BMC Medical Informatics
and Decision Making

RESEARCH **Open Access**

Digital health data security practices among health professionals in low-resource settings: cross-sectional study in Amhara Region, Ethiopia

Ayenew Sisay Gebeyew[1,2*], Wondwossen Zemene[2], Binyam Chaklu Tilahun[2], Nebyu Demeke Mengestie[2], Berhanu Fikade Endehabtu[2], Zegeye Regasa Wordofa[1], Mitiku Kassaw Takillo[1], Gedefaw Belete Ashagrie[3] and Melaku Molla Sisay[4]

Abstract

Introduction Protecting digital health data from unauthorized access, alteration, and destruction is a crucial aspect of healthcare digitalization. Currently, digital security breaches are becoming more common. Healthcare data breaches have compromised over 50 million medical records per year. In Ethiopia, health digitization has grown gradually. However, there is a limitation of study in digital health security. Studying digital health data security helps individuals protect digital data as a baseline and contributes to developing a digital health security policy.

Objective To assess the practice of healthcare professionals in digital health data security among specialized teaching referral hospitals in Amhara Region, Ethiopia.

Method A cross-sectional study design supplemented by a qualitative purposive sampling method was used to measure the digital data security practices of health professionals. The sample size was determined via single population proportion formula. A simple random sampling technique was used for the study participants. Then, self-administered questionnaires were administered. Multivariable logistic analysis was used to identify associated factors using STATA software. For the qualitative study, key informant interviews were used and analyzed using thematic analysis approach via open-code software.

Results Out of the 423 health professionals, 95.0% were involved in the survey. The finding indicates digital health data security practice of health professionals working at specialized teaching hospitals were 45.0%, CI: (40, 50). Health professionals 41–45-year age group (AOR = 0.107), master's degree (AOR = 2.45), postmaster's degree (AOR = 3.87), time to visit the internet for more than two hours (AOR = 2.46), basic computer training (AOR = 2.77), training in digital data security (AOR = 2.14), and knowledge (AOR = 1.76) were associated with the practice of digital health data security. For the qualitative study, three teams were prepared. The findings indicate digital health data security can be improved through training, advanced knowledge and working with digital security.

*Correspondence:
Ayenew Sisay Gebeyew
ayu.uog@gmail.com; ayenew_sisay@dmu.edu.et

Full list of author information is available at the end of the article

Conclusion The practice of digital health data security in specialized teaching hospitals in the Amhara region was inadequate. Therefore, it can be improved through enhancing education status, increasing the time needed to visit the internet, providing computer training, and updating health professionals' knowledge toward digital health data security.

Keywords Practice, Digital health, Digital data security, Health profession

Introduction

Healthcare digitization is one of the pillars of the information revolution agenda, which requires every institution to improve the flow of information through the digital space [1, 2]. The protection of health data needs security to maintain data integrity, availability, and confidentiality to prevent unauthorized access, alteration, or destruction and ensure an optimal level of risk perception [3, 4]. In institutions, digital security breaches are increasing globally, costing approximately $3.49 million per breach, which has threatened nearly $5.2 trillion in global value between 2019 and 2023 [5, 6].

In the context of developing countries, including Africa, digitization has grown rapidly, especially in terms of cybersecurity activity [7]. However, more than 90% of African companies operate without the required digital security [8]. As a result, online scamming, business email compromise (BEC), and ransomware are the most common digital threats affecting African institutions. More specifically, healthcare settings are the dominant area [8, 9]. Therefore, healthcare data are a popular target for hackers, and digital criminals are primarily interested in digital health data containing protected health information (PHI) [10].

Data breaches in healthcare organizations were 1.25 times more common in 2016 than they were five years ago [11]. Even though the health industry is undergoing a significant digital shift, security is a critical issue for organizations working in a networked environment [12, 13]. Over 45.7 million medical records were compromised in 2021, the second-highest number of records breached since 2015 [14]. To protect data, researchers have advocated advancing knowledge and providing training on digital health data security [15]. Previous studies have suggested that improving digital health data security status, educational status, health professionals' knowledge, computer training, risk perception, motivation, and attitudes were contributing factors [3, 16, 17, 18, 19, 20, 21, 22, 23].

The Federal Minister of Innovation and Technology drafted the Data Protection Proclamation in Ethiopia as a result of digital attacks [13, 24]. According to the findings, 11.6% of Ethiopian public agencies have trial-level legal frameworks, with 87.4% having no recognized legal frameworks to counter attackers [13]. The Health Information Management System Society (HIMSS) Healthcare Digital Data Security Survey for 2021 revealed that digital data security, outdated infrastructure, a rise in social engineering, and ransomware assaults are difficulties for the healthcare industry [25].

However, in Ethiopia, the Ministry of Health (MOH) has focused on digital health innovation [26]. However, health data are exchanged via digital technology, digital data security is a challenge in the healthcare setting [27]. The main points associated with the loss of health records are viruses, poor backup systems, and software corruption [28]. Furthermore, a qualitative study revealed that the usability of security measures is a rich topic in light of current advanced system security breaches and suggested identifying the factors of security challenges for e-health security improvement [29].

Therefore, studying the digital health data security practices of health professionals has a significant purpose for healthcare digitization because health professionals are the main targets of cybercriminals [28]. A study aimed to assess the digital data security practices of healthcare professionals working at specialized teaching hospitals in the Amhara Region, Ethiopia. This study helps improve the practice of digital data security measures. The findings will be used as a baseline for future studies and will help the responsible body guide digital health security policy.

Methods

Study design

The study was conducted in the Amhara region of Ethiopia. It is located 173 km from Bahir Dar and 493 km from Addis Ababa. Each hospital serves as a teaching and referral center for more than 3.5 million people. A hospital-based cross-sectional study supplemented with a qualitative method was conducted to assess the practices of the health profession on digital data security. The study was carried out via a cross-sectional study design and a phenomenon approach. All participants provided written informed consent to participate in the study (Appendix I). The study was conducted at specialized hospitals from June to July 2022 G.C.

Study participants

All health professionals who had worked in a specialized teaching hospital in the Amhara region were the source population, and health professionals who had used digital devices in a specialized teaching hospital were selected for the study population. Healthcare professionals who used digital health data from a specialized teaching hospital were included in the study.

Sample size determination and sampling procedure

The sample size was determined via a single population proportion. It was calculated using the assumption of a significance level of 95%, a 5% margin of error, a 50% population proportion, and 10% contingency [30]. The total sample size was 423. All the study participants were chosen via simple random sampling at specialized teaching hospitals, with proportional allocation for each health institution (Fig. 1). To ensure the robustness of the findings of the study, a qualitative method was used, and the results were measured via key informant interviews until data saturation was reached, with seven key informant interviews. Purposive sampling was used to select the study participants. Then, a phenomenology approach was used. This approach helps to get the lived experiences of health professions toward digital health data security. Hence, detail experience of health professionals towards digital health data security were collected.

Operational definition

Practice digital health data security: Health professionals who practice electronic countermeasures to protect digital health data from unauthorized access, alteration, and loss. This scale is measured via ten items with a score of yes or no question. The data were distributed normally by checking the Shapiro‒Wilk test (p value > 0.05), skewness, and kurtosis. Therefore, it selects the mean over the median for the outcome variable, and scoring above the mean value of 5.19 ± 2.1 (SD) has good digital data security practice, whereas scoring below the mean has not been practiced [19, 20, 21]. The motivation to practice digital security refers to an individual's commitment to engage in or strive to practice digital security techniques when health data are used and scoring above the median value of 23 (IQR 20–24) using six-item Likert scale questions that have good motivation, whereas those below the median value are poor motivation [23]. Knowledge of digital data security refers to the know-how of health professionals to practice security techniques when health data are used. It is measured via ten items with a Likert scale, and a score above the median value of 35 (IQR 31–40) indicates good knowledge, whereas a score below the median value indicates poor knowledge [23, 31]. Attitudes toward digital data security refer to how individual health professionals feel when handling health data using data security techniques. It is measured via eight-item Likert scale questions. A score above the median value of 31 (IQR 27–33) indicate favorable attitudes, and a score below the median value indicate unfavorable attitudes toward digital health data security [23, 32].

Data collection procedure and quality assurance

A structured, self-administered questionnaire was adapted and modified using data from various sources [3, 23, 32, 33, 34, 35]. The questionnaire was prepared in English. It was judged by research consultants and research teams to ensure its quality. Then, a pretest was conducted. A Cronbach's alpha above 70% was included. The data were collected by five trained data collectors

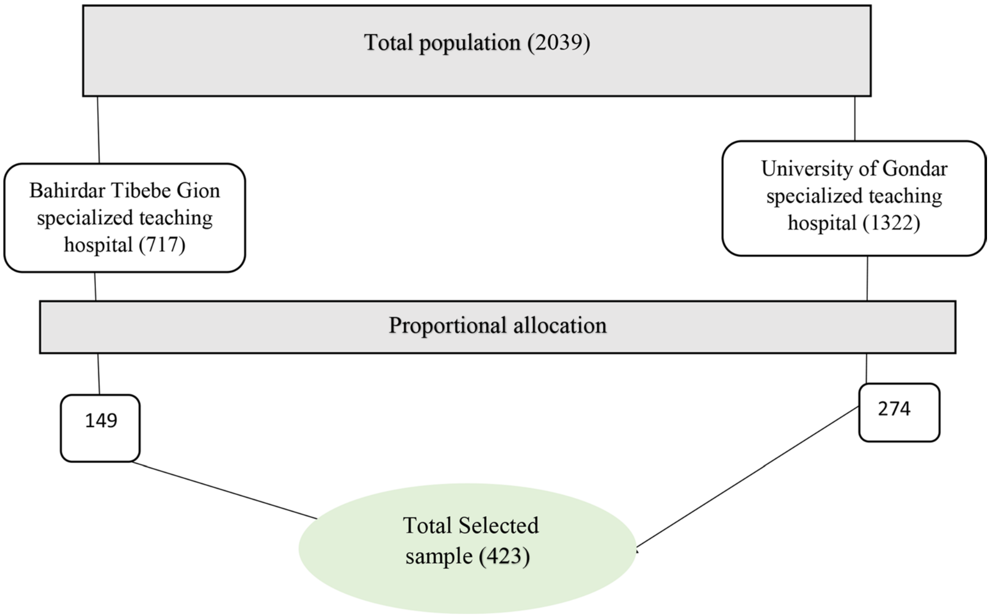
Total population (2039)
Bahirdar Tibebe Gion specialized teaching hospital (717)
University of Gondar specialized teaching hospital (1322)
Proportional allocation
149
274
Total Selected sample (423)

Fig. 1 Sampling procedure of digital data security practice among health professionals in healthcare at specialized teaching hospitals in Amhara Region, 2022

and guided by two supervisors. Health informatics professionals have collected the questionnaire. Then, the investigators performed overall supervision. Data incompleteness and data entry errors were checked using statistical software to minimize errors.

For the qualitative study, the questionnaire was developed in English and translated into the local language. The investigator used key informant interviews with semi structured, open-ended interviews. Purposive heterogeneous sampling was used to choose individuals who had experience with digital data security practices. The interviews were conducted in a secure setting, recorded via a suitable sound recorder, and transcribed and translated into English by language experts. To ensure the reliability and validity of the qualitative data, the study was conducted from multiple perspectives via triangulation techniques, and moderators were employed to reduce personal bias. The incoming data were checked to address the research questions adequately. In addition, the completeness of the data has been checked. This is accomplished through the clustering of data in groups. Finally, the data saturation was optimized.

Table 1 Socio-demographic characteristics of health professionals practice digital data security in healthcare at specialized teaching hospitals in Amhara Region, Ethiopia (*n*=402)

Variables	Frequency	Percent
Gender		
Male	254	63.18
Female	148	36.82
Age		
20-25	16	3.98
26-30	115	28.61
31-35	93	23.13
36-40	121	30.10
41-45	40	9.95
46-47	17	4.23
Marital status		
Single	166	41.29
Married	191	47.51
Other	45	11.19
Educational status		
Bachelor degree	293	72.89
Master's degree	55	13.68
Post master's degree	54	13.43
Work experience		
≤ 3 years	138	34.33
4-6 year	138	34.33
6-9 year	82	20.40
> =10 year	44	10.95
Monthly Salary		
≤ 10,000	273	67.91
< 10000-15000	97	24.13
> 15,000	32	7.96
Have smartphone		
Yes	290	72.14
No	112	27.86

*Post master's degree (specialist, subspecialist), *Other (Separated, windowed)

Statistical analysis

Epi Data Version 4.6 software was used to enter the data and exported to Stata software Version 16. Cleaned data were produced by checking the assumption of logistic regression. Binary logistic regression was used to identify the associated factors. Then, variables with a p value less than or equal to 0.2 were selected as candidates for multivariable analysis. Using adjusted odds ratios with a 95% confidence interval and a p value < 0.05, the outcome variable was determined by controlling confounding effects. To check the goodness of model fit, the Hosmer- Lemeshow test is a more trustworthy indicator of the outcome variable. Therefore, the goodness of the model fitness has been checked using the Hosmer-Lemeshow test. The p-value is greater than the significant level ($p \leq .05$). Thus, the model fits the data. For qualitative data, Open Code software version 4.02 was used to analyze the results via thematic analysis.

Results

Sociodemographic characteristics

Among the 423 study participants, only 5.0% did not complete the survey. Hence, 402 participants were included in the analysis. The average age of the study participants was 34.5 ± 5.87 (SD) years. The majority of the participants were male, accounting for 63%. The majority of health professionals were between the ages of 36 and 40, accounting for 30% of all health professionals. Among the participants with respect to marital status, the majority were married, accounting for 47.5% of them. With respect to educational status, a high proportion of health professionals had a bachelor's degree, accounting for 72%. Among professionals, 30.35% were physicians (Table 1).

Behavioral and organizational characteristics

In terms of behavioral factors, 53.98% of health professionals had favorable attitudes toward practicing digital data security. In terms of knowledge, 51.24% of the participants had poor knowledge compared with those who had good knowledge. Additionally, 52.74% of the participants were highly motivated, and 50.25% of the respondents perceived risk when they practiced digital data security. This study also revealed that 81.34% of the respondents had not received security training, whereas 57.96% agreed that there was a workload in the organization (Table 2).

Table 2 Behavioural and organizational characteristics of health professionals' practice of digital data security in healthcare at specialized teaching hospitals in Amhara Region, Ethiopia (n=402)

Variables	Freq.	Percent
Attitude		
Unfavourable	185	46.02
Favourable	217	53.98
Knowledge		
Poor	206	51.24
Good	196	48.76
Motivation		
Low	190	47.26
High	212	52.74
Perception of risk		
Low risk	200	49.75
High risk	202	50.25
Trained in digital data security		
Yes	75	18.66
No	327	81.34
Health care workload		
Low	169	42.04
High	233	57.96

Table 3 Technological characteristics of health professionals' practice of digital data security in healthcare at specialized teaching hospitals in Amhara Region, Ethiopia (*n*=402)

Technological variables	Freq.	Percent
Use internet		
Yes	394	98.01
No	8	1.99
Time spent on internet per a day		
≤ 2.5 h.	180	44.78
> 2 h.	222	55.22
Use social media		
Yes	390	97.01
No	12	2.99
Took basics computer training		
Yes	229	56.97
No	173	43.03
Shared digital device in the working area		
No	74	18.41
Yes	328	81.59
Handle (process) health data using digital device daily		
No	31	7.71
Yes	371	92.29
Trained in digital data security		
Yes	75	18.66
No	327	81.34
Computer skill		
Poor	148	36.82
Good	254	63.18

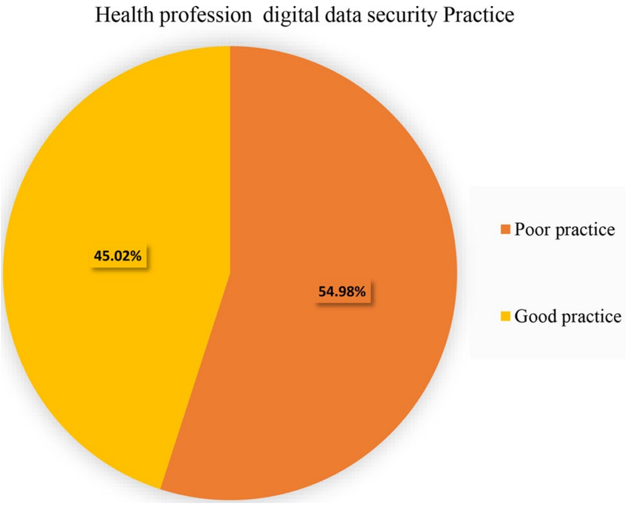

Fig. 2 Magnitude of digital data security practices among health professionals in healthcare at specialized teaching hospitals in the Amhara Region, Ethiopia (*n*=402)

Technological characteristics

In terms of technological characteristics, 92.29% of the participants handled health data using a digital device daily, 98.01% used the internet, 55% accessed the internet for more than two and a half hours, 97.0% used social media, 56.97% had basic computer training, and 63.18% had basic computer skills (Table 3).

Digital health data security practice

This diagram shows that, digital health data security practice of health professional in specialized referral teaching hospital in the Amhara region, Ethiopia was 45.0%, (95% CI [40, 50]) with a mean score of 5.19 ± 2.1 (SD). Among those, 28.11% were males, and 16.92% were females. The variation is due to the number of females in the healthcare institution is limited. Whereas 54.9% of the respondents poorly practiced digital health data security (Fig. 2).

Thematic analysis

Key informant interviews were used to conduct qualitative studies. The key informant persons were responsible and had a head role in the working area. These persons had good knowledge about the digital data security practices of health professionals. Seven key informant persons (KIP) were interviewed. The mean age and working experience of the health professionals were 30 and 5 years, respectively. The study took an inductive approach. On the basis of the data, three themes were created. These were digital health data security practices, challenges, and alternative solutions.

Theme 1: digital data security practice

Healthcare digitization has been introduced in each healthcare unit. Hence, health professionals have been close to digital health technology. However, they shared health data via digital devices, and the data were not secured. The interviewees responded that health professionals have little practice in digital health data security techniques. Thirty-one years of age feel that *"... we download everything... & like it subscribes... the expert is not as knowledgeable as to handle system security problems"* (Respondent 2). Radiology suggests that *"... we do not use data encryption because we do have not enough skills to practice" (*Respondent 1). A man who had worked in monitoring and evaluation responded, *"...I think many experts about digitalization already have a lot of recognition.... a lot of people are now turning a lot of data into digital; I trust they have a good level of recognition for that,.... However, their understanding of digital security is not significant. Because there are so many techniques out there that only a few have a good look at it, for example, using a password"* (Respondent 6).

Theme 2 challenge

Subtheme 2.1 sociodemographic challenges

Security has been a concern for health professionals, who update their data to maintain and prevent data loss. Therefore, age and educational status influence digital data security practices. A person working in radiology states that *"... data security... adults are more likely to do.... It is a challenge for old ones like professors..."* (Respondent 1). Pharmacy professionals believe that "*...a person who has received special computer training has better access.... the degree level and diploma level vary with the master's level because the study of the course..."* (Respondent 3).

Subtheme 2.2 behavioral challenges

Health professionals are interested in being familiar with digital data security. However, they have little knowledge of digital data security techniques.

The pharmacy team leader said, *"Now this time is a digital age, so everyone has... good attitudes and motivations..."* (Respondent 3). A health information professional said, *"... many professionals... very limited ability to handle information, even back up, the knowledge itself is low, how to handle it, how to manage...* (Respondent 4).

Subtheme 2.3 technological challenges

Health professionals have tried to use digital data from different sources. They were also favorable for using social media and visiting the internet frequently. This made them more vulnerable to digital hackers. A plan and program officer stated that *"...everyone is close to technology and has an opportunity to use it three or four times a day... However, it seems a little to maintain, secure..."* (Respondent 7).

Subtheme 2.4 organizational challenge

Institutions focus on digitization, and some problems exist. These problems included poor IT infrastructure and a lack of experts in digital applications and training. A monitoring and evaluation professional said that *"there is a shortage of infrastructure for many institutions... and then there is the absence of trained professionals in each institution. This is a fundamental problem"* (Respondent 6).

Theme 3 solutions for improving security practices

Healthcare digitalization smooths the flow of health data exchange within the working area and across health institutions. A pharmacy suggested that *"... online theft is on the rise...Additionally, if you do not maintain the privacy setting properly... go online and they will keep track of what I do..."* (Respondent 3). Another person stated, *"... no one has taken ICT special training but...I mean while watching YouTube in its way..."* (Respondent 3). Similarly, the Radiologist stated, "*... many of the things we want to fill are those that require a wireless connection.... to networked... if connecting... the directory will be processed elsewhere..."* (Respondent 1).

Factors associated with digital health security practices

The factors of health professionals toward digital health data security practices are assessed using binary and multivariable logistic regression. Based on this, the findings of this study revealed that computer skills, motivation towards digital data security, attitude, perceived risk, monthly salary, owner ability of smartphone, and sharing digital devices in the working area are identified as non-significant factors for digital health data security practice. Hence, this needs further investigation in different settings using different methods. The significant factors are also presented as follows.

The findings of this study identified age as a significant factor for data security practice; professionals in the 41–45 age category was 89.3% (AOR = 0.107, 95% CI [0.023–0.51]) less likely to practice digital data security. Health professionals with master's degrees were 2.45 (AOR = 2.45, 95% CI [1.138–5.3]), and those with post-master's degrees were 3.87 (AOR = 3.87, 95% CI [1.3–11.5]) times more likely to practice digital data security. The professionals who visited the internet for more than two and a half hours per day were 2.46 (AOR = 2.46, 95% CI [1.45–4.097]) more likely to practice digital data security than those who visited the internet for less than or equal to two hours per day. The other finding indicates that those who received basic computer training were 2.77 (AOR = 2.77, 95% CI [1.62–4.73]) times more likely to practice digital data security than those who did not receive basic computer training. The findings show that those trained in digital data security were 2.14 times (AOR = 2.14, 95% CI [1.1–4.16]) more likely to practice digital data security. Finally, professionals who have knowledge of digital data security were 1.766 times (AOR = 1.76, 95% CI [1.01–3.10]) more likely to practice digital data security than who have not knowledge on data security (Table 4).

Discussion

This study aimed to assess the practice of digital health data security in healthcare settings. Digital security technology is still evolving rapidly [36]. However, this study revealed that 45.0% of health professionals practice digital data security. This result is consistent with those of studies conducted in Australia [37], Canada [23], and the USA [38]. This similarity is due to health care organizations prioritizing the security of health care digitization. However, this contradicts the findings of a study conducted in Europe, which reported 34% [39]. Hence, this may be due to variation in the sampling methods used. Previous studies conducted in specialized teaching referral hospitals in the Amhara region revealed that there was high utilization of health information, accounting for 70.8% of all health information [40]. However, compared with the utilization of health information, the level of digital data security practice is not sufficient. In addition, the qualitative findings also indicated that "*health professionals are not very familiar with digital security technology and do not practice digital data* security *well*" (Respondent 3).

The findings revealed that the 41–45-year-old group had 89.3% lower odds of practicing digital data security than did the 20–25-year-old group. These findings indicate that young adults are more likely to practice digital data security than those aged 41–45 years. This is in line with a study conducted in Australia [37]. Furthermore, this finding is consistent with a study in India in which young people benefit from practicing digital data security to protect themselves from digital threats [35]. In addition, the qualitative findings show that "*young adults are more active in technology and practice digital data security techniques*" (Respondent 2).

The study revealed that master's and postmaster's degree professionals were 2.45 and 3.87 times more likely to practice digital data security, respectively. This finding contrasts with a study conducted in India that showed that educational status was not significant for practicing digital security [35]. This could be due to variation in the samples used to represent the populations. However, the key informant said that the "*…education level influences the practice of digital health data security because the study of the course is different across levels of education…*" (Respondent 3). The findings show that health professionals who visited the internet for more than two and a half hours per day were 2.46 times more likely to practice digital data security. This finding is consistent with a study conducted in India [35]. A key informant also said that "*professionals have an opportunity to use search engines three or four times a day…so, they practice digital data security more*" (Respondent 4).

The findings revealed that those who received basic computer training were 2.77 times more likely to practice digital data security. This result was supported by a key informant, who explained that "*people who have taken special computer training are more likely to practice than others*" (KIP7). The findings also show that trained health professionals in digital data security are 2.14 times more likely to practice digital data security than those not trained in digital data security. However, only 18.66% of the participants were trained in digital data security. This shows that health care management pays little attention to digital data security [15]. As a guideline, standard ISO 27,799 recommends that to prevent the exposure of sensitive data, healthcare personnel should receive affordable security training when they begin working as professionals in a hospital [36].

Finally, health professionals who have knowledge of digital health data security were 76.6% more likely to practice digital data security. However, only 48.76% of the participants have knowledge of digital data security. This result is in line with a previous study in Canada that revealed that knowledge was the strongest predictor of practicing digital security countermeasures [23], and other studies also reported that knowledge related to digital security was determined to play a significant role in the practice of digital security [38]. This finding was supported by a qualitative study in which key informant interviewees explained that "*there was a lack of training due to this, there is lack of knowledge and consequences of the poor practices in digital data security*" (Respondent 4).

Limitations and recommendation

However, the study was triangulated by using a quantitative study supplemented by a qualitative study, and a cross-sectional study was used. This limits the determination of the causal relationships between predictors and outcome variables. A small sample size in some subgroups was the confidence made wide.

The purpose of this study is to improve health professionals' practices in terms of digital health data security. Hence, they update their knowledge of digital security to secure data in the digital space. Specialized teaching hospitals should provide training on the basis of age and educational status with respect to digital data security so that health professionals can develop a safe

Table 4 Bi-variable and multi-variable analysis of factors with the practice of digital data security among health professionals working at a specialized teaching hospital in the Amhara region, Ethiopia (*n*=402)

Variables	Poor practice (%)	Good practice (%)	COR (95%CI)	AOR (95%CI)
Age				
20-25	7 (1.74)	9 (2.24)	1	1
26-30	49 (12.19)	66 (16.42)	1.045 (0.037 - 3.01)	0.901 (0.262- 3.18)
31-35	56 (13.93)	37 (9.20)	0.514 (0.176 - 1.50)	0.430 (0.119- 1.58)
36-40	74 (18.41)	47 (11.69)	0.494 (0.172 - 1.42)	0.330 (0.09 - 1.21)
41-45	27 (6.72)	13 (3.23)	0.374(0.114 - 1.23)	0.107 (0.023- 0.51) ***
46-47	8 (1.99)	9 (2.24)	0.875 (0.222 - 3.45)	0. 288 (0.048- 1.72)
[1]Educational status				
Bachelor	178 (44.28)	115(28.61)	1	1
Master's	28 (6.97)	27 (6.72)	1.493 (0.837 - 2.661)	2.45 (1.138 - 5.3) **
Post masters	15 (3.73)	39 (9.70)	4.024(2.122 - 7.632)	3.87 (1.3– 11.5) **
Monthly salary				
≤ 10,000	160 (39.80)	113 (28.11)	1	1
< 10000-15000	51 (12.69)	46 (11.44)	1.277(0.802 - 2.035)	1.165(0.573- 2.37)
> 15,000	10 (2.49)	20 (4.98)	3.115 (1.42 - 6.832)	1.29 (0.331- 5.01)
Have their own smartphone				
No	81 (20.15)	31 (7.71)	1	1
Yes	140 (34.83)	150 (37.31)	2.8(1.743 - 4.496)	1.07 (0.594- 1.93)
Share digital device in the working area				
No	21(5.22)	10 (2.49)	1	1
Yes	200 (49.75)	171 (42.54)	1.795(0.823 - 3.918)	(1) 24(0.628- (2) 45)
Process health data using digital device daily				
No	46 (11.44)	28 (6.97)	1	1
Yes	175 (43.53)	153 (38.06)	1.436(0.856 - 2.41)	0.79(0.294- 2. 156)
Visit internet per day				
< 2.5 h	126 (31.34)	54 (13.43)	1	1
≥ 2.5 h	95 (23.63)	127 (31.59)	3.119(2.06 - 4.724)	2. 46 (1. 45- 4. 097) ***
Took basic computer training				
No	132 (32.84)	41 (10.20)	1	1
Yes	89 (22.14)	140 (34.83)	5.064 (3.262 - 7.862)	2. 768 (1. 62- 4.73) ***
Trained in digital data security				
No	198 (49.25)	129 (32.09)	1	1
Yes	23 (5.72)	52 (12.594)	3.47 (3.262 - 7.862)	2.14 (1.1 - 4.16) **
Computer skill				
Poor	109 (27.11)	39 (9.70)	1	1
Good	112 (27.86)	142 (35.32)	3.543 (2.278 - 5.511)	1.507 (0.853- 2.66)
Attitude towards digital data security				
Unfavourable	119 (29.60)	66 (16.42)	1	1
Favourable	102 (25.37)	115 (28.61)	2.03(1.36 - 3.03)	0.79 (0.449- 1.391)
Knowledge about digital data security				
Poor	140 (34.83)	66 (16.42)	1	1
Good	81(20.15)	115(28.61)	3.01(2.003 - 4.529)	1.766 (1.01 - 3. 10) **
Motivation to practice digital data security				
Low	120 (29.85)	70 (17.41)	1	1
High	101 (25.12)	111 (27.61)	1.884(1.264 - 2.809)	1.11(0.633- 1.958)
Perceive risk on digital data security				
Low	127 (31.59)	73 (18.16)	1	1
High	94 (23.38)	108 (50.25)	1.99(1.34 - 2.98)	1.617(0.92- 2.821)

[1] **Educational status describes the level of education. These are bachelor degree, master's degree, and post master's degree**

*** p<.01, ** p<.05, * p<.1

digital environment. Finally, the Amhara Regional Health Bureau and Minister of Health should use the findings to guide digital health strategies to harmonize health professionals with digital security while practicing digital health applications.

Implications for health care practice and policy

Digital health data security is the hottest issue, especially in healthcare settings. Knowing digital health security practices strengthens health information systems, especially in resource-limited settings, because there is insufficient evidence on digital health security. This study revealed that healthcare professionals need to practice digital health security through continuous training and knowledge about digital security. This finding also reveals that health professionals have paid little attention to the safety of digital health data. Health policymakers should take this study as input and guide policies on digital health.

Conclusion

A previous study revealed that the digital health data security practices of health professionals were relatively inadequate. The candidate variables of age, education level, time spent visiting the internet, basic computer training, training in digital data security, and knowledge are significant for improving the practice of health professionals toward digital health data security. A qualitative result shows that these obstacles can be solved by providing appropriate digital health data security training, fulfilling the IT infrastructure, and improving the knowledge of health professionals related to digital data security. Therefore, improving and synchronizing health professionals with digital health data security is needed.

Summary table

What was already known on the topic:

- Digital health data security is an essential component for delivering efficient and effective healthcare services.
- Several digital data breaches have involved tracking sensitive health information for monetary importance.
- In resource-limited settings, there is a lack of security-keeping measurement tools to keep healthcare data/information.

What this study added to our knowledge:

- The study indicates that 45% of health professionals have practiced digital health data security tools inappropriately.
- To improve the level of digital health data security practice of health professionals, training, education, and updated knowledge constitute the core of the digital health system.

Abbreviations

AV	antivirus
DDS	digital data security
DHIS2	District Health Information System
EMR	Electronic Medical Record
EpiInfo	Statistical Software for Epidemiology
EHR	Electronic Health Record
HIE	Health Information Exchange
HIMSS	Healthcare Information and Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act
HIS	Health Information System
ICT	Information and Communication Technology
IQR	Interquartile range
KPI	Key personal Interviewee
MoH	Minister of Health
PHR	Personal Health Record
PII	Personally Identifiable Information
STATA	Statistical Software Package
VPN	Virtual Private Network
WHO	World Health Organization
Wi	Fi-Wireless Fidelity

Supplementary Information

The online version contains supplementary material available at https://doi.org/10.1186/s12911-025-02902-2.

Supplementary Material 1

Acknowledgements

First and foremost, I would like to express my deepest gratitude to a compassionate God for caring for me despite my hardships. Next, I would like to express my gratitude to Debre Markos University and the University of Gondar for their contributions, and I want to express my special gratitude to the eHealth Innovation and Research Center program coordinators, Dr. Biniyam Chaklu (Ph.D.) and Mr. Birhanu Fikade (Ph.D. candidate), for their support. Finally, I express my pleasure to Mr. Wondossen Zemene (MPH) and Mr. Nebiyu Demeke (MPH), Mr. Zegeye Regasa (MPH), Mr. Mitiku Kassaw (MPH), Mr. Melaku Molla (BSc. in nursing), and Mr. Gedefaw Belete (BSc. in computer science) and my colleagues for your unwavering help in developing the research.

Author contributions

The authors confirm their contributions to the studies as follows: A.S.G., N.D.M, and W.Z. conceived and designed the study; S.G., B.C.T., B.F.E., and M.K.T. revised the data collection instruments, analyzed, and interpreted the results; and A.S.G., Z.R.W., M.M.S., and G.B.A. wrote the first draft of the manuscript. All the authors reviewed the results and approved the final version of the manuscript.

Funding

Funding was obtained from the Doris Duke Charitable Foundation. This work would not be possible without the financial support of the Doris Duke Charitable Foundation under grant number 2017187. The mission of the Doris Duke Charitable Foundation is to improve the quality of people's lives through grants supporting performing arts, environmental conservation, medical research, and child wellbeing and through the presentation of the cultural and environmental legacy of Doris Duke properties.

Data availability

The datasets generated or analyzed in the current study are available upon reasonable request.

Declarations

Ethics approval and consent to participate

The Institutional Review Board (IRB) of the University of Gondar, College of Medicine and Health Science, the institution of the public health ethical review committee, approved the ethical clearance with ref. no/ IPH/2013/2014/. To collect further information, a formal letter was then sent from the main executives of specialized teaching hospitals to the concerned unit coordinator. Written consent forms were provided with each questionnaire. The respondents were well informed about the purpose, and appropriate informed written consent was obtained from them. In addition, each method was performed in accordance with the relevant guidelines and regulations of the Helsinki declaration.

Consent for publication

Not applicable.

Competing interests

The authors declare no competing interests.

Author details

[1]Department of Health Informatics, College of Medicine and Health Science, Debre Markos University, Debre Markos, Ethiopia
[2]Department of Health Informatics, Institute of Public Health, College of Medicine and Health Science, University of Gondar, Gondar, Ethiopia
[3]Department of Computer Science, Tibebe Gion Specialized Teaching Hospital, Bahir Dar, Ethiopia
[4]Department of Health Informatics, School of Public Health, College of Medicine and Health Science, Wollo University, Dessie, Ethiopia

Received: 5 January 2023 / Accepted: 29 January 2025
Published online: 05 February 2025

References

1. Ethiopia federal ministry of health. Information revolution strategic plan. 2018. Available from: https://extranet.who.int/countryplanningcycles/sites/default/files/public_file_rep/ETH_Ethiopia-National-Information-Revolution-Strategy-Plan_2018-2025.pdf
2. Ethiopia federal ministry of health. Digital health blueprint. 2021. Available from: https://cdhi.uog.edu.et/wp-content/uploads/2024/03/Ethiopian-Digital-Blueprint_V2_16April2021.pdf
3. James T, Nottingham Q, Kim BC. Determining the antecedents of digital security practices in the general public dimension. Inf Technol Manage. 2013;14(2):69–89.
4. Simplilearn. What is digital security: Overview, Types, and Applications explained 2022. Available from: https://www.simplilearn.com/what-is-digital-security-article#what_is_digital_security
5. World bank group. Cybersecurity-trust-fund overview 2022. Available from: https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview
6. Maria G. Ultimate data security checklist 2020. Available from: https://www.msp360.com/resources/blog/data-security-checklist/
7. Chernyshev M, Zeadally S, Baig Z. Healthcare Data breaches: implications for Digital Forensic Readiness. J Med Syst. 2018;43(1):7.
8. Interpol. African cyberthreat assessment report 2021. Available from: https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf
9. Africa's Digital. Cyber Security threat in Africa 2021. Available from: https://liquid.tech/wp-content/uploads/2023/01/LiquidIntelligentTechnologiesCybersecurityReport2021.pdf
10. Taitsman JK, Grimm CM, Agrawal S. Protecting patient privacy and Data Security. N Engl J Med. 2013;368(11):977–9.
11. Khan S, Hoque A. Digital health data: a comprehensive review of privacy and security risks and some recommendations. Comput Sci J Moldova. 2016;71(2):273–92.
12. Healthcare information and management systems society. Cybersecurity in healthcare 2022. Available from: https://www.himss.org/resources/cybersecurity-healthcare
13. Adane K. The current status of cyber security in Ethiopia. Available SSRN 3545189. 2020.
14. Compliancy group. HIPAA wall of shame healthcare data breaches 2022. Available from: https://compliancy-group.com/2021-healthcare-data-breaches/
15. Fernández-Alemán JL, Sánchez-Henarejos A, Toval A, Sánchez-García AB, Hernández-Hernández I, Fernandez-Luque L. Analysis of health professional security behaviors in a real clinical setting: an empirical study. Int J Med Inf. 2015;84(6):454–67.
16. Schaik P. Risk perceptions of cyber-security and precautionary behaviour. Comput Hum Behav. 2017.
17. Khan HU, AlShare KA. Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. J Organizational Comput Electron Commer. 2019;29(1):4–23.
18. Wilkowska W, Ziefle M. Privacy and data security in E-health: requirements from the user's perspective. Health Inf J. 2012;18(3):191–201.
19. Manyazewal T, Woldeamanuel Y, Blumberg HM, Fekadu A, Marconi VC. The potential use of digital health technologies in the African context: a systematic review of evidence from Ethiopia. Npj Digit Med. 2021;4(1):125.
20. Oumer A, Muhye A, Dagne I, Ishak N, Ale A, Bekele A. Utilization, determinants, and Prospects of Electronic Medical Records in Ethiopia. Biomed Res Int. 2021;2021:2230618.
21. Halevi T, Memon N, Lewis J, Kumaraguru P, Arora S, Dagar N, et al. editors. Cultural and psychological factors in cyber-security. Proceedings of the 18th international conference on information integration and web-based applications and services; 2016.
22. Lubua E, Semlambo A, Mkude C. Factors affecting the Security of Information Systems in Africa: A literature review. Univ Dar es Salaam Libr J. 2023;17:94–114.
23. Hull MS. Factors affecting Secure Computer Behaviour. Carleton University; 2015.
24. Dadimos H. Ethiopia - Data protection overview 2021. Available from: https://www.dataguidance.com/notes/ethiopia-data-protection-overview
25. Healthcare information and management systems society. Healthcare Information and Management Systems Society(HIMSS). Healthcare Cybersecurity Survey 2021. Available from: https://www.himss.org/resources/2021-himss-healthcare-cybersecurity-survey-report
26. John Snow I, JSI, Ethiopia Launches Digital Health Innovation and Learning Center. 2020| News, August 6th. Available from: https://www.jsi.com/ethiopia-launches-digital-health-innovation-and-learning-center/
27. Hindawi. Privacy and Security in eHealth Systems 2022, Apr 01. Available from: https://www.hindawi.com/journals/jhe/si/373027/
28. Gopal D, Hariharan U. Safety measures for EHR systems. 2019. pp. 249–66.
29. George Antonyo. Evaluating Usability of Security Mechanisms of E-Health Applications: Cases from Ethiopia. Addis Ababa University (AAU) Institutional Repository 2020:69.
30. Naing L, Nordin RB, Abdul Rahman H, Naing YT. Sample size calculation for prevalence studies using scalex and ScalaR calculators. BMC Med Res Methodol. 2022;22(1):209.
31. Dagnew E, Woreta SA, Shiferaw AM. Routine health information utilization and associated factors among health care professionals working at public health institution in North Gondar, Northwest Ethiopia. BMC Health Serv Res. 2018;18(1):685.
32. Howard DJ. Development of the cybersecurity attitudes scale and modeling cybersecurity behavior and its antecedents. University of South Florida; 2018.
33. Cassidy R. Attitudes towards digital health technology: Introducing the Digital Health Scale. medRxiv. 2021:2021.09.03.21262482.
34. Adedeji P, Irinoye O, Ikono R, Komolafe A. Factors influencing the use of electronic health records among nurses in a teaching hospital in Nigeria. J Health Inf Developing Ctries. 2018;12(2).
35. Balaji J. Knowledge, attitude and practice study on awareness and preventing cyber threats among the electronic devices used by the doctors of government medical college Vellore, Tamil Nadu, India. Int J Community Med Public Health. 2020;7(1):283.
36. International standard organization. Information security management in health using ISO/IEC 27002 2016. Available from: https://www.iso.org/standard/62777.html
37. Pattinson M, Butavicius M, Parsons K, McCormac A, Calic D, editors. Factors that Influence Information Security Behavior: an Australian web-based study. Human aspects of Information Security, privacy, and trust; 2015 2015//; Cham: Springer International Publishing.
38. Rajivan P, Moriano P, Kelley T, Camp LJ. Factors in an end user security expertise instrument. Information & Computer Security; 2017.

39. Gallego-Arrufat M-JG-A, Torres-Hernández NT-H, Pessoa TP, Gallego-Arrufat M-J, Torres-Hernández N, Pessoa T. Competence of future teachers in the digital security area. Comunicar Media Educ Res J. 2019;27(2).

40. Tesfa GA, Kalayou MH, Zemene W. Electronic Health-Information Resource utilization and its Associated factors among Health professionals in Amhara Regional State Teaching hospitals, Ethiopia. Adv Med Educ Pract. 2021;12:195.

Publisher's note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.