International Journal of Business Management and Economic Review

Vol. 6, No. 04; 2023

ISSN: 2581-4664

EFFECT OF BEHAVIOUR MONITORING ON SECURITY OF ELECTRONIC HEALTH RECORDS IN TANZANIAN PUBLIC HOSPITALS

Ernest Godson[1], George Oreku[2] and Deus Ngaruko[3]

[1]Ph.D. Scholar, Department of Economics and Community Economic Development, Faculty of Arts and Social Science, the Open University of Tanzania

Email address: godsonernest21@gmail.com

[2]Professor, Department of Mathematics and ICT, Faculty of Science, Technology and Environmental Studies, the Open University of Tanzania

[3]Professor, Department of Economics and Community Economic Development, Faculty of Arts and Social Science, the Open University of Tanzania

http://doi.org/10.35409/IJBMER.2023.3512

ABSTRACT

This paper assesses the effects of behaviour monitoring on the security of electronic health records in Tanzanian public hospitals. A total of 300 users of EHRs from six purposefully selected public hospitals in Tanzania participated in this cross-sectional study. The study was designed using an explanatory hypothesis-testing survey with a quantitative approach. Data were collected using an online survey questionnaire with five-point scale questions. Multiple linear regression analysis was performed to assess the effects of behaviour monitoring on the security of electronic health records in Tanzanian public hospitals. The findings of the study revealed that behaviour monitoring had a positive significant effect on the security of electronic health records in Tanzanian public hospitals. Regression analysis found that, behaviour monitoring affects security of EHRs in Tanzanian public hospitals by 27.8% and was significant at 0.000, $p<0.05$. The study concluded that, behaviour monitoring had a positive significant effect on security of electronic health records in Tanzanian public hospitals. The study recommends that, the public hospitals should ensure effective behaviour monitoring in order to ensure that, all employees comply with the information security policies, rules and procedures for adequate security controls of EHRs.

Keywords: Behaviour Monitoring; Security Controls; Electronic Health Records; Public Hospitals.

1. INTRODUCTION

Users of information system are an essential part of successful security controls in information technology, Ifinedo (2014). The role of user behaviours in security controls is increasingly recognized as an important issue in the study of information security compliance, Siponen MT 2000;Bulgurcu B, Cavusoglu H, Benbasat (2010). According to Bulgurcu et al., (2010), information security behaviour is defined as an employee's behaviour in interactions with organizational information systems, comprising hardware, software, and networks etc., which have security consequences. Calic et al., (2016), specified that, users' behaviour related to security and privacy breaches in an information systems includes, but not limited to, sharing of passwords, over sharing of information on social media, accessing suspicious websites, using unauthorized external devices, random clicking on links, using the same passwords in various places, opening of attachment from an unknown sources, sending sensitive personal information

Vol. 6, No. 04; 2023
ISSN: 2581-4664

through mobile networks, not physically protecting personal electronic media and failure in updating the security software.

The study by Aurigemma and Mattson, (2017), stated that, individual choices and behaviours are influenced by their state of mind (personal attitude), social pressure from others (subjective norms), and a perception of control. Concurrent with this, Bulgurcu et al., (2010) postulate that an employee's intention to obey with the organization's information security policies is influenced by subjective norms (social pressures from other), perceived behavioural control, and attitude toward compliance. However, Aurigemma and Mattson (2017) added that, an organization's hierarchy with respected authority and control structures might impact how much control an individual has over a set of behaviours. Herath and Rao (2009) appreciate that social pressure such as behaviour monitoring may affect an employee's compliance behaviour, therefore implementing an effective users monitoring mechanism or an environment that fosters the security is a good strategy.

Verizon (2019), states that, in healthcare settings, highest health data breaches have resulting internally, with many occurrences being errors and incidents of misuse resulted from user's behaviours. Thus, the administration of healthcare organizations must promote users to practice best security behaviour for the health of healthcare information systems. Roer et al., (2020), added that, healthcare organizations are in large risk of internal threats and vulnerabilities originating from users' behaviour than other industries like banking or insurance which both capture, store and manage sensitive information. Dimkov et al., (2010) states that, threats can be posed by employees with legalised access to health information system such as temporary staff like medical students or interns, who are attached in the hospitals for learning purpose.

Employees in healthcare have different perceptions, values and norms on security controls, some employees can see information security as impeding productivity in healthcare, thus, increasing the rate of carelessness in security controls,(Alumaran et al., 2015; Kolkowska et al., 2017). Therefore, information security behaviour monitoring is critical in ensuring that, users' behaviour in information systems are monitored to protecting patient's information, Bulgurcu et al., (2010). Although different studies related to the security of electronic health records have been conducted in Tanzania, (Busagala 2013; Nehemia,L 2014; Kajiruga, et al, 2015; Kanani, 2016;Freye et al 2020), there is a scarce of studies which has specifically conducted to explore the effects of behaviour monitoring on the security of electronic health records in Tanzania. Thus, the knowledge gap still exists, therefore, this study intends to fill the gap by examining the effect of behaviour monitoring on the security of electronic health records in Tanzanian public hospitals.

2. LITERATURE REVIEW

2.1 Theoretical Perspectives

The study based on a theory of planned behaviour. The theory of planned behaviour Ajzen (TPB; 1985, 1991) is an extension of the theory of reasoned action (TRA) introduced by Fishbein and Ajzen (1975). This theory suggests that, behaviour is influenced by intention, and intention is inspired by attitude, subjective norms and perceived behavioural controls Ajzen, (1975). Attitude toward behaviour affects user's feelings about performing the behaviour. In other words, when users believed that it is important to understand and comply to certain behaviour, this feeling towards compliances positively influenced user's intentions to comply.

Vol. 6, No. 04; 2023
ISSN: 2581-4664

The theory contends that behaviour is a function of beliefs or information relevant to a specified behaviour. These beliefs are thus primary determinants of intentions and actions, Ajzen and Doll, (1992). These beliefs also link the specified behaviour with the outcomes generated by conducting that behaviour and any potential cost generated by performing the behaviour. Intentions which indicate the number of efforts individuals is willing to employ to perform a given behaviour are assumed to catch the motivational factors that influence a behaviour, Beck and Ajzen, (1991). Attitude toward behaviour captures an individual's positive or negative perceptions of performing the behaviour. For example, individuals with more positive perceptions of security control should also have a higher intention to comply with security controls policies. Subjective norms reflect the individual's impression of other's feelings about performing the behaviour, Ajzen (1991).

In healthcare organizations, users will be more enthusiastic about involving on security compliance behaviour if they think a favourable outcome is what will happen as a result of doing it (Ajzen, 1991). Also, users will feel more positive about promoting and participating in the proper information security actions if they are taught, highly acknowledged and heavily rewarded (Ajzen, 1991). On the other hand, if users lack understanding, have little knowledge in the information security issues particularly information security policies, and no vested interest and are frustrated in a way strongly that creates a convincing belief that performing a behaviour is negative, the employees will have an adverse attitude towards a behaviour (Ajzen, 1991), and hence will not comply to the security controls in information systems. This theory helped researchers to understand how behaviour is influenced by intention, and how intention is inspired by attitude, subjective norms and perceived behavioural controls.

2.2 Empirical studies

The study by van Niekerk, (2010), showed that, rewarding appropriate behaviour and punishing unsuitable behaviour are both important factors in shaping users' compliance to information security in organization. Training can help to change behaviour but must also be supported through the proper positive and/or negative incentives, as well as strong leadership (van Niekerk, 2010). The perceived threat of sanctions influences individual behaviours through the certainty and severity of punishment, i.e., as there is an increase of punishment certainty and punishment severity the level of illegitimate behaviour should decrease (Herath and Rao, 2009). They further suggest that, auditing mechanisms are a good deterrent measure for deviant behaviour. It is expected that, the more awareness of existing security detection means in an organization, users in information systems are more likely to comply with the security policies.

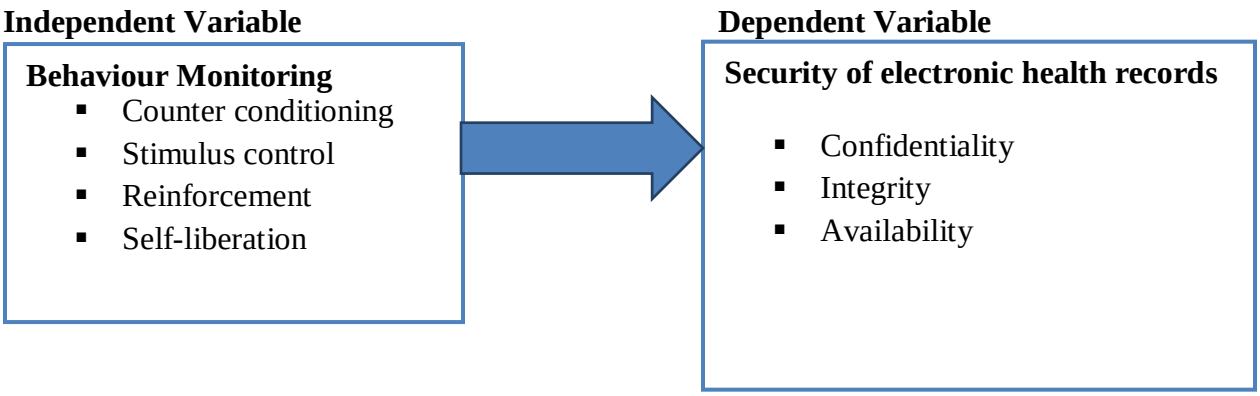
However, instead of using deterrent measures, Kabay (as cited in van Niekerk, 2010) suggests that employees should be praised for exhibiting the correct information security behaviour as this will result in a better response towards compliance. Kabay further suggested that a change of attitude can also be achieved by using persuasion. Some other studies also agree that sanctions and formal punishment may not be the best approach towards achieving information security compliance. The study conducted by D'Arcy, J., & Devaraj, S. (2012) shows that, a predisposition about the need for social authorization and moral beliefs concerning the behaviour are key indicators of technology misuse. This demonstrates that moral beliefs and social pressures are considered when employees make compliance decisions

According to the study by Hu, Xu, Dinev, and Ling (2011), deterrence have no influence on an

Vol. 6, No. 04; 2023
ISSN: 2581-4664

individual's intention to adhere to information security policy. Hu et al (2011) further stated that perceived benefits and intrinsic satisfactions are more influential in compliance decision making which must be built through continuous monitoring of user's behaviours. Additionally, top management must be committed in terms of resources to enable rewards for desirable behaviour, and in terms of authority to punish undesirable behaviour in an organization, van Niekerk, (2010).

According to Alqahtani and Robin Braun (2021), when users who are aware of monitoring know that their activities and behaviour may be directly or indirectly observed by others, especially in case of non-compliance and misconduct in the information systems, by not following the security policies requirements, they will try their best to adhere to the security policies to avoid getting punishment from the management. The FBI report 2021 revealed that, insider threat is not technical, it is user-related, and they proposed a behavioural monitoring approach to fight against internal threats posed by users.



3. MATERIAL AND METHODS

This cross-sectional research design used a quantitative research approach. The target population in this study were IT officers, medical doctors, nurses, pharmacists, health laboratory technologists, record officers and administrative officers from the six public hospitals in Tanzania. Purposive sampling techniques were used to select sampling frame from the population, this method enabled researchers to restrict to the targeted individuals only. The sample included 300 respondents who participated voluntarily. The five-point Likert scale questionnaire was used to collect data from the respondents. Security of electronic health records (EHRs) was the dependent variable and the variables that explained it included counter conditioning, stimulus control, reinforcement and self-liberation. Multiple linear regressions was used to create a model that predicts the effects of behaviour monitoring on security of electronic health records in Tanzanian public hospitals.

The collected quantitative data were assessed using descriptive statistics such as mean, frequencies, percentage and standard deviation. The SPSS version 25 was used to perform the analysis. To examine the relationship between independent variables and their effects on dependent variable, multiple linear regression analysis was used. This method enabled researchers to determine the variance of the model as well as the proportional contributions of each independent variable to the outcome variable, (Kumari & Yadav, 2018).

Vol. 6, No. 04; 2023
ISSN: 2581-4664

Structural Equation

The below model specification guided multiple linear regression analysis for this study

SCEHR= f (BM)…….……..…….….... (1)

Whereby,

SCEHR= Security Controls of Electronic Health Records

BM=Behaviour Monitoring

As stipulated in Table 1, behaviour monitoring is a composite score of counter conditioning, stimulus control, reinforcement and self-liberation, therefore equation 1 can be rewritten into equation 2.

SCEHR= f (CC, SC, RC, and SL) …. …..…….…… (2)

Structurally, equation 2 can be presented as in equation 3 when an error term is introduced.

$$\mathbf{SCEHR = \beta_0 + \beta_1 CC + \beta_2 SC + \beta_3 RC + \beta_4 SL + \varepsilon_i} \quad \text{……...……... (3)}$$

Whereby,

SCEHR=Security Controls of Electronic Health Records

β0 = Constant Term

β1= Beta coefficients

CC= Counter conditioning

SC= Stimulus control

RC= Reinforcement

SL= Self-liberation

ε = Error Term

Testing Multiple Linear Regression Assumptions

Before conducting regression analysis, the multiple linear regression assumptions were examined. The equation comprises of ordinary least squire. In the ordinary least squire, five assumptions such as linearity, normality, homoskedasticity, outliers and multicollinearity was assessed, (Tabachnick and Fidel 2014; Pallant, 2016).Normality test was done by developing the normal distribution table and assessment of kurtosis and skewness. The finding revealed that, values were within range (i.e., greater or equal to -2 and less or equal to 2), as suggested by Hair et al. (2010) hence normal distribution. Further, a Linearity test was conducted using the analysis of the graphs produced by the use of SPSS IBM version 25, in which linear correlation was observed between the variables. Furthermore, researchers created and analyzed scattered plots using SPSS IBM version 25 to test for homoscedasticity as suggested by Hair et al. (2010). The result revealed that, the homoscedasticity assumption was met. Finally, researchers assessed for the outlier using histogram, the result revealed that, there were no outliers as the produced histogram shows that, the residual values fall inside the 3 cutoffs as Tabachnick and Fidell (2007), stated that, any value outside the cut off of 3 is an oddity.

Test of Validity and Reliability

Validity

The validity of this study was ensured by conducting a pre-test or pilot test of the tools used for data collection. Before the actual data collection, the pre-test was carried out to 60 participants

Vol. 6, No. 04; 2023
ISSN: 2581-4664

who were homogeneous sample using the same research tools. The content validity index (CVI) was also used to check validity of the tool. The mean CVI for the study was 0.782, hence the value was higher than 0.70. Construct validity was maintained by restricting the question to the conceptualization of the variables and ensuring that the metrics for a given variable fit within the same construct.

Reliability

This study measured the scale reliability using Cronbach's alpha. A Cronbach's alpha of 0.70 and above is deemed suitable, 0.80 and above is better and 0.90 and above is best. The study therefore accepted a cut off point of 0.70 as the 0.8 was above the accepted level. The finding revealed that, Cronbach's alpha was 0.745 which is higher than 0.70. Hence, the data was reliable.

4. RESULT

4.1 Demographic characteristics

52.7% of respondents were male whereas 47.3% were female. On the other hand, 40.3% of respondents were at the age range of 20-30 years, 37.3% were between 31-40 years, 13.7% were between 41-50 years and 8.7% were between 51-60 years. Further, 51.7% of respondents had a bachelor's degree, 28% had a diploma, 14.3% had a certificate and 6% had a master's degree level of education. Furthermore, 49% of respondents had more than 5 years of working experience, 33.3% had 1-5 years of working experience, 13.7% had 1-3 years of experience and 4% had less than 1 year of working experience. Moreover, 23.7% of respondents were nurses, 22.7% were medical doctors, 18.7% were pharmacists, 14% were health laboratory technologists, 8.7% were IT officers, 7% were record officers and 5.2% were administrative staff.

Table 1: Demographic Characteristic of Respondents

Variables	Category	Frequencies	Percentages
Gender	Male	158	52.7
	Female	142	47.3
Age group	20-30	121	40.3
	31-40	112	37.3
	41-50	41	13.7
	51-60	26	8.7
Education Level	Certificate	43	14.3
	Diploma	84	28
	Bachelor degree	155	51.7
	Master degree	18	6
	PhD	00	00
Occupations	IT Officers	26	8.7
	Doctors	68	22.7
	Nurses	71	23.7
	Pharmacists	56	18.7
	Lab. Technologists	42	14

Vol. 6, No. 04; 2023
ISSN: 2581-4664

	Record officers	21	7
	Administrative officers	16	5.2
Working Experiences	Less than 1 year	12	4
	1-3 years	41	13.7
	1-5 years	100	33.3
	More than 5 years	147	49

Source: Field data 2022

4.2 Descriptive statistics

Respondents were given items to indicate their level of agreement or disagreement under the five-point Likert scale ranging from 5=strongly agree, 4=agree, 3= somehow agree, 2=disagree and 1=strongly disagree. Descriptive measures included frequency, percentage, mean and standard deviation. The pertinent results are presented in table 2.

Table 2: Descriptive Results

SN	Items	1	2	3	4	5	Mean	Std.
1	Users' access right is reviewed at regular interval	(20%)	(28%)	(11%)	(23%)	(17%)	2.89	1.410
2	Users are motivated to follow good security practices	(19%)	(31%)	(11%	(26%)	(11%)	2.78	1.333
3	All users return all of the organization's assets upon termination of their employment	(25%)	(22%)	(12%	(27%)	(13%	2.80	1.409
4	Security rules and policies are enforced by sanctioning the employees who break them	(37%)	(34%	(7%)	(14%)	(6%)	2.17	1.248
5	All employees, contractors and third-party users receive security awareness training	(25%)	(35%	(10%	(19%)	(11%	2.56	1.339
6	Background checks on all candidates for employment, contractors and third party are carried out	(16%)	(26%)	(10%	(28%)	(19%	3.08	1.403
7	Users are deterred from using information processing facilities for unauthorized purposes	(10%)	(23%)	(9%)	(34	(23%	3.37	1.332
8	Repeat security offenders are appropriately disciplined	(35%)	(37%	(10%)	(12%)	(6%)	2.20	1.213

Key: 1=Strongly Disagree; 2=Disagree; 3=Somehow agree; 4=Agree and 5=strongly agree

Vol. 6, No. 04; 2023
ISSN: 2581-4664

The responses on whether, users' access right was reviewed at regular interval using formal processes was as follows; 20% strongly disagreed with the statement, 28.3% disagreed, 11.7% were somehow agree, 23% agreed and 17% strongly agreed. On whether, users are motivated to follow good security practices in the use of passwords, the following were the results; 19.7% strongly disagreed, 31.3% disagreed, 11.3% were somehow agree, 26.3% agreed and 11.3% strongly agreed with the statement. On whether, all users return all of the organization's assets upon termination of their employment, 25% strongly disagreed, 22.7% disagreed, 12.3% were somehow agree, 27% agreed and 13% strongly agreed with the statements. On whether, security rules and policies are enforced by sanctioning the employees who break them, 37.7% strongly disagreed, 34.7% agreed, 7.3% were somehow, 14% agreed and 6.3% strongly agreed.
When respondents asked on whether, all employees, contractors and third-party users receive security awareness training, 25% strongly disagreed, 35% disagreed, 10% were somehow agree, 19% agreed and 11% strongly agreed with the statement. On whether, background checks on all candidates for employment, contractors and third party are carried out, 16.3% strongly disagreed, 26% disagreed, 10% were somehow agree, 28.3% agreed and 19.3% strongly disagreed. On other hand, findings on whether users are deterred from using information processing facilities for unauthorized purposes, 10% strongly agreed, 23.3% disagreed, 9.3% were somehow, 34% agreed and 23.3% strongly agreed with the statement. Moreover, finding revealed that, repeat security offenders are appropriately disciplined through disciplinary process, 34% strongly disagreed, 37% disagreed, 10.3% were somehow agreed, 12.3% agreed and 6.3% strongly agreed with the statement.

4.3 Inferential statistics

Inferential statistics was used to make inferences about the populations based on the survey results. To generalize from the study to the population, hypothesis testing techniques was used. Inferential statistics consisted of Pearson correlations and regression analysis. Pearson correlation coefficient was used to compute the correlation between the dependent variable (security of electronic health records) and the independent variable (behaviour monitoring) in order to determine the strength of the relationship at 1% significance level. A result shows that behaviour monitoring was positively correlated to security of electronic health records, counter conditioning ($r=0.25$, p-value<0.005), stimulus controls ($r=0.11$, p-value<0.005), reinforcement($r= 0.38$, p-value<0.005), self-liberation ($r= 0.30$, p-value<0.005. Therefore, the findings showed a positive relationship between behaviour monitoring and security of electronic health records in Tanzanian public hospitals.

Vol. 6, No. 04; 2023
ISSN: 2581-4664

Table 3: Correlation analysis

		Security of EHRs	Counter conditioning	Stimulus control	Reinforcement	Self-liberation
Security of EHRs	Pearson Correlation	1				
	Sig. (2-tailed)					
Counter conditioning	Pearson Correlation	.251**	1			
	Sig. (2-tailed)	.000				
Stimulus control	Pearson Correlation	.116*	-.022	1		
	Sig. (2-tailed)	.045	.708			
Reinforcement	Pearson Correlation	.388**	.035	.053	1	
	Sig. (2-tailed)	.000	.546	.364		
Self-liberation	Pearson Correlation	.300**	.096	.092	.065	1
	Sig. (2-tailed)	.000	.098	.113	.261	

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

4.4 Regression Analysis

Multiple linear regression analysis for behaviour monitoring and security of electronic health records was done to find out the effect of behaviour monitoring on security of electronic health records in Tanzanian public hospitals. The multiple linear regression (R) indicates that the regression between dependent variable and the independent variable jointly predicts the model. The coefficient of determination (R^2) determines the alteration of variation independent variable as enlightened by dependent variable jointly. Table 4 below shows the summary of the results of the values of R and R^2.

Table 4: Model Summary

					Change Statistics				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig.F Change
1	.527[a]	.278	.268	8.44951	.278	28.347	4	295	.000

a. Predictors: (Constant), Self-liberation, Reinforcement, Counter conditioning, Stimulus control

In Table 4, coefficient of variation (R) was 0.52 which implies that the degree of association between behaviour monitoring and security controls of EHRs is significant and positive. The (R^2) was 0.278 which implies that 27.8% variations in security controls of electronic health

Vol. 6, No. 04; 2023
ISSN: 2581-4664

records are explained by behaviour monitoring in the model, while 72.2% was explained by other factors.

Table 5: ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	8095.273	4	2023.818	28.347	.000[b]
	Residual	21061.314	295	71.394		
	Total	29156.587	299			

a. Dependent Variable: Security of EHRs
b. Predictors: (Constant), Self-liberation, Reinforcement, Counter conditioning, Stimulus control

From the ANOVA table 4, the F value of the model was F=28.347, p<0.01), this shows that it was significant at a 99% confidence level hence, the model is feasible. Thus, the model is stable and significant at a 99% confidence.
The statistical analysis was done to determine the association of variables. The result in Table 5 indicates that behaviour monitoring had significant effect on security of electronic health records since the p-value was 0.000, which is less than 0.05. Significance level (see table 5). This implies that, behaviour monitoring has a significant effect on enhancing security of electronic health records in Tanzanian public hospitals.

Coefficients of determination
In determining the causal effect relationship between the dependent variable and the independent variables, the regression coefficient was tested at the 5% level of significance using t-test, the result shows that, counter conditioning (B=217, P=0.000), stimulus control (B=0.079, P=0.015), Reinforcement (B=0.360, P=0.000), Self-liberation (B=0.248, P=0.000), as shown in Table 6. This result indicates a positive significant relationship between behaviour monitoring and security of electronic health records in Tanzanian public hospitals

Table 6: Coefficients of regression

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	13.525	2.677		5.052	.000
	Counter conditioning	1.158	.266	.217	4.351	.000
	Stimulus control	.406	.257	.079	1.580	.015
	Reinforcement	1.822	.251	.360	7.250	.000
	Self-liberation	1.325	.267	.248	4.966	.000

a. Dependent Variable: Security of EHRs

Vol. 6, No. 04; 2023
ISSN: 2581-4664

5. DISCUSSION

The objective of this study was to assess the effects of behaviour monitoring on security of electronic health records in Tanzanian public hospitals. Findings from the descriptive results indicated that, public hospitals practices on behaviour monitoring had a positive significant relationship with security controls of electronic health records. However, the level of behaviour monitoring to the surveyed public hospitals was not enough as the use of electronic health records is still in its infancy, it was revealed that, more investment on behaviour monitoring is needed for the effective security controls in electronic health records in a Tanzanian public hospital.

The inferential results revealed that, there is a direct positive significant relationship between behaviour monitoring and security of electronic health records in Tanzanian public hospitals, (B=217, P=0.000), stimulus control (B=0.079, P=0.015), Reinforcement (B=0.360, P=0.000), Self-liberation (B=0.248, P=0.000) as provided for by the regression analysis. This stipulates that an increase in behaviour monitoring would result in a significant increase in security controls of electronic health records in Tanzanian public hospitals. This confirms the views of Idowuet al., (2013), in their study on effects of monitoring and control activities on fraud detection which found that, monitoring activities had a positively significant at 5% level, adjusted R^2 was 0.268 which implied that 26.8% of the variation on performance was explained by monitoring activities in the model. It also, agrees with the study conducted by Hassidim et al (2017), which showed that, in healthcare organizations, user's behaviours such as poor passwords and sharing of passwords with colleagues is the most common forms of security incidents caused by users and should be monitored for effective security controls.

The findings of this study were also in line with the study conducted by Balozian and Leidner (2017) which showed that, monitoring and control were one of the factors that strongly affects the compliance behaviour of the employees regarding security controls in an organization. The study argued that, those users who were aware of monitoring practices know that their work and behaviour may be directly or indirectly observed by others, especially in the case of non-compliance and misconduct at work, i.e., by not following the information security policy requirements, will try their best to follow the security policy in order to not be fired by the management.

The coefficient of determination through the R square indicated that up to 27.8% of the change in the security of electronic health records in Tanzanian public hospitals is significantly accounted for by behaviour monitoring (R^2=0.278, p=0.000). This implies that, behaviour monitoring is significant predictor of security of electronic health records in Tanzanian public hospitals. These results are adequately supported by (Farooq, Ndiege, &Isoaho, 2019; Yoon, Hwang, & Kim, 2019) which revealed that, users 'behaviour monitoring was relatively weak positive and only 14.9% of the variability in information security behaviour was explained, suggesting that other factors are also important in improving information security controls in an organization. The result is in agreement with the findings of Klein Rodrigo and Luciano Edimara (2016), who investigated what influence users' behaviour on security controls and found that user's behaviour controls have a positive influence on security controls in information system of an organization.

Vol. 6, No. 04; 2023

ISSN: 2581-4664

6. CONCLUSION AND RECOMMENDATIONS

Based on the research findings, the study concluded that, behaviour monitoring has a positive significant relationship with security of electronic health records in Tanzanian public hospitals. With appropriate behaviour monitoring, healthcare organizations are in a better position to protect electronic health records kept in the hospital's information systems..

This study recommends that, public hospitals management should constantly monitor its user's behaviours in electronic health record systems for effective security controls. Specifically, user's access right should be reviewed at the regular interval, background checks to potential candidates for employment, contractors and third party should be performed before engaging them to the hospital's information systems, security rules and policies should be enforced by sanctioning users who break them, all users should return all hospital's facilities upon termination of their employment and repeated offenders should be punished using appropriate punishment actions.

REFERENCES

Abiola, I., & Adedokun, T. O. (2013). Evaluation of the effect of monitoring and control activities on fraud detection in selected Nigerian commercial banks. *Evaluation*, *4*(6), 12-20.

Abuhammad S, Alzoubi KH, Al-Azzam SI, Karasneh RA. (2020). Knowledge and practice o patient's Data Sharing and Confidentiality Among Nurses in Jordan. J Multidiscip Healthc. 2020 Sep 16;13: 935-942.doi: 10.2147/JMDH.S269511.PMID: 32982270; PMCID: PMC7502382

Alqahtani, M., & Braun, R. (2021). Examining the Impact of Technical Controls, Accountability and Monitoring towards Cyber Security Compliance in E-government Organisations.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179-211.

Alumaran, S.; Bella, G.; Chen, F. The role and impact of cultural dimensions on information systems security in Saudi Arabia National Health Service. Int. J. Comput. Appl. 2015, 112, 21–

Aurigemma, S. and Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. Retrieved on 6/28/2020 from: https://facultystaff.richmond.edu/~tmattson/Status_Computers_Security_2017.pdf

Balozian, Puzant, and Dorothy Leidner, (2017). "Review of IS Security Policy Compliance: Toward the Building Blocks of an IS a security Theory." *Data Base for Advances in InformationSystems*.

Bulgurcu B, Cavusoglu H, Benbasat I. Information Security Policy Compliance:An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly. 2010 September: p. 523-548

Busagala L. S. P. and Kawono G. C. (2013a). Underlying Challenges of E-Health Adoption in Tanzania. International Journal of Information and Communication Technology Research. Volume 3No. 1, January. ISSN 2223-4985.

Cushing, T. 2017, May 23. FBI Insider Threat Program Documents Show How Little It Takes to Be Branded a Threat to the Agency. Tech Dirt.

Vol. 6, No. 04; 2023

ISSN: 2581-4664

https://www.techdirt.com/articles/20170517/12422437396/fbi-insider-threat-program-documents-show-how- little-it-takes-to-be-branded-threat-to-agency.shtml

Dimkov, T.; Pieters, W.; Hartel, P. Laptop Theft: A Case Study on the Effectiveness of Security Mechanisms in Open Organizations. In Proceedings of the 17th ACM Conference on Computer and Communication Security, Chicago, IL, USA, 4–8 October 2010; pp. 666–668.

D'Arcy, J., and Greene, G. (2009). The Multifaceted Nature of Security Culture and Its Influence on End User Behavior. Paper presented at the IFIP TC 8 International Workshop on Information Systems Security Research, Cape Town, South Africa.

Farooq, A., Ndiege, J. R. A., & Isoaho, J. (2019). Factors affecting security behavior of Kenyan students: An integration of Protection Motivation Theory and Theory of Planned Behavior. In *2019 IEEE AFRICON*. Accra, Ghana

Hair, J. F, Babin, J.B., Anderson, R.E & Black, C.W. (2010). Multivariate data analysis. (7th edition). Upper Saddle River: Pearson Prentice Hall.

Herath, T.; Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis. Support Syst. 2009, 47, 154–165.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? Retrieved on 6/29/2020 from: https://dl.acm.org/doi/pdf/10.1145/1953122.1953142 6/29/2020

Hwang, J., Kim, J., Choi, K. J., Cho, M. S., Nam, G. B., & Kim, Y. H. (2019). Assessing accuracy of wrist-worn wearable devices in measurement of paroxysmal supraventricular tachycardia heart rate. *Korean circulation journal*, *49*(5), 437-445.

Ifinedo, P. (2014). Information systems security policy compliance: an empirical study of the effects of socialization, influence, and cognition. *Inf. Manag.* 51, 69–79. doi: 10.1016/j.im.2013.10.001

ISO 27799; Health Informatics—Information Security Management in Health Using ISO/IEC 27002. International Standard Organization: Geneva, Switzerland, 2016

Van Niekerk, J. F. (2010). Fostering Information Security Culture Through Integrating Theory and Technology Retrieved on 6/27/2020 from:https://pdfs.semanticscholar.org/be30/7fe1c35e58da0340ea22d72676b3c914c1a9.pdf

Kajirunga A., Kalegele K. (2015). Analysis of Activities and Operations in the Current E-Health Landscape in Tanzania: Focus on Interoperability and Collaboration. (IJCSIS) International Journalof Computer Science and Information Security, Vol. 13, No. 6, June 2015.http://sites.google.com/site/ijcsis/Jacobs, S. (2016). Engineering Information Security. Hoboken: Jacobs.

Kanani G. (2016). Money Matters in Health & Tech: The Road Towards E-Health in Tanzania. The Citizen Online Magazines (Monday, November 7, 2016). Retrieved on 08th March. 2019 athttps://www.thecitizen.co.tz/magazine/The-road-towards-e-Health-in-Tanzania/1840564-3443772-format-xhtml-nboinv/index.html

Klein, R. H., & Luciano, E. M. (2016). What influences information security behavior? A study with Brazilian users. *JISTEM-Journal of Information Systems and Technology Management*, *13*, 479-496.

Kolkowska, E.; Karlsson, F.; Hedström, K. Towards analysing the rationale of information

Vol. 6, No. 04; 2023
ISSN: 2581-4664

security non-compliance: Devising a Value-Based Compliance analysis method. J. Strateg. Inf. Syst. 2017, 26, 39–57.

Kumari, K., & Yadav, S. (2018). Linear regression analysis study. *Journal of Primary Care Specialties*, *4*(1), 33-36.

Nehemiah, L. (2014). Towards EHR interoperability in Tanzania hospitals: issues, challenges and opportunities. *arXiv preprint arXiv:1410.2205*.

Pallant, J. F., Haines, H. M., Green, P., Toohill, J., Gamble, J., Creedy, D. K., & Fenwick, J. (2016). Assessment of the dimensionality of the Wijma delivery expectancy/experience questionnaire usingfactor analysis and Rasch analysis. *BMC pregnancy and childbirth*, *16*

Roer, K.; Petriˇc, G.; Eriksen, A.; Huisman, J.; Smothers, R.L.; Carpenter, P. Measure to Improve: Security Culture Report 2020.2020. Available online: https://www.knowbe4.com/hubfs/Security-Culture-Report.pdf (accessed on 10 November 2022).

Siponen MT. A conceptual foundation for organizational information security awareness. Information Management & Computer Security. 2000; 1: p. 31-41

Tabachnick, B. G., & Fidell, L. S. (2014). Using multivariate statistics. Harlow. *Essex: Pearson Education Limited*.

Verizon. Protected Health Information Data Breach Report. Available online: https://enterprise.verizon.com/resources/reports/protected_health_information_data_breach_report.pdf (accessed on 21 December 2022)