International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
http://ijcjournal.org/

Relative Influence of Social Media Socio-Technical Information Security Factors on Medical Information Breaches in selected Medical Institutions in Uganda

Joe Mutebi[a]*, Margaret Kareyo[b], Victor Turiabe[c], Maxima Ainomugisha[d], Adeyemi Aderonke Latifat[e]

[a,b]*Department of Information Technology, School of Mathematics and Computing, Kampala International University (KIU) – Main Campus, Kampala Uganda*

[c,d,e]*Department of Computing, Faculty of Science and Technology, Kampala International University (KIU) – Western Campus, Ishaka-Bushenyi, Uganda*

[a]*Email: mutebi.joe@kiu.ac.ug,* [b]*Email: kareyo.margaret@kiu.ac.ug,* [c]*Email: victor.turiabe@kiu.ac.ug*

[d]*Email: maxima.ainomugisha@kiu.ac.ug,* [e]*Email: adeyemi.latifat@kiu.ac.ug*

Abstract

This manuscript presents a study based on research conducted to assess the relative impact of social media (SM) socio-technical information security factors on medical information breaches in selected medical institutions in Uganda. The study was motivated by reported cases of medical data breaches through the use of SM. Procedurally, the study used an online survey method using Google forms and a literature search technique. Data were solicited from 566 medical students from Mbarara University of Science and Technology (MUST), and Kampala International University (KIU), accordingly. The key datasets collected included respondent's demographic profile, SM usage characteristics, and medical information breaches. Through literature search, the key SM socio-technical information security factors were identified. Afterwards, Spearman's rank correlational analysis was performed to determine the type of relationships existing between SM socio-technical information security factors and medical information breaches. According to the percentage distribution summary of medical information breaches, the respondent's level of agreement ranges from 39% to 43%. Spearman's rank correlational coefficients indicate significant levels ($p \leq 0.05$) for the key factors identified. However, 6 of the factors presented negative and stronger relationships, while 3 factors yielded weaker correlational relationships. Relatively, the results showed stronger relationships between the social dimensional factors, compared to the technical dimension. The negative relationships imply that medical information breaches on SM would decrease with increase in end-user compliance levels of SM socio-technical information security factors. While the stronger relationship indicate the key SM usage factors associated with medical information breaches. Overall, the study outcome would provide theoretical and empirical basis for medical institutions, SM researchers, and practitioners to rationalize and leverage SM usage in their operations.

---

* Corresponding author.

Keywords: Social Media usage; Socio-technical; Usable-security; Social dimension; Technical dimension.

1. Introduction

In Uganda, over 80% of healthcare services in hospital sites are provided by medical interns [1,2]. Over 90% of medical students and staff in medical institutions are using SM in their operations [3,4,5]. Medical (MBChB) students often engage with their colleagues and supervisors online by sharing clinical contents and knowledge, and could easily receive feedback on urgent matters related to their training and operations [4,6,5]. However, medical institutions are still conservative in fully ratifying and adopting SM usage in their operations [7,9,6]. This caution is usually attributed to the risks and profound needs of preserving medical information safety among medical students, and medical staff including supervisor [10,11,6]. Recently, numerous studies have reported on the challenge of medical information breaches due to SM usage [7,1,10,5]. For instance, according to Alunyu et al. [1] study of electronic healthcare data management, 22% to 31% of respondents reported IT related breaches in medical data in healthcare sites in Uganda. However, the key factors associated with those breaches are often scantly defined [12,10,6]. Hence, this study was intended to fill the gap by assessing the relative influence of Social Media (SM) socio-technical information security factors associated with medical information breaches in selected medical institutions in Uganda, [12,13].

From existing studies, the major challenge hindering the ratification of SM usage in medical institutions could be linked to the profound needs of preserving medical information safety [8,11,6] According to Pander et al., [14], an analysis study of related literatures, 0.02% to 16% of medical students who were using SM got involved in unethical behaviors including medical information breaches. In Uganda, Kaddu & Mukasa [5] study of SM usage in higher education indicates that 29% to 38% of students got involved in unethical behaviors, including violation of medical privacy and confidentiality, [1,4,5]. Recently, Alunyu et al. [1] study of electronic healthcare data management indicated that 22% to 31% of respondents reported IT related breaches in medical data in healthcare sites in Uganda [1]. Among the global IT related breaches reported in 2018, SM incidents accounted for more than 56% of 4.5 billion information records compromised globally [15,16,17]. Institutionally, the consequences of medical information breaches include; loss of trust and reputation, legal suit, financial harm, etc. [18,19,6]. According to Liaw & Hannan [20], 49.1% of patients in Australia confirmed withholding information from clinicians based on privacy and confidentiality concerns [21]. While in the healthcare industry, the global estimated cost of electronic data breaches in 2019 amounted to $6.45 million [15,17].

Nevertheless, in the context of SM usage and medical information breaches, little is known about the key SM socio-technical information security factors associated with medical information breaches in medical institutions in Uganda [10,6,22]. Contrarily, existing studies often focus on information security attributes associated with mainly the technical aspect of SM usage [4,10,6,14]. And yet, numerous studies have reported social engineering (behavioral) attacks as one of the prevalent forms of online information security breaches [23,22]. Therefore, this study envisages the components of SM socio-technical information security factors into social and technical dimensions, accordingly [7, 24 , 13, 22].Whereby, the social dimension comprises of; 1) usability factors – *visibility, learnability,* and *satisfaction*, 2) education and training factors – *help* and *documentation* [7,

25, 26, 27]. On the other hand, the key factors identified under technical dimensions include; 3) SM technology development factors – *error handling*, and *process revocability*; 4) information security factors – *security, privacy* and *expressiveness*, [23,25,27]. In this case, SM socio-technical information security factors are attributes of SM usage that embraces information security requirements ranging from hardware, software, personal, and organizational structures [12, 23]. While the act of medical information breaches entails illegal acquisition, usage, and disclosure of electronic medical information with respect to SM usage [16,15].

Notably, from the technical dimension perspective, various SM platforms are enhanced with customizable security features to support SM users in managing information security requirements[7, 2, 13]. For instance, Facebook and Twitter use two-factor verification principles; passwords, as well as verification codes established using mobile devices. This authentication process helps to diminish the risk of compromising user accounts and could avert attackers from appropriating an authentic account [28]. Furthermore, Facebook users can adjust security configurations and select users who can view their contents and sensitive information. It can also authorize users to allow or deny accessibility to a third party to their private contents. On the other hand, WhatsApp communications channel is end-to-end encrypted between two parties. Other additional technical security configurations include; firewall setting, anti-virus protection, anti-spam filter, VPN settings, intrusion detection, etc. [7,13]. This therefore, could imply that much of the reported risks and breaches associated with SM usage could emanate from the social (behavioral) aspects of SM usage, such as lack of knowledge, education and training, and effective security policy, [29, 24, 22, 13]. Since the technical aspects are enhanced with capabilities to manage and mitigate some of the dominant information security risks associated with SM usage [28]. Therefore, this study was intended to fill this gap by assessing the relative influence of SM socio-technical information security factors on medical information breaches in selected medical institutions in Uganda. Overall, the research output would add knowledge by identifying the vulnerable information security features associated with SM usage, which would provide an empirical basis for medical institutions, as well as SM researchers and practitioners to rationalize and leverage SM usage in their operations.

1.1 Objectives

The main objective of this study was to assess the relative influence of SM socio-technical information security factors on medical information breaches in selected medical institutions in Uganda. Precisely, the study focused on the following specific objectives:

1) To identify Social Media (SM) socio-technical information security factors, in line with usable-security principles.
2) To establish the prevalence of medical information breaches due to SM usage in selected medical institutions in Uganda.
3) To examine the type of correlational relationships existing between SM socio-technical information security factors, and medical information breaches.

2. Methodology

In congruent with the study objectives, the study followed literature search techniques using mainly web of science databases. The strategies used in the literature search included Boolean keyword search and citation guides. Subsequently, relevant literatures were identified in line with the study objectives, and relevant SM socio-technical information security factors were identified and scrutinized. Afterwards, an online questionnaire was developed, and data was solicited from 566 medical students from Mbarara University of Science and Technology (MUST), and Kampala International University (KIU), accordingly. The key datasets collected included respondent's demographic profile, SM usage characteristics, and medical information breaches. The datasets were then processed and subjected to analysis using SPSS software. The analysis results generated include a reliability test – Cronbach's alpha coefficient (α-values), a normality test to determine the appropriate choice of correlational analysis tools, which eventually led to nonparametric analysis option – Spearman's rank correlation analysis, accordingly.

3. Analysis and presentation of results

Section 3 covers data analysis and presentation of results. In line with specific objectives, the results are presented in a narrative, tabular and chart formats accordingly. The key datasets used in the analysis process include; respondent's demographic profiles, SM usage characteristics, and medical information breaches. Therefore, at the beginning of the section, the presentation commenced with literature search results and demographic profile of respondents. Then later followed by reliability test, normality test, and Spearman's rank correlation analysis, accordingly.

3.1. Literature search results

The main sets of Boolean keywords used to initiate the search process include; "Social Media usage AND information security"; "socio-technical"; and "usable-security", accordingly. The other search criteria used to filter and streamline the results further included; sort by relevance (keywords), availability of source (peer reviewed journals), resource type (journal articles), subject area (keywords), literature date range (2012 to 2022), and language used (English). At the onset of the literature search process, 170 literatures were retrieved. However, after applying the other search criteria, the results were reduced to 99 literatures. Afterwards, 99 literatures were scrutinized using citation guides and 13 literatures were found to be relevant to the study. With respect to "socio-technical" keywords, 4 out of 15 literatures were found relevant, and for "usable-security" keywords, 3 out of 14 literatures were found relevant. However, after applying search criteria using a combination of Boolean keywords; "Social Media usage AND socio-technical factors", in line with the study gap, only 1 literature was retrieved [12].

Eventually, the key factors identified from the relevant literatures included; 1) SM usage and information security factors (**SMISF**) – *education* and *training, error handling, information security, user monitoring, software update, authentication mechanism, report users, visibility, increased awareness, legal factors, technical factors, user satisfaction, effective policy, user motivation, user trust,* and *computer knowledge,* [7, 30,

2, 31, 8, 32, 729, 33, 34, 24, 13, 22, 35] 2) Socio-technical information security factors (**STF**) – social dimensions: *visibility*, *learnability*, *satisfaction*, *help* and *documentation*, *user language*, *user suitability*, and *legal factors;* technical dimensions: *error handling*, *process revocability*, *availability*, *security*, *privacy* and *confidentiality*, *authentications*, *expressiveness*, and *information security*, [7, 12, 23, 36]. 3) Usable-security factors (**USF**) – security factors: *confidentiality*, *availability*, *accessibility*, *accountability*, and *none-repudiation*, usability factors: *effectiveness*, *efficiency*, *satisfaction* and *error protection*, *visibility*, *learnability*, *user satisfaction*, *help* and *documentation*, *user language*, *user suitability*, *error handling*, *clarity*, *revocability*, *availability*, *security*, *integrity*, *privacy* and *confidentiality*, *expressiveness*, *help and documentation*, and *learning*, [7, 37, 8, 23, 25, 27].

Overall, the common factors featuring in the 3 main sets of relevant literatures (**SMISF, STF,** and **USF**) were considered appropriate and relevant for inclusion into the list of key SM socio-technical information security factors [7, 12, 23]. In this case, the common factors identified under the social dimension include; 1) usability factors – *visibility*, *learnability*, and *user satisfaction*, 2) education and training factors – *help* and *documentation* [25, 26, 27]. On the other hand, the common factors identified under technical dimensions include; 3) technology development factors – *error handling*, and *process revocability*; 4) information security factors – *security*, *privacy* and *confidentiality*, and *expressiveness* [23, 25, 27]. According to Wilcox & Bhattacharya [13], the dominant information security challenges associated with SM usage include; privacy and confidentiality, litigation, and information overload. Altogether, the key factors would be the common factors of the set elements represented by the intersection of the 3 sets (**SMISF** ∩ **STF** ∩ **USF**) [7, 23]. Figure 1 present a venn-diagram indicating the common factors of the set elements, accordingly [7].

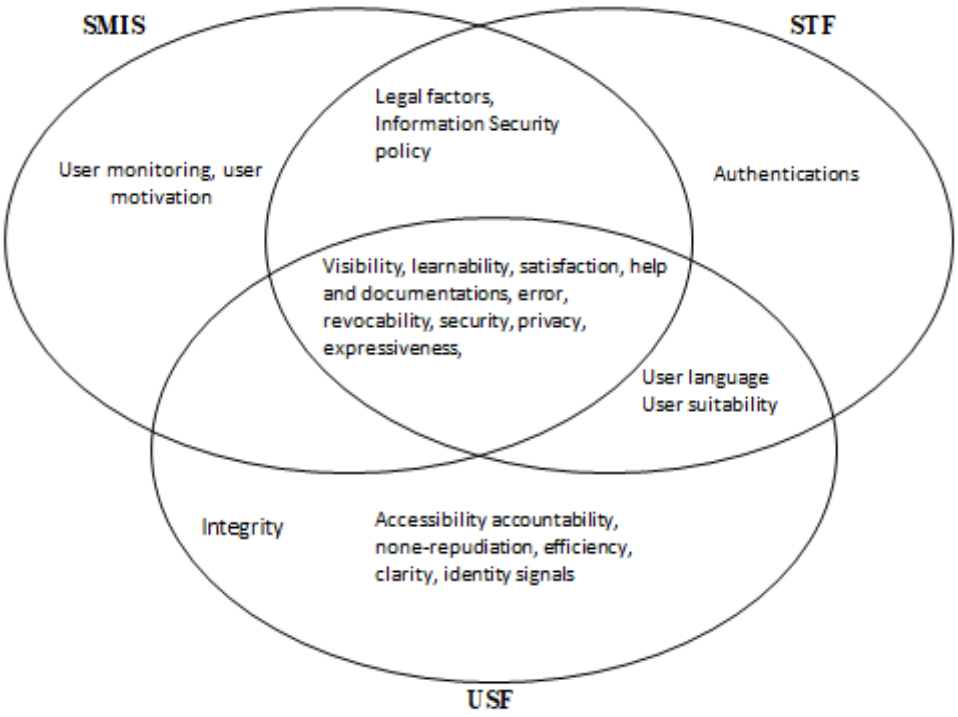

Figure 1: SM socio-technical information security factors: [7].

3.2. Data evaluation

After identifying the relevant SM socio-technical information security factors, questionnaire items were then developed based on the key factors (*Visibility, learnability, user satisfaction, help and documentation, error, revocability, security, privacy, expressiveness*). However, much of the questionnaire items were adopted from validated information security principles developed by Mujinga, Eloff & Kroeze, [23], and Mutebi et al., [7], but revised to suit the study theme and objectives. Each questionnaire item was constructed with 5-point Likert scale measure, with responses ranging from "1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree". To avoid misinterpretation of the results, the items were revised to conform to positively worded questions [38]. Thus, factors with "agree" and "strongly agree" would therefore mean better information security compliance, while low agreement levels such as "disagree" and "strongly disagree" would mean vulnerable or weak information security compliance. While questionnaire items for medical information breaches were developed based on the guidelines that stipulate the act of medical information breach with respect to SM usage [16,15]. Table 1 present the final questionnaire items covering respondents demographic profiles, SM usage characteristics, and medical information breaches, respectively, [7,23,39].

Table 1: Questionnaire, SM socio-technical information security factors.

Gender_____ Age group_____ Academic department_____

	1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree					
1	**Visibility**: Social Media systems should visibly keep users informed about their security status:	1	2	3	4	5
1.1	Social Media systems shows the user 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 systems clearly highlights the problem field regarding 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 provides easy-to-learn training material					
2.2	Social Media system has 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	**User 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 systems 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 error					
4.2	Social Media systems warn users if they are about to make a potentially serious error					
4.3	Social Media systems allows 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 systems 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 systems has '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 systems 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 systems provides 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 initiates 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 systems implements an appropriate time-out logoff period					
7.4	Social Media systems encrypts passwords in storage and in transmission					
7.6	Social Media systems enforce password restrictions, such as complexity, length, expiry period, reuse, etc.					
8	**Privacy and Confidentiality**: Social Media systems should protect user information against unauthorized access by third parties	1	2	3	4	5
8.1	Social Media systems clearly state what personal information is collected and for what purposes it will be used					
8.2	Social Media systems requires users to confirm statements indicating that they understand the conditions of access					
8.3	Social Media systems 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 systems 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 systems 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 accessed on Social Media against institutional policy					

3.3. Demographic profile – respondents

The respondents used in this study were 566 medical students from Mbarara University of Science and Technology (MUST), and Kampala International University (KIU), accordingly. The study preferred medical institutions of learning because of profound needs of preserving medical information safety, [16]. Additionally, SM usage are more prevalent in higher education than the other formal settings in Uganda, [2,4]. Table 2 summarizes and presents the demographic profiles of the respondents, showing the representativeness of the sample characteristics within the category divides. Thus, indicating the frequency counts, and the corresponding percentage distributions, respectively.

Table 2: Respondent demographic profiles.

	MEDICAL INSTITUTIONS	MUST		KIU	
	Demographic profile	Medical students		Medical students	
1	Gender	*n = 260*	*(100%)*	*n = 306*	*(100%)*
	Male	151	58%	171	56%
	Female	109	42%	135	44%
2	Age group				
	18 – 25	195	75%	197	64%
	26 – 35	049	19%	085	28%
	36 – 45	011	04%	014	05%
	46 years and above	005	02%	010	03%
3	Academic department				
	Internal medicine	029	11%	037	12%
	Pathology	026	10%	037	12%
	Anesthesia	037	14%	036	12%
	Dermatology	042	16%	036	12%
	Obstetrics and gyn	030	12%	041	13%
	Pediatrics	033	13%	039	13%
	Psychiatry	030	12%	041	13%
	Others	033	13%	039	13%

Altogether, 566 respondents were given questionnaire to complete. Afterwards, the completed questionnaires were collected, processed, and the datasets were captured into SPSS for analysis.

Table 3 summarizes and presents the results for the key SM sociotechnical information security factors, indicating the average percentage level of agreement on each key factor, accordingly. (MUST n = 260, KIU n = 306).

Table 3: SM socio-technical factors, agreement levels (compliance).

MBARARA UNIVERSITY OF SCIENCE AND TECHNOLOGY – MUST (n = 260)						
Factors	Strongly disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly agree (%)	Total (%)
Usability factors					average 33%	
Visibility	09%	22%	40%	19%	10%	100%
Learnability	08%	21%	41%	24%	06%	100%
User satisfaction	06%	16%	39%	29%	10%	100%
System development factors					average 38%	
Error handling	04%	18%	40%	25%	13%	100%
Revocability	07%	16%	40%	26%	11%	100%
Education and training factors					average 30%	
Help and documentation	10%	21%	39%	20%	10%	100%
Information security factors					average 39%	
Security	07%	17%	38%	25%	13%	100%
Privacy/confidentiality	06%	14%	40%	27%	13%	100%
Expressiveness	06%	16%	39%	27%	12%	100%
Medical Information Breaches	06%	18%	34%	28%	11%	100%
KAMPALA INTERNATIONAL UNIVERSITY – KIU (n = 306)						
Usability factors					average 33%	
Visibility	11%	21%	39%	18%	11%	100%
Learnability	09%	18%	40%	23%	10%	100%
User satisfaction	07%	17%	38%	28%	10%	100%
System development factors					average 39%	
Error handling	05%	16%	40%	26%	13%	100%
Revocability	06%	17%	38%	29%	10%	100%
Education and training factors					average 29%	
Help and documentation	10%	21%	40%	17%	12%	100%
Information security factors					average 39%	
Security	06%	16%	39%	28%	11%	100%
Privacy/confidentiality	06%	18%	36%	27%	13%	100%
Expressiveness	07%	18%	38%	25%	12%	100%
Medical Information Breaches	07%	18%	33%	31%	12%	100%

According to Table 3 above, the percentage agreement score for each higher level factor was derived from their respective groups of items. In this case, the scores include; *visibility* (MUST 29%; KIU 29%), *learnability* (MUST 30%; KIU 33%), *user satisfaction* (MUST 39%; KIU 38%), *error handling* (MUST 38%; KIU 39%), *revocability* (MUST 37%; KIU 39%), *help* and *documentations* (MUST 30%; KIU 29%), *security* (MUST 38%; KIU 39%), *privacy* (MUST 40%; KIU 40%), *expressiveness* (MUST 39%; KIU 37%). However, the percentage scores for the dimensions were derived from their respective groups of factors; 1) social dimension – usability factors (MUST 33%; KIU 33%), and education and training factors (MUST 30%; KIU 29%). 2) Technical dimension – system development factors (MUST 38%; KIU 39%), and information security factors (MUST

39%; KIU 39%). Notably, the average percentage compliance score is 31% for social dimension, and 39% for technical dimension. Hence, implying end-user are more compliant with technical dimension than social dimension. With respect to medical information breaches, the respondent's level of agreement ranges from: MUST 39% to KIU 43%, accordingly.

3.4. Factor validation

Afterwards, a reliability test was conducted on 49 Likert scale items, involving 9 SM socio-technical information security factors, and 1 medical information breaches factor. Each item was developed with 5-point Likert scales, with measures ranging from "1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree" (40,39). Subsequently, Cronbach's alpha (α) values were then generated to reveal the consistency of the responses within the dataset. Items with Cronbach's Alpha value ($\alpha \geq 0.70$) were considered strong reliability items, while those with Cronbach's Alpha value 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, (41,40,39). Table 4 presents the summary of the reliability test results for the items under each factor, indicating the Cronbach's alpha (α) values for each factor, and the conclusion thereof.

Table 4: 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	5	5	0 revised	0.874	Acceptable
Learnability	5	5	0 revised	0.808	Acceptable
Satisfaction	5	5	0 revised	0.959	Acceptable
Error handling	5	4	1 revised	0.772	Acceptable
Revocability	5	3	2 revised	0.632	Acceptable
Help and documentation	5	4	1 revised	0.707	Acceptable
Security	5	5	0 revised	0.821	Acceptable
Privacy/confidentiality	5	5	0 revised	0.902	Acceptable
Expressiveness	5	4	1 revised	0.788	Acceptable
Medical information breaches	4	3	1 revised	0.820	Acceptable

According to Table 4 above, all 10 factors attained the acceptable level of reliability results. However, the reliability result for the *revocability* factor did not meet the minimum value range of $0.70 \leq \alpha \leq 0.90$. Altogether, the validated and maintained factors under social dimension include; 1) usability factors – *visibility*, *learnability*, and *satisfaction*, 2) education and training factors – *help* and *documentation*. Meanwhile, the factors identified under technical dimensions include; 3) SM technology development factors – *error handling*, and *process revocability*; 4) information security factors – *security*, *privacy* and *expressiveness* [7,23,25,27].

3.5. Normality test

Before selecting appropriate statistical analysis tools, a normality test was conducted to check the normality distribution within the dataset. According to Joshi et al. [39], if the datasets are normally distributed, then the appropriate analysis option would be parametric test. Otherwise, the alternative analysis option would be nonparametric test. Therefore, using SPSS, the datasets were subjected to a normality test and the results (z-scores and Kolmogorov Smirnov results) were generated, and verified based on the following key assumptions:

Assumption 1: z-score 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 factors.

Table 5 summarizes and presents the normality test results, indicating the z-scores and Kolmogorov Smirnov results, respectively.

Table 5: Test of normality results.

Factor/Items	Skewness z-scores values	Kurtosis z-scores values	Kolmogorov Smirnov Statistics	P > 0.05
Social factors				
Visibility	-1.435	-1.847	0.098	0.002
Learnability	1.500	-2.295	0.108	0.000
Users satisfaction	3.076	-1.950	0.107	0.000
Help and *documentation*	1.226	-1.092	0.033	0.008
Technical factors				
Error handling	2.793	1.118	0.117	0.001
Process revocability	-5.500	1.244	0.016	0.021
Security	-0.045	-1.432	0.074	0.012
Privacy and *confidentiality*	0.457	-1.366	0.092	0.001
Expressiveness	4.891	0.148	0.081	0.011
Medical information breaches	-2.120	-2.612	0.114	0.000
Conclusion: Datasets are not normally distributed; possible analysis option: non-parametric test, (Taherdoost, 2016; Joshi et al., 2015)				

According to Table 5 above, the skewness and kurtosis (z-score) results indicate the 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), *visibility* (z = -2.295), *revocability* (z = -5.500), and medical information breaches (z = -2.120). Thus, suggesting that the datasets are not normally distributed. With respect to assumption 2, the Kolmogorov Smirnov values (*p-vales*) are less than 0.05. Thus, suggesting that the datasets are still not normally distributed, since $p < 0.05$ for all factors. Therefore, based on the 2 assumptions and the normality test results generated, the datasets are not normally distributed. In this case, the appropriate analysis option would be nonparametric test [40,39]. However, for an appropriate choice of nonparametric statistical tools, more assumptions need to be made on the dataset. In this case, the factors considered were the types and the scale levels of the variables. Whereby, the variables are ordinal scale with 5 levels of response; usability factor, education and training factor, technology development factor, information

security factor, and medical information breach factor. Therefore, the appropriate corresponding nonparametric analysis tool would be Spearman's rank correlational analysis [40,39].

3.6. Spearman's rank correlational analysis

Subsequently, Spearman's rank correlational analysis was performed to measure the strength and direction of associations between SM socio-technical information security factors, and medical information breaches. Thus, Spearman's rank correlation coefficient (*r-value*) indicated the level of strength and direction of association between the variables. The level of strength ranges from $r = 0.00$ *to* ± 1.00, and the *p-values* determine the significance level of the relationships. In this case, $p \leq 0.05$ are considered significant. While for correlational direction, the positive/negative *r-values* indicates the direction of the correlation between the variables. Altogether, Table 13 presents Spearman's rank correlational results, indicating the factors, correlation coefficient (*r-value*), *p-values*, and the conclusion thereof, accordingly [40,39].

Table 6: Spearman's Rank correlation results.

Factors	Medical information safety levels: Correlation coefficient (*r-values*)	*p-values*	$p \leq 0.05$?
Visibility	- 0.58	0.000	Significant
Learnability	- 0.62	0.000	Significant
Satisfaction	- 0.75	0.000	Significant
Error-handling	0.36	0.041	Significant
Revocability	- 0.42	0.029	Significant
Expressiveness	0.44	0.002	Significant
Help and *documentation*	- 0.77	0.000	Significant
Security	- 0.76	0.001	Significant
Privacy and *confidentiality*	- 0.62	0.000	Significant
Conclusion: there is negative and significant relationships between the variables, (Zamanzadeh, et al., 2015)			

With respect to specific objective 3, the correlational relationships between 7 SM socio-technical information security factors and medical information breaches were negative, significant, and stronger. The factors include; *visibility* ($r = -0.58, p = 0.000$), *learnability* ($r = -0.62, p = 0.000$), *satisfaction* ($r = -0.75, p = 0.000$), *help* and *documentation* ($r = -0.77, p = 0.000$), *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; *error handling* ($r = 0.36, p = 0.041$), *revocability* ($r = -0.42, p < 0.029$), and *expressiveness* ($r = 0.44, p < 0.002$). In this case, stronger correlations imply strong relationships between the variables [42]. While the negative correlations could imply that the level of medical information breaches decreases with increase in the level of compliance in SM socio-technical information security factors [42], Altogether, section 4 stipulate a detailed discussion of the results.

4. Discussion of results

Presumably, the key SM socio-technical information security factors were mainly adopted from existing

literatures, as guided by socio-technical and usable-security principles [23,36,43,44]. In this case, the key factors identified under the social dimension include; 1) usability factors – *visibility*, *learnability*, and *satisfaction*; and 2) education and training factors – *help* and *documentation*. Meanwhile, the key factors identified under the technical dimensions include; 3) SM technology development factors – *error handling*, and *process revocability*; and 4) information security factors – *security*, *privacy*, and *confidentiality*, and *expressiveness*. Overall, the 9 factors attained the acceptable level of reliability test results. Remarkably, categorizing these factors under social and technical dimensions is a reasonable way of defining and pinpointing the vulnerable scope of SM usage with respect to medical information breaches [12]. Thus, the identified factors would provide SM practitioners and researchers with an empirical basis for rationalizing information security requirements on SM usage [45].

According to the frequency distribution summary in Table 3, the average percentage compliance level (respondent's agreement level based on 5-points Likert scale response) recorded were 31% for the social dimension and 39% for the technical dimension. It is worth noting that the percentage difference of 8% could be significant enough to guide the effort needed to establish SM usage policies and strategies. On the other hand, Spearman's rank correlational coefficients (*r-values*) indicate significant levels of correlational relationships for the 9 SM socio-technical information security factors identified. However, 6 of the factors presented negative and stronger relationships, compared to the 3 factors that yielded weaker correlational relationships. Relatively, the results showed stronger relationships between the social dimensional factors, compared to the technical dimension. The negative relationships could imply that an increase in end-user compliance level of SM socio-technical information security factors could minimize the occurrence of medical information breaches on SM. While the stronger relationship factors point out the key SM usage factors associated with medical information breaches. Notably, the average percentage compliance scores of 31% recorded for the social dimension and 39% for the technical dimension could propound on the need for strengthening the social dimensional factor, which presented stronger associations with medical information breaches, compared to technical dimensional factors. Overall, the results could suggest that much of the information security challenges are associated with the social dimension aspects of SM usage compared to the technical dimension. With respect to related studies, numerous studies have reported social engineering (behavioral) attacks as one of the prevalent forms of online information security breaches [23,22,13,36]. Overall, the study outcome would provide an empirical basis for medical institutions, as well as SM researchers and practitioners to rationalize and leverage SM usage in their operations.

5. Recommendations and conclusion

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). Notwithstanding the study limitations, the study outcome could be adopted to provide an empirical basis for medical institutions, as well as SM researchers and practitioners to rationalize and leverage SM usage in their operations. Remarkably, categorizing SM socio-technical information security factors under social and technical dimensions is a reasonable way of defining the vulnerable scope of information security challenges associated with SM usage [7,12,13]. Thus, the key factors would then provide

SM practitioners and researchers with a theoretical basis for rationalizing information security requirements on SM usage. SM socio-technical information security approaches would enhance the process of developing comprehensive models, strategies, and policies on SM usage. For instance, the study outcome provides 9 key factors to consider in ratifying, standardizing, and adopting SM usage in medical operations and researches, including curriculum and policy development. More so, formalizing SM usage would help institutions to enforce accountability in SM usage and protect the institutions against uncensored usage of SM by stakeholders. This would protect institutions against negative consequences such as loss of trust and reputation, legal suits, or financial harm [8,18,11,19,6] Nevertheless, the study also recommends for more empirical studies to be conducted to enrich the theoretical foundations of SM researches.

References

[1] 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.

[2] 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.

[3] 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

[4] Mirembe, D., Lubega, J. and Kibukamusoke, M. (2019) 'Leveraging social media in higher education: a case of Universities in Uganda', European Journal of Open, Distance and e-Learning, Vol. 22, No. 1, p.71, ISSN: 1027-5207 © 2019 EDEN

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

[6] 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

[7] 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.

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

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

[10] 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

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

[12] 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

[13] 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

[14] 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.

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

[16] 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

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

[18] 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.

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

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

[21] 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

[22] 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

[23] 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

[24] Di Gangi, Johnston, A. C., Worrell, J. L., & Thompson, S. C. (2016). 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

[25] 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.

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

[27] Yeratziotis, Pottas, D., & Van Greunen, D. (2012). 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

[28] Jain, Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, *7*(5), 2157–2177. https://doi.org/10.1007/s40747-021-00409-7

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

[30] 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

[31] 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

[32] 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

[33] 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

[34] 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

[35] He, W. (2012). A review of social media security risks and mitigation techniques. Journal of Systems and Information Technology, 14(2), 171-180.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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

[43] Mutebi, J., et al., (2022). A model for adopting a secure Social Media usage in selected Medical Institutions in Uganda. *International Journal of Computer*, 10 (10): 43 – 46

[44] Mutebi, J., et al., (2022). Medical information breaches occurrence with respect to Social Media usage, in selected medical institutions in Uganda. *Journal of Computer and Communications*, 10 (10): 10 – 33

[45] Akampurira P., Mutebi J. et al., (2022). A Framework for Evaluating the Usability of Mobile Learning Applications in Universities", *Journal of Science and Technology*, 07, (05): 42-59