5
4
3
2
1
VB

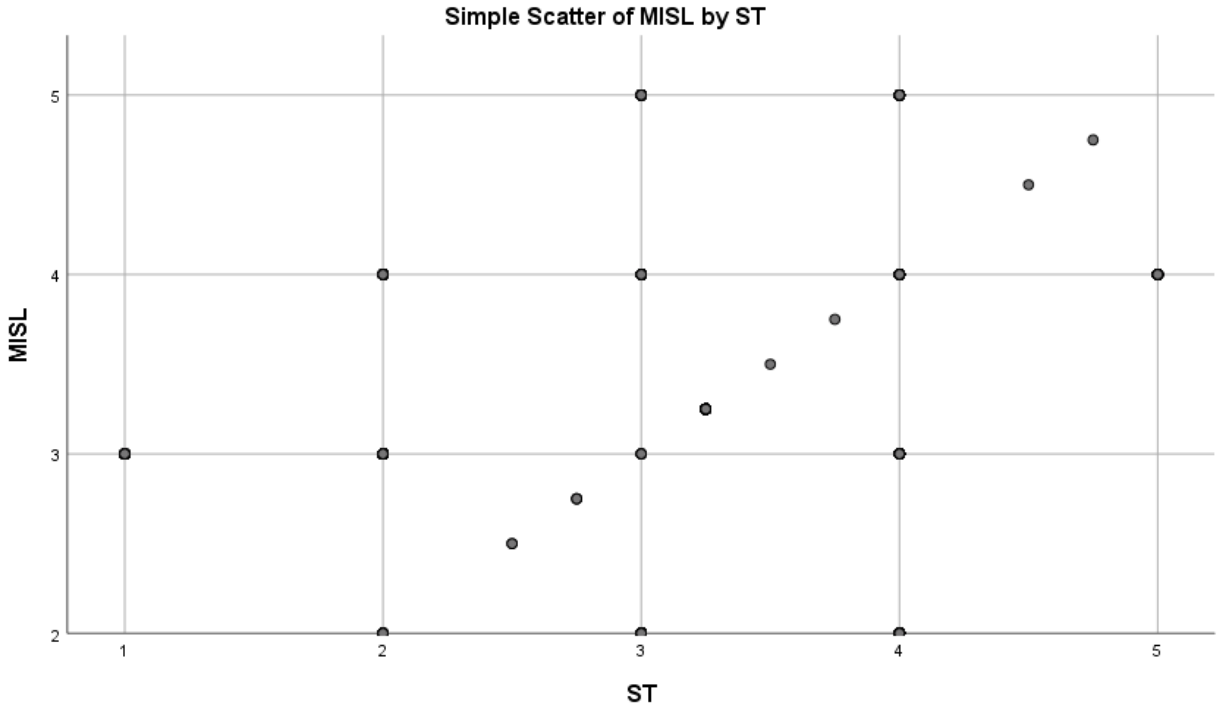

Normal Q-Q Plot of LN
Expected Normal
Observed Value
3
2
1
0
-1
-2
-3
2
3
4
5

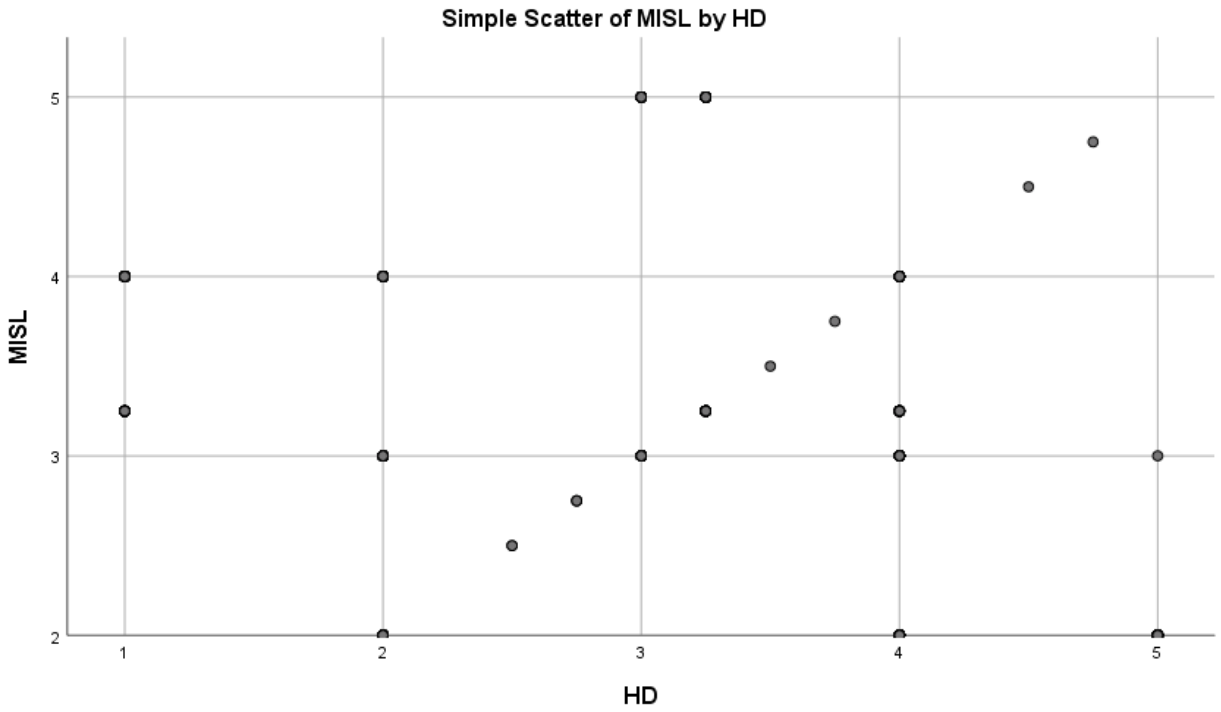

5.0
4.5
4.0
3.5
3.0
2.5
2.0
LN


Normal Q-Q Plot of ST
Expected Normal
Observed Value
3
2
1
0
-1
-2
-3
0
1
2
3
4
5
6


Simple Scatter of MISL by VB
MISL
VB
5
4
3
2
1
2
3
4


Simple Scatter of MISL by LN
MISL
LN
5
4
3
2
1
2
3
4
5


Simple Scatter of MISL by ST
MISL
ST
5
4
3
2
1
2
3
4
5



Correlations

			VB	LN	ST	HD	SC	PR	ER	EX	RV	MISL
Spearman's rho	VB	Correlation Coefficient	1.000	-.211	.316	.203	-.049	.517	.252	-.279	.049	-.580
		Sig. (2-tailed)	.	.000	.000	.000	.189	.000	.000	.000	.193	.000
		N	710	710	710	710	710	710	710	710	710	710
	LN	Correlation Coefficient	-.211	1.000	-.088	.009	.487	.005	-.210	.224	.250	-.620
		Sig. (2-tailed)	.000	.	.019	.801	.000	.897	.000	.000	.000	.015
		N	710	710	710	710	710	710	710	710	710	710
	ST	Correlation Coefficient	.316	-.088	1.000	-.434	.087	.391	-.067	.029	.197	-.750
		Sig. (2-tailed)	.000	.019	.	.000	.021	.000	.076	.433	.000	.000
		N	710	710	710	710	710	710	710	710	710	710
	HD	Correlation Coefficient	.203	.009	-.434	1.000	.023	-.136	-.111	-.228	-.058	-.770
		Sig. (2-tailed)	.000	.801	.000	.	.545	.000	.003	.000	.122	.001
		N	710	710	710	710	710	710	710	710	710	710
	SC	Correlation Coefficient	-.049	.487	.087	.023	1.000	-.068	-.045	.237	.123	-.760
		Sig. (2-tailed)	.189	.000	.021	.545	.	.069	.233	.000	.001	.000
		N	710	710	710	710	710	710	710	710	710	710
	PR	Correlation Coefficient	.517	.005	.391	-.136	-.068	1.000	.077	-.159	.125	-.620
		Sig. (2-tailed)	.000	.897	.000	.000	.069	.	.040	.000	.001	.000
		N	710	710	710	710	710	710	710	710	710	710
	ER	Correlation Coefficient	.252	-.210	-.067	-.111	-.045	.077	1.000	-.113	-.266	.360
		Sig. (2-tailed)	.000	.000	.076	.003	.233	.040	.	.002	.000	.041
		N	710	710	710	710	710	710	710	710	710	710
	EX	Correlation Coefficient	-.279	.224	.029	-.228	.237	-.159	-.113	1.000	.323	.440
		Sig. (2-tailed)	.000	.000	.433	.000	.000	.000	.002	.	.000	.002
		N	710	710	710	710	710	710	710	710	710	710
	RV	Correlation Coefficient	.049	.250	.197	-.058	.123	.125	-.266	.323	1.000	-.420
		Sig. (2-tailed)	.193	.000	.000	.122	.001	.001	.000	.000	.	.000
		N	710	710	710	710	710	710	710	710	710	710
	MISL	Correlation Coefficient	-.580	-.620	-.750	-.770	-.760	-.620	.360	.440	-.420	1.000
		Sig. (2-tailed)	.000	.015	.000	.001	.000	.000	.000	.002	.000	.
		N	710	710	710	710	710	710	710	710	710	710

KAMPALA INTERNATIONAL UNIVERSITY

WSTERN CAMPUS
P. O. Box, 71 Ishaka - Bushenyi
Website https//kiu.ac.ug. Tel: +256 (0) 772684503

Faculty of Clinical Medicine and Dentistry
Office of the Dean

12TH April, 2022

FROM: DEAN, FACULTY OF CLINICAL MEDICINE AND DENTISTRY,
KAMPALA INTERNATIONAL UNIVERSITY – WESTERN CAMPUS

TO: MEDICAL STUDENTS (MBCHB) AND RESPECTIVE MEDICAL STAFFS,
FACULTY OF CLINICAL MEDICINE AND DENTISTRY
KAMPALA INTERNATIONAL UNIVERSITY – WESTERN CAMPUS

SUBJECT: REQUEST TO COLLECT DATA FOR RESEARCH PURPOSE, BY MUTEBI JOE PHD STUDENT

The above mentioned person is a PHD student at the School of Mathematics and Computing (SOMAC), Kampala International University (KIU) Main Campus. He is conducting a study on Social Media (SM) usage in medical institutions in Uganda, and would like to know your experience of medical information safety due to SM usage. The study is intended to develop a model for adopting a secure SM usage in medical institutions in Uganda. This will help medical institutions to ratify and adopt SM usage in their operations. Please, feel free to interact and engage with him on the subject, as your responses are confidential and anonymous.

Thank you,

12 APR 2022

Dr. Okello Maxwell
DEAN, FACULTY CLINICAL MEDICINE AND DENTISTRY
C: DIRECTOR OF HIGHER DEGREE AND RESEARCH
C: SCHOOL OF MATHEMATICS AND COMPUTING