






Health Professionals' Ethical, Security, and Patient Safety Concerns Using Digital Health Technologies: A Mixed Method Research Study

Health Services Insights
Volume 17: 1–12
© The Author(s) 2024
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/11786329241303379



Nathan Kumasenu Mensah^{1*}, Godwin Adzakpah^{1*}, Jonathan Kissi¹, Hannah Taylor-Abdulai², Stephen Benyi Johnson¹, Princilla Awudu Agbeshie¹, Christabell Opoku¹, Jessica Abakah¹, Emmanuel Osei¹, Ama Yeboaa Agyekum¹ and Richard Okyere Boadu¹

¹Department of Health Information Management, School of Allied Health Sciences, University of Cape Coast, Cape Coast, Ghana. ²Department of Physician Assistant Studies, School of Allied Health Sciences, University of Cape Coast, Cape Coast, Ghana.

*These authors contributed equally to this work.

ABSTRACT

BACKGROUND: Digital Health Technologies (DHTs) offer numerous health benefits but raise ethical and security concerns about patient health data among health professionals due to potential security breaches. This study explores the ethical, patient safety, and security issues concerning healthcare professionals using DHTs in hospitals in Ghana.

METHODS: The study used a mixed method design, including a descriptive survey and in-depth interviews with health professionals in 3 tertiary hospitals, between July and September 2022, with thematic content analysis using QSR NVivo 12 software. The descriptive survey was analyzed using Stata 15 to produce percentages, means, and standard deviations.

RESULTS: A total of 369 health professionals participated in the study. Disclosure of health data on DHTs without consent from patients 299 (81.03%) was the most frequently mentioned concern. The most often raised concern was the disclosure of the patient. Overall, 298(80.76%) health professionals worried about safety issues relating to the use of the DHTs. On occasion, staff members neglect to log out of the system, which compromises all the security measures in place. Other factors such as system unavailable due to unplanned shutdown affected patient safety.

CONCLUSION: Health professionals are concerned about patient information confidentiality and security. They believe staff access to patient information should be on a “need-to-know basis,” and safety policies be periodically updated to prevent human behavior from compromising security measures.

KEYWORDS: Digital health technology, ethical issues, security, patient safety, health professionals, Ghana

RECEIVED: June 12, 2024. **ACCEPTED:** November 8, 2024.

TYPE: Original Research

FUNDING: The author(s) received no financial support for the research, authorship, and/or publication of this article.

DECLARATION OF CONFLICTING INTERESTS: The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

CORRESPONDING AUTHOR: Godwin Adzakpah, Department of Health Information Management, School of Allied Health Science, University of Cape Coast, Cape Coast, Ghana. Post Office Box PMB, Cape Coast. Email: godwin.adzakpah@ucc.edu.gh

Introduction

There is a growing urgency worldwide to address the ethical, patient safety and security concerns associated with the usage of Digital Health Technologies (DHTs).^{1,2} Maintaining the confidentiality, integrity, and availability of digital health data significantly influences its security. Since multiple parties are involved in generating patient information, there is a risk that the confidentiality or privacy of the information generated may be compromised.³

Ethical concerns in the healthcare sector primarily revolve around patient privacy and confidentiality. Privacy refers to a patient's right to control how their medical information is used, which is expressed through their consent.^{3,4} Safeguarding this right is essential to preserving patient trust and health professionals are obligated to ensure that only authorized individuals can access sensitive information. This responsibility reflects the respect that healthcare professionals must show for the trust

patients place in them and the healthcare facilities.⁵ Any unauthorized access to patient data not only undermines this trust but can also result in legal consequences for the healthcare providers.^{2,6}

DHTs, such as Electronic Health Records (EHRs), have revolutionized healthcare by increasing efficiency and reducing medical errors.^{7–9} However, these systems have introduced new ethical concerns related to the privacy, confidentiality and safety of patient data. This has led to a higher risk of data breaches and unauthorized access to health data.¹⁰ To address these risks, regulations such as the Data Protection Act 2012 (Act 843) in Ghana and the Health Insurance Portability and Accountability Act (HIPAA) in the USA, are in place to ensure that healthcare professionals uphold the integrity of patient data within DHTs.¹¹

Security remains a top priority when using DHTs, as these systems store vast amounts of sensitive health data that are



Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (<https://creativecommons.org/licenses/by-nc/4.0/>) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

highly vulnerable to breaches. The increased adoption of DHTs has exposed healthcare systems to a greater risk of cyber-attacks, unauthorized access, and data breaches.¹² Such breaches not only compromise patient confidentiality but can also lead to identity theft, financial losses, and compromised patient safety.¹³

In addition to external threats, internal security risks, such as disgruntled workers or improper data handling, further complicate the security challenges. Human errors, including password sharing or failure to follow security protocols, frequently contribute to significant breaches.^{14,15} To address these challenges, healthcare organizations must implement robust access control measures, ensure regular software updates, and strengthen encryption methods.⁵

Moreover, compliance with data protection regulations is critical. Non-compliance can lead to legal consequences, including fines and reputational damage,¹¹ emphasizing the importance of ongoing staff education on security best practices and the need to continually update and enhance security systems.^{16,17} Proactive measures to protect DHTs from internal and external threats are essential to safeguarding patient information in an increasingly digital healthcare environment¹⁴

A study by Lee¹⁷ underscored that healthcare workers pose a major threat to the confidentiality of patient information.¹⁷ The majority of security breaches involving DHTs stem from human error, underscoring that human factors remain the weakest link in information security.^{10,17,18}

The implementation of DHT raises significant safety concerns, particularly regarding the potential for clinical errors. While DHTs like EHRs improve healthcare delivery, they also expose systems to risks such as data entry mistakes and system failures, which can disrupt patient care.¹³ Inadequate design or poor system interoperability can further hinder effective use, increasing the likelihood of errors that could compromise patient safety.¹⁹

In some regions, particularly in low- and middle-income countries (LMICs), challenges such as outdated equipment, unstable power supplies, and unreliable internet services exacerbate safety risks.¹⁹ Healthcare workers in these areas may resort to using personal devices, which introduces additional vulnerabilities and threatens the safety and confidentiality of patient information.^{6,20,21}

To effectively safeguard patient information, health organizations must establish and continually enhance security measures that address the evolving threats and vulnerabilities associated with the use of DHTs.^{14,22,23} This includes developing and enforcing policies to manage both internal and external threats, providing ongoing education and training on security best practices, and investing in more secure, user-friendly, and interoperable technologies.^{24,25}

While most studies on DHTs in LMICs have focused on their implementation and adoption, more research is needed on ethical and security perspectives.²⁶ Understanding the

challenges healthcare professionals in LMICs face when using DHTs is vital for promoting the adoption and implementation of these technologies, which have struggled to gain momentum in such settings. Evaluating and enacting specific laws governing the use of technology in healthcare is essential to addressing these concerns. To this end, the study aims to investigate the ethical, security and safety issues faced by healthcare professionals using DHTs in hospitals in Ghana. The specific objectives are to investigate the privacy, confidentiality, security, and patient safety issues confronting healthcare professionals using DHTs to provide services, to identify significant technological and non-technological factors that concern healthcare professionals using the DHTs, and to propose strategies to mitigate these concerns.

Methodology

All methods in this research were carried out following the Strengthening of Reporting of Observational Studies in Epidemiology (STROBE) guidelines for reporting a cross-sectional study.²⁷

Study design

This study employed an exploratory parallel mixed-method approach that combined qualitative and quantitative techniques to investigate the ethical, security, and safety issues of concern to healthcare professionals using DHTs and to determine other significant factors of concern to health professionals using DHTs in selected hospitals in Ghana. The purpose was to obtain different but complementary perspectives to answer the research objectives,²⁸ clarify gray areas, and gather experiences to enrich the findings.²⁹ Qualitative research describes and captures the feelings, experiences and perceptions of individuals on the investigated issues through words. We conducted In-depth Interviews (IDIs), which is a highly explorative qualitative design.²⁹ For the quantitative part, we used a survey tool. Both parts received equal attention, with data collected concurrently and analyzed independently. The results were presented separately, but integration occurred during the interpretation to generate a comprehensive understanding of participants' concerns about using DHTs in hospitals.^{4,28,30} The measurement strategies employed to address each research objective are shown in Table 1.

Study site

The investigation was conducted in 3 tertiary hospitals in Ghana, referred to as Facility A, B, and C to maintain anonymity. Hospital A is a 600-bed facility situated in the Central region. It serves as 1 of 3 main hospitals serving the metropolis. Hospital B is a 650-bed facility located in the capital of Ghana, which offers quaternary-level health services. Hospital C has a bed capacity of about 800 and serves metropolitan areas with a population of about 2 million in the Ashanti region. All 3

Table 1. Measurement strategies used to address respective objectives.

NO	OBJECTIVE	MEASUREMENT STRATEGY
1.	To investigate privacy, confidentiality, security, and patient safety issues confronting healthcare professionals using DHTs to provide services	Qualitative/ Quantitative
2.	To identify significant technological and non-technological factors that concern healthcare professionals when using the DHTs	Qualitative/ Quantitative
3	To suggest strategies to mitigate the concerns of healthcare professionals using DHTs	Qualitative

facilities offer both general and specialized outpatient and inpatient care services. These health facilities were selected because they used the Lightwaves Health Information system, a type of DHT accessible to the researchers.

Targeted population

The study population included healthcare professionals such as doctors, nurses, biomedical scientists, pharmacists and other allied health professionals.

Quantitative

Sample size, sampling, and sampling procedures

The study's quantitative component used Slovin's formula to determine the sample size. The estimated total population of health professionals who use the DHTs in hospitals is about 2000.

Using the formula:

$$n = \frac{N}{(1 + N \times e^2)}$$

where N is the population size (N = 2000)

and e is the margin of error (with a 5% margin of error), a sample size of 367 was determined which includes a 10% provision for non-response. Consequently, 369 participants were recruited through a list of DHT users obtained from the systems administrator of the respective hospitals, which was used to select the respondents at random. Table 2 shows the distribution of the sample per facility.

Inclusion and exclusion criteria

Inclusion criteria

The study recruited healthcare professionals who work in the selected hospitals and have been using DHTs for at least 6 months.

Exclusion criteria

Excluded from the study were healthcare professionals who do not use DHTs and had less than 6 months of working experience in the hospitals.

Table 2. Distribution of samples per health facilities.

FACILITY	THE POPULATION OF DHT USERS	EXPECTED SAMPLE	ACTUAL SAMPLE	PERCENT
A	808	148	149	40.4
B	542	100	100	27.1
C	650	119	120	32.5
Total	2000	367	369	100

Data collection instruments and procedures. The quantitative and qualitative data were collected from respondents between July and September 2022. The data collection instruments were adapted and modified for the study.⁴ A pretest was conducted among 15 healthcare professionals including doctors, nurses, and other allied health professionals, after the training to assess the performance of the data collectors and clarify any ambiguities. This process helped the authors finalize the survey instruments before actual data collection began.

A list of DHT users was obtained from the systems administrator of the respective hospitals and used to select the respondents at random. A pretested self-administered structured paper questionnaire was given to the participants selected at random to complete. This was done to avoid disruption in routine health activities. The questionnaire consisted of closed-ended questions. The close-ended question captured information about the demographic characteristics of the healthcare professionals and on study constructs in the form of Likert scale. Each item of the Likert-type questions assessed participants' concerns using a Likert-type scale which ranged from 1 (not concerned at all) to 5 (very concerned).⁴ The questionnaire addressed several topics including privacy (3 questions), confidentiality (2 questions), access security (4 questions), physical security (4 questions), and administrative security (4 questions). Safety concerns were in 2 parts, non-technological and technological concerns, with the former comprising 4 questions and the latter 14 questions. The questionnaire was adapted from an earlier study and modified by adjusting the text to focus on healthcare professionals.⁴

Data management and data analysis. The quantitative and qualitative components of the data were analyzed individually, and the results were later integrated, but integration occurred during the discussion.

Before entering the survey questionnaires in an electronic data-capturing tool designed using EpiData 3.1 software, each one was checked for accuracy, completeness, and eligibility. The data screens had built-in safeguards to reduce data entering errors. Each completed questionnaire received a unique identification number for quality control and recall.

The quantitative data was exported and then translated to STATA version 15 for analysis. Cronbach's alpha coefficient

was calculated to determine the overall internal reliability of the survey tool. Cronbach's alpha was also computed for each of the study's dimensions. To describe the respondents' concerns about ethical, security, and safety issues related to DHTs, descriptive statistics (including frequencies, percentages, means, and standard deviations) were utilized. For example, the privacy concern was computed by generating the mean of individual responses under each construct. An average for the 5-point Likert scale was then calculated for each item by summing all the number of responses divided by the total number of respondents for each item. The variables "Not concerned at all," "Not concerned" and "Neutral" responses in the questionnaire were combined as "Not concerned", whereas "Somewhat Concerned" and "Very Concerned" were combined as "Concerned." Using a binary categorization, the 5-point Likert scale was categorized for each item as "Not concerned" < 3.5 and "Concerned" \geq 3.5.

Qualitative

In-depth interviews

A purposive sampling approach was used to select respondents in the qualitative component, allowing the researchers to select the participants who could provide detailed information about the topic under investigation. This is a widely used approach in qualitative studies to solicit information.²⁹ Therefore, we used a purposive sampling technique to select 3 health facilities and health professionals capable of providing rich information to clarify ambiguities. The selected participants comprised healthcare professionals, such as doctors, nurses, biomedical scientists, pharmacists, and other allied health professionals who had been working in these hospitals and using DHTs for more than 6 months before the start of the study. We assumed that each facility used a different DHT, each with its unique characteristics.

Data collection instruments and procedures

A semi-structured interview guide was used to explore the views of the respondents on the study objectives. The interview guide was developed based on the study objectives and themes derived from the adapted questionnaire. The questions were intended to elicit the thoughts of healthcare professionals on ethical, safety, and security issues around the use of DHTs. The interview questions centered on privacy, confidentiality, security, and patient safety concerns.⁴

A group comprising final-year undergraduate students (SBJ, PA, and AYA) conducted face-to-face interviews in English. These individuals had undergone 2 days of training in qualitative research techniques and understood the importance of the questions. Before conducting the interviews, the interviewers obtained the required administrative permission from the facility heads. They then introduced themselves to potential participants and explained the purpose of the study. Written

informed consent was obtained from all participants who agreed to take part in the study. This approach was chosen to encourage open-ended conversations between the interviewers and participants, allowing for the uncovering and exploration of important information that could not be captured through a quantitative approach.

An interview guide consisting of 20 questions with probes was used to clarify any gray areas. The interviews were conducted in a serene environment within the hospitals and were recorded. Interviews lasted about 35 minutes. A total of 62 interviews were conducted, with data collection continuing until no new remarks were emerging, at which point we considered that data saturation had been reached.

Data management and analysis

Content analysis was used to identify the themes.³¹ We developed a codebook based on the interview guide and the original research questions. Using NVivo 12 qualitative analysis software, the data was organized according to themes. The themes were discussed with the co-authors for relevance.

Validity, reliability, and rigor

To enhance rigor in the qualitative data analysis, 2 persons (SBJ and PA) transcribed the interviews independently. The first author read through and edited the transcripts, making sure that the meanings were not lost. To ensure unbiased data interpretation, the first and second authors coded the data, which was then reviewed by the co-authors. The coding method included a rigorous assessment of each transcript, and the data was classified into themes. To obtain comprehensive data, we employed methodological triangulation through the administration of surveys and IDIs. To guarantee thorough data triangulation, we gathered information from multiple hospital departments. Through the independent analysis of the data by the researchers, investigator triangulation was accomplished. The findings were presented as narratives and supported by relevant quotes selected from the data.

Results

Quantitative

Socio-demographic characteristics of healthcare providers. A total of 369 healthcare professionals out of 450 participated in the study representing an 82% response rate. The characteristics of the respondents are summarized in Table 3. A total of 369 respondents from 3 selected health facilities took part in the study. The majority of the respondents were female, accounting for 55.56% (205), and the majority of the health professionals, 66.12% (244) were between the ages of 25 and 35.

Scale and test for reliability. Cronbach's alpha was used to determine scale reliability, and .7 was considered sufficient.³²

Table 3. Socio-demographic characteristics of healthcare providers.

CHARACTERISTICS	NUMBER OF RESPONDENTS	PERCENT
	N = 369	
Age-group		
Below 25 y	41	11.11
25-34 y	244	66.12
35-44 y	72	19.51
Above 45 y	12	3.25
Gender		
Male	164	44.44
Female	205	55.56
Education level		
PhD/MSc	48	13.01
BSc	200	54.20
HND	11	2.98
Diploma	99	26.83
Other (specify)	11	2.98
Employment status		
Full-time	299	81.03
Part-time	14	3.79
Temporary/Casual	56	15.18
Total years of service		
Below 1 y	61	16.53
1-5 y	214	57.99
6-10 y	61	16.53
11-15 y	19	5.15
Above 15 y	14	3.79
Total years of practice		
Below 1 y	83	22.49
1-5 y	214	57.99
6-10 y	50	13.55
11-15 y	16	4.34
Above 15 y	6	1.63

The data is presented as numbers and percentages. N is the total number of participants in the survey.

Therefore, an alpha value of .95 for the total scale is considered excellent. Cronbach's alpha coefficients for each study construct range from .72 to .93, except for privacy (.67) and confidentiality (.69) (Table 4).

Table 4. Descriptive statistics, scale and test for reliability.

CONSTRUCT	NUMBER OF ITEMS	CRONBACH'S ALPHA
Privacy concerns	3	.67
Confidentiality concerns	2	.69
Security concerns	4	.78
Physical security concerns	4	.76
Administrative security concerns	4	.79
Non-technological safety concerns	4	.72
Technological safety concerns	14	.93
Overall	35	.95

Ethical, Security, and Patient Safety Concerns of Health Professionals Using the DHTs

Health professionals' concerns about privacy, confidentiality, security, and safety of patient information when using the DHTs to provide service are outlined in Table 5. The overall mean score for privacy, confidentiality, security (both physical and administrative), and non-technological and technological safety concerns was higher than 4.0. This indicates that the health professionals were concerned about how patient information was handled in the DHTs.

The majority (n = 297, 80%) of the respondents expressed concerns about the privacy of patient information in DHT. Disclosure of DHT-related health data without the patient's written consent was the most (n = 299, 81%) often selected privacy-related item. The least selected concern (n = 266, 72%) regarding privacy was whether DHTs restrict patient's access to their medical records.

The majority of participants (n = 282, 76%) expressed concern about confidentiality. The most selected confidentiality-related concern (n = 305, 83%) was the inappropriate disclosure or exchange of identifiable, sensitive patient information through DHTs with individuals outside the medical profession. The least selected concern (n = 289, 78%) was the inappropriate disclosure or exchange of such information with other medical professionals.

Regarding access security, most health professionals (n = 291, 79%) expressed security concerns about access to patient information in the DHTs. The most (n = 297, 81%) selected item of concern in this category was inappropriate access to all possible users' stored data due to a lack of control of the facility (clerks, billings, and appointments). Inappropriate access to stored data by authorized staff (eg, through sharing login credentials and access keys) was reported by 292 participants (79%).

Among the 4 items related to physical security concerns that could potentially risk patient information, the majority (n = 318, 86%) of health professionals expressed the greatest concern over

Table 5. Ethical, security, and patient safety concerns of health professionals using the DHTs.

CODE	STATEMENT	MEAN (STANDARD DEVIATION)	NOT CONCERNED N (%)	CONCERNED N (%)
	Privacy concerns	4.14 (0.85)	72 (19.51)	297 (80.49)
	Confidentiality concerns	4.26 (0.93)	87(23.58)	282 (76.42)
	Access security concerns	4.19 (0.82)	78 (21.14)	291 (78.86)
	Physical security concerns	4.31 (0.77)	57 (15.45)	312 (84.55)
	Administrative security concerns	4.17 (0.80)	82 (22.22)	287 (77.78)
	Non-technological safety concerns	4.11 (0.73)	85 (23.04)	284 (76.96)
	Technological safety concerns	4.12 (0.75)	71 (19.24)	298 (80.76)

The questionnaire was adapted from Ban Issa but was modified to focus on healthcare professionals.⁴

the lack of secure passwords, access, and workstation locks. In contrast, the least concern (n=312, 85%) was about unanticipated system failure or power outage without backup.

In the category of administrative security concerns, the overall score was (n=287, 78%). Health professionals were most particularly concerned, with (n=297, 81%) worrying about whether medical and non-medical staff receive adequate training on DHT security-related issues. On the other hand, misuse of data for scientific purposes was the least concern, with (n=282, 76%) citing it as an issue.

Patient safety concerns were classified into non-technological and technological safety. In total, (n=284, 77%) of health professionals concerns was related to non-technological issues. Within this category, their main concern (n=294, 80%) was improper error reporting among healthcare professionals, while the least concern (n=269, 73%) was the absence of an audit or staff log documenting frequent system errors.

In the category of technological safety, a total of (n=298, 81%) health professionals expressed concerns about safety issues related to the use of the technology. Specifically, most of the health professionals (n=319, 86%), were concerned about the reliability of the technology (ie, unplanned shutdown), whilst the least technological safety concern (n=263, 71%), was about functional appropriateness, or the extent to which features in software are accurate, full, and suitable.

Qualitative

In-depth interviews results

The analysis of the transcribed interviews yielded 6 thematic categories with various subthemes, which are summarized in Table 6 and discussed in the findings section.

Privacy

DHTs enhance the privacy of patient information. Healthcare professionals using DHTs perceived them to have enhanced the privacy of patient information compared to paper folders. Furthermore, participants mentioned that not everyone could

access patient information when using DHTs, as only authorized staff have access to the system. Some respondents expressed their views as follows:

“There is some information that only medical practitioners can see and there is some that only nurses can see and so [. . .], I think for now it is not everything that is accessible to everybody” (IDI-14 with a medical officer, hospital B)

Patients' right to information

Most health professionals believe patients should have access to their information to facilitate decision-making.

“It's very important for the patients to know what is wrong with them at a particular given time therefore, I feel it is their right and responsibility to know what is wrong with them and also what is been entered into the system for them” (IDI-14 with a medical officer, hospital B)

However, the DHTs system does not offer patients access to their information. Some health professionals fear that knowledge of the information could harm patients. Participants were of the view that information should be released to patients on a 'need to know basis. Their views were echoed as:

“Patient having access to their information is very very very bad because, when patients know their information, [. . .] it can be harmful to the patient. For example, if the patient has HIV/AIDS or any type of sickness, the person can even kill him/herself” (IDI-11 with a nurse, hospital C).

DHTs influence patients' right to consent

Many healthcare providers assume that patients automatically waive their right to consent when they enter a healthcare facility for treatment. This is because they believe that patients are aware the facility operates DHTs and have therefore given their consent for their information to be recorded.

“. . . if a patient comes to see me then the understanding is that there is a contract between the patient and the hospital; and so,

Table 6. Main themes and sub-themes on ethical, security, and safety concerns of health professionals using DHTs, and how to mitigate these concerns.

MAIN THEMES	SUB-THEMES
Privacy concerns	DHTs enhance the privacy of patient information
	Patients' right to information
	DHTs influence patients' right to consent
Confidentiality concerns	Health workers are knowledgeable about confidentiality
	How confidentiality is ensured in DHTs
	DHTs facilitate staff breach of confidentiality
Access security concerns	DHTs enforce access security control
Physical security concerns	Physical access restrictions
Administrative security concerns	Security breaches of patient information
Safety (Technical related factors of concern)	Impact of unplanned shutdown
	Use of personal devices
	External threats
Safety (non-technical related factors of concern)	Perceived threat from staff
	Mistrust of DHT data
	Lack of documented policies
Suggestions and strategies to mitigate concerns	Provision of targeted training
	Frequent software updates
	Provision of backup storage
	Provision of adequate devices
	Provision of access on a "need to know basis"

there is no need for me to [seek] consent from them to use their data; because that consent has been sought by virtue of the fact that 'you have come to the hospital'." (IDI-14 with a medical officer, hospital B)

However, other health professionals held divergent views and opined that patient consent is sought before the commencement of the care process. They added that this encourages patients to give them accurate information. Participants' views were expressed as:

"Before we take data from the patient, we, by all means, seek patient consent, what you need that information for. . .we seek by telling the patient the reason for taking that data, this also helps them to give us accurate data." (IDI-10 with a medical officer, hospital A)

Confidentiality

Health workers are knowledgeable about confidentiality. Health professionals are well aware that sharing or utilizing patient information without their consent is ethically and legally

wrong. The respondents emphasized that patient information could only be disclosed when written consent or an official request for such information was made.

"...our job ethics states clearly that, aside from the patient no other person should know the condition or should get any other information of the patient without the consent of the patient" (IDI-5 with HIM officer, hospital C).

How confidentiality is ensured in the DHTs. Confidentiality in DHTs is maintained through user credentials and password controls. These credential controls come in different access levels, which help determine who can access specific information. This is done to prevent unauthorized access to patient information.

"...before you access the system, you probably need a password. It depends on your level in this facility and the kind of access you have into the system" (IDI-6 with Medical Officer Hospital C)

DHTs facilitate staff breach of confidentiality. Health professionals have concerns regarding the maintenance of privacy

and confidentiality of patient information. In their view, it is quite challenging to keep patient information confidential, especially from staff belonging to different departments. They opined that staff access is not limited to specific departments, and everybody can access patient information from across any department.

“When it comes to the privacy aspect, it is quite challenging in a way [. . .] Somebody from a different department can see whatever you keyed in for a particular patient which I think it shouldn't be. . .” (IDI-13 with a nurse, hospital B)

Furthermore, there is a possibility that medical personnel not directly involved with the patient may access patient information. This poses a higher level of concern among healthcare providers.

“I wish that patient information should be limited to only the people [staff] who are taking care of the patient. So, if the patient is admitted to one unit, other staff from other units shouldn't have access to patient information unless the patient goes to such unit for care. (IDI-8 with a nurse Hospital C)

Some staff can disclose patient information through unprofessional conduct, which raises concerns for health workers as all authorized staff have access to patient information in the DHTs.

“Some of our colleagues [. . .] I mean their mouth don't close so when you put patient information on the EHR, some of the nurses, they can even disclose it by sharing it among themselves. . .” (IDI-11 with a nurse, hospital C)

Security

DHTs enforce access security control. Patient information in the DHTs is protected through different methods such as physical and administrative restrictions, or software access restrictions. A common method is the use of login credentials, including usernames and passwords, to control access. Access privileges are assigned at different levels.

“. . .security of information is always enforced in our EHR system [. . .] everybody has a user name and a password; so, you don't see beyond your access level. Only those that work directly on the information have the highest access level” (IDI-1 with a Public health officer, hospital B)

Physical access restrictions. Physical access was limited to staff common areas, such as nurses' stations where computers are stationed.

“Physical access to the computers is restricted [. . .], and areas with computers are locked and if it is not locked like the nurses' station, there are security cameras all around [. . .] to see who comes to use the system” (IDI-12 with a medical officer, hospital B).

Additionally, several administrative policy measures have been implemented to restrict unauthorized access to patient data/information stored in the DHTs. These measures include restricting the use of personal devices such as pen drives and phones on the hospital network system to prevent contracting viruses.

“. . .they do not allow personal devices like phones and pen drives to protect against the risk of viruses.” (IDI-12 with a medical officer, hospital B)

“Pen drive ports are blocked so that no one can insert a pen drive that can bring the virus into the system” (IDI-9 with a medical laboratory scientist, hospital B)

Security breaches of patient information. Although there are several security protocols implemented to safeguard patient information within the system, security breaches unfortunately still occur. A significant breach that was identified was influenced by behavioral factors, which pose a major concern. On occasion, staff members neglect to log out of the system after using it, which puts the patient's confidential information at risk and compromises all the measures that were taken to protect it.

“My only concern is that whoever works on a system must remember to log out, so other people using the same machine wouldn't get information of the patient, because patient confidentiality is very necessary.” (IDI-6 with IT officer, hospital C)

Other factors of concern to healthcare professionals

Safety (Technology related factors of concern).

Among the technological-related factors, unplanned shutdown had the most debilitating effect on patients, health professionals, and work and was of much concern to health professionals.

Impact of unplanned shutdown

Participants expressed concern about the impact of unplanned system shutdowns on both patients and workflow. They noted that such shutdowns caused delays and brought the entire work process to a halt, which in turn caused unnecessary stress to patients for hours.

“My concern is that unplanned shutdown slows down [and] delays the work. And not only the work alone, it brings a whole work to halt. . .people in the queue will not move, they will have to wait till its restored for provision of care to continue. . .” (IDI-6 with a public health nurse Hospital A)

Unplanned shutdowns impacted negatively by increasing patient waiting time and reduced productivity. When the system goes down, information on services rendered but not recorded in the system are lost.

“It [unplanned shutdowns] can reduce productivity and also patient waiting time is prolonged. . .” (IDI-7 with an HIM officer, hospital A)

“. . .when there is an unexpected system shutdown and all the information is not saved or backup, then there is a threat of losing patient’s information” (IDI 15 with Nurse, Hospital A)

Apart from causing security breaches and frustration, unplanned shutdowns disrupted work processes, leading to negative impacts on patients and decision-making.

“Even we can’t access our previous diagnosis or anything; so, we can’t make any meaningful decision, unlike the manual system. So, we have to stop [until] the system is back then we resume” (IDI-6 with public health nurse, hospital A).

System shutdowns can have unforeseen consequences on decision-making and patient care continuity. It posed a potential risk to patient data since unsaved information is lost or cannot be referenced. Any delay in administering medication due to a system breakdown can further complicate the patient’s health.

“. . .when there is an unexpected system shutdown and all the information is not saved or backup, then there is a threat of losing patient’s information” (IDI 15 with Nurse, Hospital A)

“. . .it doesn’t make the work smooth. . .clinically if patients don’t receive their medication on time due to the unplanned shutdown, it complicates their health. . .so sometimes at emergency unit, when it happens like that, we have to [rely]on our expertise to save the patient first. . .” (IDI-14 with a clinical pharmacist, hospital A)

Use of personal devices. The use of personal devices by some healthcare workers to provide services was seen as a potential threat to patient information security. Due to inadequate equipment, some healthcare workers use their own devices like iPads and laptops. Although this was noted in only 1 facility, staff expressed concern that patient information security could be compromised if such devices were lost or accessed by unauthorized individuals:

“Yes, as far as the use of the DHTs is concerned, especially, like I said when the device used is a personal one, that is the fear that comes, what about the person accidentally or intentionally loses the phone and a non-clinical person chance upon it” (IDI 11 with a midwife hospital C)

External threats. Health workers also expressed concerns about potential threats to patient information from hackers.

“The only threat is the hackers. When there are loopholes in the system the hackers make use of this vulnerability to have access to patients’ information” (IDI 12 with medical officer hospital B).

Safety (non-technological related factors of concern)

Perceived threat from staff. Respondents noted that staff with custody and access to patient information posed a potential threat to patients’ information. This is how they put it:

“The perceived threat to [patients’ information] is the health workers ourselves since we have a lot of patient information in our custody. . .” (IDI 6 with public health nurse hospital A)

Mistrust about DHT data. Health workers expressed concerns about trusting the system, as they feared that patient information could be manipulated. This is how a participant puts it:

“. . ., I believe figures or data in the EHR system can be manipulated” (IDI-2 with a pharmacist, hospital C).

Lack of documented policies. Data integrity policies are to ensure regulatory compliance and safeguard the use of patient information in the EHR system. However, a large number of health professionals were unaware of these data integrity policies. The majority of respondents expressed limited or no knowledge about the availability of such data integrity policies within their facilities. Some respondents were emphatic that no such policies existed:

“Well, I have not sighted on any data policy” (IDI-1 with a HIM officer, hospital C)

“. . .in terms of policies, as I said, I will not be able to spell it out because I haven’t seen them, okay.” (IDI-1 with a medical officer, hospital A)

Suggestions and strategies to mitigate concerns. Several suggestions were made to improve the privacy, confidentiality, patient safety and security of patient information in DHTs. One way to relieve health professionals’ concerns about DHTs was to provide staff training.

Provision of targeted training. Some participants advised providing targeted training for specific areas including privacy, confidentiality, safety, and security, to safeguard patient information.

“We received training on the usage, but when it comes to security, how to protect client information, we didn’t receive any training, . . ., so if we receive training on security, confidentiality and other things, it would help” (IDI 13 with a nurse, hospital C)

Frequent software updates. During the discussion, some participants suggested that the system needed to be updated to fix the loopholes and enhance its overall performance. They hoped

that this measure would also help to prevent the use of leaked passwords. Participants' opinions were expressed as:

“. . .the only way to ensure [security] is to keep updating the password so that even if it is shared among people or breached in any way, it can quickly be fixed because the password would have been changed by then and there is no way people can have access to patients' information” (IDI 5 with HIM Officer, hospital B)

“. . .I think going forward there should be a thorough review of the system based on functionalities, security and usability and other factors around it.” (IDI 1 with a public health officer, hospital B)

Provision of backup storage. Additionally, some respondents suggested providing alternative backup systems for patient information, as well as improving internet services and electrical power supply to facilitate easy retrieval.

“I think, there should be an alternative storage for patient information, so that should in case the system stops working we can always easily retrieve information. . .” (IDI 16 with Nurse, hospital A)

The problem is not the training, it is rather the general system backup, there should be a backup concerning network, and internet services. At least power stabilizers for the computers. There should be general electrical backup as well.” (IDI 12 with a medical officer, hospital A)

Provision of adequate devices. A suggestion was made to provide more laptops and computer devices to the facility to prevent patient information from leaking.

“. . .again, provision of more laptops and computers so that people will not be forced to use other means that will leak patients' information.” (IDI 10 with Midwife, hospital C)

Provision of access on a “need to know basis.” Some participants expressed concern about the attitudes of certain colleagues and suggested that only staff involved in a patient's care should have access to their information.

“. . .as an institution, it is good to restrict how people get access to information. . . As I said earlier on, it should be ‘need to know basis’. . .there should be written consent before patient information can be released. . . Even as a health practitioner in general, it should not be that any doctor. . .just a click of a button can access the information. It should be restricted. The restriction in this way will prevent people from getting hold of the information and use it for their own things.” (IDI 6 with a HIM officer, hospital C)

Discussion

This present study provides clear evidence of the primary concerns healthcare professionals have regarding the use of DHTs in hospitals, particularly in relation to the protection of patient information. Both qualitative interviews and quantitative survey findings highlight that protecting patient information is a significant concern, aligning with Bani Issa et al,⁴ who found

similar worries among nurses about privacy and confidentiality in DHTs. Despite health professionals perceiving DHTs as secure due to access restrictions, concerns persisted about colleagues potentially misusing their credentials.

A critical issue revealed by the study was the differing views on patient consent when using DHTs. While some healthcare professionals believed DHTs negated the need for explicit consent, 81% of survey respondents disagreed, emphasizing the importance of establishing clear guidelines to safeguard privacy. This issue mirrors concerns noted in existing literature about the ambiguity of consent in DHT use.^{4,33} Moreover, patient access to information was debated. Some professionals advocated for full access to help patients make informed decisions, while others feared it could lead to misinterpretation. Notably, 28% of respondents in the quantitative arm expressed little concern over this issue.

The qualitative findings revealed that DHTs could potentially enhance privacy and confidentiality. However, the quantitative data showed serious concerns about unauthorized access, particularly from staff not directly involved in patient care.³⁴ The broad access to patient data across departments within DHTs raised significant risks of confidentiality breaches. About 80% of respondents were concerned about the inappropriate sharing of sensitive patient information, consistent with previous findings on such breaches being motivated by curiosity or gossip.^{6,34}

Internal security risks, particularly improper use of access credentials, were identified as major vulnerabilities. While access control measures such as usernames and passwords were enforced, human error remains a significant threat. About 80% of participants from the survey expressed concerns over credential sharing, which mirrors findings from studies in Iran, where universal access compromised confidentiality.^{7,35} Failing to log off properly was a recurring issue, leaving systems vulnerable to unauthorized access, as seen in prior research.^{3,4,36}

External threats, such as hacking, malware, and viruses, were major concerns among healthcare professionals. Nearly 75% of survey respondents expressed feared that malware or external hacking could compromise patient data, an anxiety echoed in the qualitative data consistent with other studies, where health professionals voiced similar fears.²⁰ Security measures like firewalls, antivirus software, and encryption were acknowledged as essential in both the qualitative and quantitative data, along with administrative policies, such as restricting personal devices from accessing hospital networks. However, 22% of survey respondents reported insufficient knowledge of DHT security concerns, which may have contributed to some staff using personal devices due to a lack of adequate hospital equipment. This lack of awareness increases the risk of breaches and aligns with concerns identified in prior research.⁶

Elahi and Geman²⁰ identified common health data breaches such as hacking, illegal access, theft, and data loss. To prevent such breaches, stronger equipment, updated security protocols,

and attention to human factors are essential, as suggested by the qualitative findings. Regular password updates and staff training are critical to improving security, especially considering that 80% of medical and non-medical staff surveyed expressed concerns about inadequate training on DHT security topics—an issue that aligns with existing research on healthcare professionals' knowledge of security concerns.²⁰ The study further revealed that many healthcare professionals were unaware of data integrity policies designed to ensure regulatory compliance and secure DHT usage. This was corroborated by the survey, where 77% of respondents reported insufficient knowledge of these policies. To address this gap, the qualitative data strongly recommended tailored training on data security to enhance staff awareness and preparedness.

Concerns about data manipulation within DHTs, raised in both this study and previous research by Enaizan et al,²⁶ emphasize the importance of ensuring data credibility. The trustworthiness or reliability of DHTs depends on the accuracy of the data they store, but issues such as power outages and poor internet connectivity undermine health professionals' confidence in the accuracy of recorded information. In this study, about 76% of respondents from the survey expressed concern about incomplete documentation. Similar concerns have been reported in other studies,⁷ further emphasizing the need for a robust infrastructure to support the effective use of DHTs.

System unavailability due to unexpected shutdowns was a major concern for more than 86% of survey respondents. These interruptions not only caused frustration and delays but also compromised patient safety by limiting access to crucial information as explained in the qualitative data. Similar issues have been reported in studies from Iran and the UAE, where system failures and internet disruptions adversely impacted healthcare services.^{4,7,37} While effective backup systems are essential to address this challenge, financial constraints, as seen in Ghana, often make even basic backup systems ineffective.²¹ Therefore, ensuring reliable backups and uninterrupted system access is critical to maintaining the integrity of DHTs in healthcare.

Implications for Policy

The lack of well-defined policies governing DHTs poses significant risks to patient safety and confidentiality. To mitigate these risks, health facilities must establish clear and enforceable policies that specifically regulate the operation of DHTs. Many health professionals also lack awareness of existing security protocols, underscoring the need for ongoing policy updates and mandatory training. Since human behavior is a key vulnerability in security breaches, stringent policies should enforce controlled access to patient data on a “need-to-know” basis, minimizing exposure to sensitive information. Furthermore, policy frameworks should be regularly reviewed and adapted to address evolving threats and technological advancements.

Implications for Practice

Health facilities should prioritize comprehensive safety and security training for all staff, including new hires, to ensure everyone is knowledgeable about DHT security protocols. This step is critical in safeguarding patient information and mitigating both internal and external risks. The concerns about unrestricted access to sensitive data underscore the need for strict access controls within DHTs, addressing health professionals' apprehensions about data confidentiality. Additionally, usability issues, such as time-consuming mandatory fields and limited system functionalities, must be resolved to enhance efficiency and prevent workflow disruptions. System malfunctions can compromise patient safety by jeopardizing the security of patient information. Addressing these concerns will promote the confident and secure use of DHTs, ensuring both patient safety and continuity of care.

Implications for Future Research

Future research should focus on understanding how human behavior contributes to vulnerabilities in DHTs and develop targeted strategies to mitigate these risks. Additional studies should also explore more effective backup systems to address frequent downtimes caused by unplanned shutdowns, thereby ensuring greater system reliability in similar healthcare settings.

Strength and Limitations

A key strength of this study lies in its use of exploratory in-depth interview methodology, which provided valuable insights into how DHTs impact healthcare delivery and revealed strategies to address associated challenges. However, a limitation lies in the variation in DHT systems across facilities, with 1 system sourced from a different vendor. Differences in system stability may have influenced the outcomes, potentially affecting the comparability of the findings across sites.

Conclusion

DHTs have brought substantial changes to the healthcare industry, offering numerous benefits but also introducing significant risks that must be carefully managed. Ensuring security, limiting access to sensitive patient data, and maintaining effective backup systems are necessary for the successful and safe use of DHTs in healthcare settings. With the right policies, training, and improvements in design, DHTs can effectively protect patient information and enhance the quality of patient care.

Acknowledgements

The authors wish to thank all study participants for the valuable time they shared during the study. We are also grateful to the heads of the facilities for their support and permission to conduct the study in their facilities. Finally, we would like to thank all those who arranged the necessary logistics for conducting the study and the research assistants for supporting us during data collection.

Author Contributions

NKM and GA conceptualized and designed the study, conducted data analysis, and were responsible for the interpretation of data and writing of the manuscript. NKM, GA, JK, HTA, SBJ, PA, CO, JA, EO, and AYA implemented and conducted the study. NKM wrote the first draft of the article. NKM, GA, JK, HTA, SBJ, PA, CO, JA, and EO participated in data interpretation and manuscript writing. NKM, GA, JK, HTA, and ROB reviewed the final draft and provided substantial input. All authors read the article and substantially contributed to this paper.

Ethical Considerations


The Institutional Review Board (IRB) of the Cape Coast Teaching Hospital (CCTH - CCTHERC/EC/2022/086) and the University of Ghana Medical Centre (UGMC - IRB/MSRC/009/2022) provided ethical clearance for the study. The leaders of the various health facilities where the study was carried out were asked to give their approval to conduct the research. The research team meticulously followed all COVID-19 protocols to avoid any needless disturbance or distraction at work. Each respondent provided written informed consent, and every effort was made to preserve anonymity and confidentiality by not collecting any personally identifiable information such as names, designations, or positions. Participants were told they reserved the right to withdraw from the study at any time without consequences and were informed that all data collected would be utilized strictly for this study.

Statement of Responsibility

I, Godwin Adzakupah as the corresponding author for this study, accept full responsibility for the study's design, thorough data analysis, results presentation, and decision to publish.

ORCID iD

Nathan Kumasenu Mensah  <https://orcid.org/0000-0001-5333-589X>

Godwin Adzakupah  <https://orcid.org/0000-0002-6916-6733>

Jonathan Kissi  <https://orcid.org/0000-0003-2942-5654>

Christabell Opoku  <https://orcid.org/0009-0002-4352-259X>

Richard Okyere Boadu  <https://orcid.org/0000-0003-2243-593X>

SUPPLEMENTAL MATERIAL

Supplemental material for this article is available online.

REFERENCES

- Obaid OI, Salman SA-B. Security and privacy in IoT-based healthcare systems: a review. *Mesop J Comput Sci.* 2022;2022:29-40.
- Raghupathi W, Raghupathi V, Saharia A. Analyzing health data breaches: a visual analytics approach. *AppliedMath.* 2023;3:175-199.
- Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. *J Med Syst.* 2017;41:127-129.
- Bani Issa W, Al Akour I, Ibrahim A, et al. Privacy, confidentiality, security and patient safety concerns about electronic health records. *Int Nurs Rev.* 2020;67:218-230.
- Ladis H, Zolkefi Y. Health care students' views on protecting patients' privacy and confidentiality. *Int J Nurs Educ.* 2021;13:7-13.
- Basil NN, Ambe S, Ekhaton C, Fonkem E. Health records database and inherent security concerns: a review of the literature. *Cureus.* 2022;14:14.
- Kalkhajeh SG, Aghajari A, Dindamal B, Shahvali-Kuhshuri Z, Faraji-Khiavi F. The integrated electronic health system in Iranian health centers: benefits and challenges. *BMC Primary Care.* 2023;24:53.
- Pankhurst T, Lucas L, Ryan S, et al. Benefits of electronic charts in intensive care and during a world health pandemic: advantages of the technology age. *BMJ Open Quality.* 2023;12:e001704.
- Zaman I, Chauhan I. Effect of electronic medical records on improving patient care. *Diversity and Equality in Health and Care.* 2021;18(1).
- Yeng PK, Fauzi MA, Yang B. A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals. *Information.* 2022;13:335.
- Edemekong P, Annamaraju P, Haydel M. Health insurance portability and accountability act. 2018.
- Khando K, Gao S, Islam SM, Salman A. Enhancing employees information security awareness in private and public organisations: a systematic literature review. *Comput Secur.* 2021;106:102267.
- Keshta I, Odeh A. Security and privacy of electronic health records: concerns and challenges. *Egypt Inform J.* 2021;22:177-183.
- McDermott DS, Kamerer JL, Birk AT. Electronic health records: a literature review of cyber threats and security measures. *Int J Cyber Res Educ.* 2019;1:42-49.
- Choi S, Martins JT, Bernik I. Information security: listening to the perspective of organisational insiders. *J Inf Sci.* 2018;44:752-767.
- Jeremiah P, Samy G, Shanmugam B, et al. Potential measures to enhance information security compliance in the healthcare internet of things. In: Recent Trends in Data Science and Soft Computing: Proceedings of the 3rd International Conference of Reliable Information and Communication Technology (IRICT 2018), 2019, pp.726-735. Springer.
- Lee I. Analysis of insider threats in the healthcare industry: a text mining approach. *Information.* 2022;13:404.
- Esteves J, Ramalho E, De Haro G. To improve cybersecurity, think like a hacker. *MIT Sloan Management Review.* 2017.
- Mensah NK, Adzakupah G, Kissi J, et al. Perceived impact of digital health technology on health professionals and their work: a qualitative study in southern Ghana. *Digit Health.* 2023;9:20552076231218838.
- Elahi H, Geman O. Recent healthcare information breaches and their lessons. *Arch Surg Res.* 2020;1:17-23.
- Mensah NK, Boadu RO, Adzakupah G, et al. Electronic health records post-implementation challenges in selected hospitals: a qualitative study in the Central Region of southern Ghana. *Health Inf Manage J.* 2023;52:204-211.
- Lemke J. Storage and security of personal health information. *OOHNA J.* 2013;32:25-26.
- Wanyonyi E, Rodrigues A, Abeka S, et al. Effectiveness of security controls on electronic health records. 2017.
- Fox G, James TL. Toward an understanding of the antecedents to health information privacy concern: a mixed methods study. *Inf Syst Front.* 2021;23:1537-1562.
- Sari PK, Handayani PW, Hidayanto AN, Yazid S, Aji RF. Information security behavior in health information systems: a review of research trends and antecedent factors. *Healthcare.* 2022;10:2531.
- Enaizan O, Zaidan AA, Alwi NHM, et al. Electronic medical record systems: decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health Technol.* 2020;10:795-822.
- von Elm E, Altman DG, Egger M, et al. The strengthening of reporting of observational studies in Epidemiology (STROBE) statement: guidelines for reporting observational studies. *Lancet.* 2007;370:1453-1457.
- Halcomb E, Hickman L. Mixed methods research. 2015.
- Creswell JW, Creswell JD. *Research Design: Qualitative, Quantitative, and Mixed-Methods Approaches.* Sage publications; 2017.
- Schoonenboom J, Johnson RB. How to construct a mixed methods research design. *Kolner Z Soz Sozialpsychol.* 2017;69:107-131.
- Clarke V, Braun V. *Thematic Analysis: A Practical Guide.* Sage; 2021.
- DeVellis R, Thorpe C. *Scale Development: Theory and Applications.* Sage Publications; 2021.
- Harle CA, Golembiewski EH, Rahmanian KP, et al. Patient preferences toward an interactive e-consent application for research using electronic health records. *J Am Med Inform Assoc.* 2018;25:360-368.
- Stablein T, Loud KJ, DiCapua C, Anthony DL. The catch to confidentiality: the use of electronic health records in adolescent health care. *J Adolesc Health.* 2018;62:577-582.
- Fakhrzad M, Fakhrzad N, Dehghani M. The role of electronic health records in presenting health information. *Interdiscip J Virtual Learn Med Sci.* 2012;2:31-40.
- Chen Y-Y, Lu J-C, Jan J-K. A secure EHR system based on hybrid clouds. *J Med Syst.* 2012;36:3375-3384.
- Jafari H, Ranjbar M, Amini-Rarani M, Hashemi FS, Bidoki SS. Experiences and views of users about delivering services through the integrated health system: a qualitative study. *J Tolooebehdasht.* 2020;19(2).