

Healthcare Professional's Knowledge, Awareness, and Attitude toward Patients' Data Privacy and Security in Clinical Research

Monirah A. Albabtain^a Dalal AlOtaibi^b Nourah AlMazial^b Nouf Aloudah^c
Haneen Mohammed Alghosoon^a Amr A. Arafat^{d,e}

^aResearch Department, Prince Sultan Cardiac Center, Riyadh, Saudi Arabia; ^bCollege of Pharmacy, AlMaarefa University, Riyadh, Saudi Arabia; ^cClinical Pharmacy Department, College of Pharmacy, King Saud University, Riyadh, Saudi Arabia; ^dAdult Cardiac Surgery Department, Prince Sultan Cardiac Center, Riyadh, Saudi Arabia; ^eCardiothoracic Surgery Department, Tanta University, Tanta, Egypt

Keywords

Health Insurance Portability and Accountability · National Committee of Bioethics · Privacy · Security

Abstract

Introduction: The privacy and security of healthcare information are essential to maintaining good patient-physician relationships, protecting individuals' interests, and respecting their dignity and worth. This study assessed healthcare professionals' (HCPs) knowledge, awareness, and attitudes toward patients' data privacy and security in clinical research. **Methods:** The study consisted of a cross-sectional survey in which 108 HCPs' awareness and knowledge of HIPAA and NCBE rules and regulations were measured, followed by an in-depth semistructured interview to explore HCPs' attitudes and perspectives. The study was conducted between January and May 2022. **Results:** Most participants agreed that the IRB/REC rules and regulations strengthened participants' trust in the researchers, enhanced confidentiality, and improved the privacy and security of patients' information. HIPAA knowledge was affected by prior participation in research ($\beta: 1.16; p = 0.001$) and NCBE knowledge by working on a research project ($\beta: 0.87; p = 0.001$), years of work experience ($\beta: 0.35; p = 0.003$),

and age ($\beta: -0.28; p = 0.04$). Participants believed that the nature of research, involvement of inexperienced persons, and human errors could affect patients' privacy and security in clinical research, which could be improved by limiting the number of personnel who access the data, continuous education, and sending reminders about the rules and regulations. **Conclusions:** Patients' data privacy and security remain vital to clinical research. HCPs realize the role of IRB/REC to maintain data privacy and security. Enrollment of HCPs in clinical research and continuous education could improve HCP knowledge of regulatory rules.

© 2024 The Author(s).
Published by S. Karger AG, Basel

Introduction

For effective medical treatment, sensitive and private information must be shared between patients and healthcare professionals (HCPs). This information is recorded and kept in medical records and databases at all times, which patients assume to be private and secure [1]. Privacy is defined as “a state or condition of physical or informational accessibility that will determine the type, nature, and, to what extent, patient information can be

communicated to others” [2]. Furthermore, security can be defined as “the procedural and technical measures required to prevent unauthorized access, modification, use of data stored or processed in a computer system, to prevent any deliberate denial of service.” It helps keep health records safe from unauthorized use [3, 4]. In this information age, privacy is a valuable commodity and an important security component. It protects the interests of individuals and respects their dignity and worth as human beings.

In Saudi Arabia, maintaining the privacy of health-care information is of utmost importance. It is a culturally sensitive environment; patients are less likely to seek medical care in cases of substance abuse and reproductive or sexual health matters for fear that their health information will be shared or will not be securely maintained. In some cases, patients suffering from psychiatric disorders may refuse to reveal vital information affecting their treatment plan since divulgence will lead to discrimination or social stigmatization [5]. That fear will not only affect the patient-physician relationship; it will most definitely prevent such patients from consenting to enroll in research studies covering sensitive subjects.

There are a variety of rules and policies that regulate the use of patients’ health information in research [6]. In the USA, for instance, the Health Insurance Portability and Accountability (HIPAA) Act of 1996 is very well established and is followed by HCPs to protect the privacy and security of patients’ health information [7, 8]. HIPAA rules and regulations are federal laws protecting who and how health information is handled [6, 8].

Moreover, in Saudi Arabia, in 2001, royal decree No. 7/B/9512 ordered the creation of a National Committee of Bioethics (NCBE). The committee’s responsibilities included establishing and monitoring compliance with biomedical research ethics and requirements in a way consistent with the Islamic Sharia Law and the traditions and essence of the culture of Saudi Arabia [9].

A few HCPs consider security and privacy measures interchangeable; however, they are dissimilar. The term “privacy,” as mentioned before, is more focused on the (what) aspect of information, while the term “security” is defined as the (how) [10, 11]. There has been a notable growth in research and an increased development of research centers in the Middle East. Therefore, applying HIPAA rules and regulations in research has become essential for protecting patient information, privacy, and security. The basic law of government in Saudi Arabia dictates the state’s importance of providing public health and healthcare to all citizens, as mentioned in Article No.

31. Privacy of information in all types of communication shall be inviolate, as mentioned in Article No. 40 [5]. Legally, there are laws for implementing healthcare and providing information privacy, but there are no specifications for protecting patients’ health information. This study aimed to assess the awareness, knowledge, and attitude of HCPs toward patients’ data privacy and security in clinical research using the HIPAA and NCBE rules and regulations.

Methods

Study Design

A mixed methods approach was used, and it consisted of two parts: a cross-sectional study in which the HCPs’ awareness and knowledge of HIPAA and NCBE rules and regulations were measured using an anonymous self-administered survey as a descriptive method that was followed by an in-depth semi-structured interview based on the Theoretical Domains Framework (TDF) to explore HCPs’ attitudes and perspectives (a supplementary focus group).

Survey Design

The questionnaire items were created after a review of pertinent literature on security, privacy, and privacy in relation to clinical research. The questionnaire comprised two sections; the first included demographic data (age, gender, marital status, education level, and work experience). The second section included 15 questions to measure the awareness of HIPAA rules and regulations, NCBE laws and policies, and the awareness of HCPs toward the role of Institutional Review Board (IRB)/Research Ethics Committee’s (REC) to protect patients’ data privacy and security in clinical research. Ten HCPs pilot-tested the survey items for clarity and comprehension before distribution. After that, the questionnaire was distributed to the participants (including physicians, pharmacists, and nurses) physically and via an Internet link. The participant inclusion criteria were HCPs who had experiences with both practice and research in a single tertiary referral center. The survey was distributed between January 2022 and March 2022.

Interview Design

A follow-up phone call was conducted with interested participants to provide information, explain the study objectives, and decide upon the interview time. Consent was obtained verbally at the beginning of each focus group (FG) interview. Three in-depth, semistructured FG interviews were conducted with a sample of the participants until saturation of knowledge was reached in the data. All conversations were digitally recorded with the participant’s permission and were transcribed verbatim.

Topic Guide

A topic guide was created (online suppl. material, available at <https://doi.org/10.1159/000538617>). We used a TDF to build the topic guide. TDF is a synthesis of 33 theories to understand behavior and behavior changes [12]. It was developed by collaborations of psychiatrists, health psychologists, and healthcare

providers to help implement these theories by nonexperts [12]. The questions were amended to fit our topic and were revised by two HCPs for understanding. A warm-up question about the participants' opinions about privacy in their research was asked at the start of the interview. The interviews were conducted in English (as many of the HCPs are English speakers), the participants were allowed to use the Arabic language to express opinions more easily, and the section spoken in Arabic was translated to English by N.A. and revised by a professional translator. The interviews were recorded and transcribed verbatim by a professional transcriber. Furthermore, the semi-structured interviews were undertaken virtually using Zoom videoconferencing. Finally, the interviews took place from March to May 2022 and lasted between 40 and 60 min.

Ethical Considerations

The questionnaire was distributed only after receiving approval from the Research Ethics Committee, approval number (withheld for review). Participants were informed of the aim and content of the study. No identifiable information was collected from the participants, i.e., names, ID numbers, or contact information.

Data Analysis

Data were computed using Stata 16 (Stata Corp, College Station, TX, USA). The calculations of the survey were summarized using descriptive statistics (frequency and percentages) and presented in tables. The χ^2 or Fisher's exact test was used to compare group responses. Each correct answer about HIPAA or NCBE knowledge was given a score of one. The total HIPAA and NCBE scores were compared between both groups using the Wilcoxon test. Stepwise quantile regression was used to evaluate factors affecting the knowledge scores. Baseline data and variables related to participants' research history were introduced into the model, and variables with a *p* value of less than 0.05 were retained in the final model.

Thematic analysis of the interviews was performed with MAXQDA Analytics Pro 2020 (VERBI Software). Thematic analysis is the systematic identification and analysis of patterns, meanings, and themes within qualitative data [13]. Thematic analysis is initiated by familiarization with the data, then generating initial code and potential themes. Next, the themes are refined by reviewing and defining them. Throughout the thematic analysis process, multiple researchers are involved to enhance the trustworthiness of the findings [13]. Two authors (N.A., M.A.) examined each transcript independently, and a third author (A.A.) checked for discrepancies between the two versions. Discussions were used to settle disagreements. Data were examined following each interview to create initial codes and identify significant and new information.

Each FG was concluded with a summary that was to be verified by the participants and checked for any ambiguity to increase rigor and reliability. The two researchers (N.A., M.A.) met after each interview to discuss the data they had gathered. Memoranda was made during the interviews and used for data collection and analysis utilizing MAXQDA memos (such as describing interviewee's expressions or hesitation to answer specific questions effectively). Interviewers continued collecting data until they found enough information to supplement their understanding of the topic. Interview data were kept private.

Results

Survey Design

Description of the Participants

The majority of the 108 survey respondents, who were divided into two groups based on their field of practice – physicians (20.37%) and nonphysicians (79.63%) – were women (64.81%). Nearly 90% of all responders fell within the age range of 44 or younger. Both categories (physicians and nonphysicians) showed that >80% have a bachelor's degree. The majority of respondents in the nonphysician categories have a bachelor's degree. In contrast, the majority of respondents in the physician group have either a bachelor's degree or a fellowship/board educational level (40% and 31%, respectively). Additionally, the majority of survey participants (60%) (60% for nonphysicians and 68% for physicians) had >5 years of professional experience. There were significant differences in gender, age groups, and educational levels between physicians and non-physicians (Table 1).

Research History

Respondents were questioned about their history or engagement in research. The majority (64.81%) claimed a history of engagement, and out of the 108 people surveyed, 27 said they were presently engaged in research projects either in the proposal writing, data gathering, or data analysis stages. More physicians were working on research and had significantly more publications than nonphysicians (Table 2).

Perceptions of the Impact of the IRB/REC Rules and Regulations

In reporting perception of the impact of the IRB/REC rules and regulations for protecting health information, half of physicians respondents reported that they agree that the rules made research easier (50%), while the other half were either undecided (36.36%) or disagreed with the statement (13.64%). Almost all nonphysicians (80%) and physicians (72.73%) agreed that the IRB/REC rules and regulations strengthened participants' trust in the researchers. Another point that both groups agreed on was that the rules and regulations also enhanced confidentiality (81.82% and 84.88% for physicians and nonphysicians, respectively). The perceived benefit of the rules and regulations to improve the privacy and security of patients' healthcare information was reported to be agreed on by both groups (68.18% and 88.37% for physicians and nonphysicians,

Table 1. Baseline data of study participants

Variables	Nonphysicians (n = 86; 79.63%)	Physicians (n = 22; 20.37%)	Total (n = 108)	p value
Female	66 (76.74)	4 (18.18)	70 (64.81)	<0.001
Age groups, years				0.01
25–34	52 (60.47)	7 (31.82)	59 (54.63)	
35–44	23 (26.74)	6 (27.27)	29 (26.85)	
45–54	8 (9.30)	5 (22.73)	13 (12.04)	
55–64	1 (1.16)	3 (13.64)	4 (3.70)	
65+	2 (2.33)	1 (4.55)	3 (2.78)	
Educational level				<0.001
Bachelor's degree	74 (89.16)	7 (31.82)	81 (77.14)	
Master's degree	3 (3.61)	2 (9.09)	5 (4.76)	
Medical degree	3 (3.61)	3 (13.64)	6 (5.71)	
Fellowship/board	3 (3.61)	9 (40.91)	12 (11.43)	
Doctorate's degree	0	1 (4.55)	1 (0.95)	
Work experience				0.07
6 months–5 years	34 (40.96)	7 (31.82)	41 (39.05)	
6–10 years	21 (25.30)	4 (18.18)	25 (23.81)	
11–15 years	13 (15.66)	1 (4.55)	14 (13.33)	
+16 years	15 (18.07)	10 (45.45)	25 (23.81)	

Table 2. Research history of survey respondents

Variables	Nonphysicians (n = 86; 79.63%)	Physicians (n = 22; 20.37%)	Total (n = 108)	p value
Have you ever been a part of or conducted a research study? (Yes)	53 (61.63)	17 (77.27)	70 (64.81)	0.22
Are you currently working on a research study? (Yes)	14 (16.28)	13 (65)	27 (25.47)	<0.001
In which phase are you currently working on?				0.57
Proposal writing	4 (22.22)	2 (12.5)	6 (17.65)	
Data collection or data analysis	8 (44.44)	8 (50)	16 (47.06)	
Publication	6 (33.33)	4 (25)	10 (29.41)	
How many publications do you have?	0 (0–1)	2 (1–5)	1 (0–3)	<0.001

respectively). Last, both groups had equal opinions in agreement, disagreement, and undecidedness about the claim that the rules and regulations increased the amount of time needed to complete the study (Table 3).

HIPAA Knowledge

The survey included six general questions to gauge respondents' knowledge of HIPAA, including questions about specific rules (such as privacy and security rules), who should adhere to HIPAA, and what steps should be taken if research participants' personal

information is discussed. Five out of the six questions in this section of the survey were correctly answered by more than 50% of the survey respondents, with no differences in the responses between physicians and nonphysicians (Table 4). The median score for the correct answers in both groups was 4 (25th–75th percentiles: 3–5). There was no difference between physicians and nonphysicians in the total correct answers about HIPAA knowledge; this reflects the awareness of HCPs on patients' health information security and privacy ($p = 0.659$). HIPAA score was affected only by prior participation in research which

Table 3. Scaled perceptions of the impact of the Institute Review Board (IRB)/Research Ethics Committee's (REC) rules and regulations for protecting health information

Have the rules and regulations	N (%)						p value
	agree		undecided		disagree		
	nonphysician	physician	nonphysician	physician	nonphysician	physician	
Made research easier	51 (59.30)	11 (50)	29 (33.72)	8 (36.36)	6 (6.98)	3 (13.64)	0.54
Strengthened the participant's trust	69 (80.23)	16 (72.73)	15 (17.44)	6 (27.27)	2 (2.33)	0	0.60
Added cost	40 (46.51)	6 (27.27)	29 (33.72)	8 (36.36)	17 (19.77)	8 (36.36)	0.15
Enhanced confidentiality?	73 (84.88)	18 (81.82)	11 (12.79)	3 (13.64)	2 (2.33)	1 (4.55)	0.74
Delayed time to study completion	34 (39.53)	7 (31.82)	32 (37.21)	8 (36.36)	20 (23.26)	7 (31.82)	0.66
Improved the privacy and security of participant's healthcare information?	76 (88.37)	15 (68.18)	9 (10.47)	5 (22.73)	1 (1.16)	2 (9.09)	0.03

Table 4. Health Insurance Portability and Accountability (HIPAA) knowledge of survey respondents

Questions	Nonphysicians (n = 86; 79.63%)	Physicians (n = 22; 20.37%)	p value
The major goal of privacy rules is to ____.			0.12
• Protect an individuals' health information in clinical and in research settings (Correct)	76 (88.37)	21 (95.45)	
• Protect the insurance company	0	1 (4.55)	
• Keep all health information documents sealed	9 (10.47)	0	
The security rules aim is to ____.			0.18
• Allow healthcare professionals flexibility to create their own privacy procedures	9 (10.47)	4 (18.18)	
• Protect all health information that is held or transferred in physical and electronic form (Correct)	67 (77.91)	17 (77.27)	
• Protect healthcare information for medical insurance companies	9 (10.47)	0	
Health information that contains at least ____ patient identifier(s) is protected.			0.51
• One (Correct)	36 (41.86)	12 (54.55)	
• Two	45 (52.33)	10 (45.45)	
• Five	5 (5.81)	0	
If you observe someone wrongfully disclosing a research participant's health information, what should you do <i>first</i> ?			0.39
• Talk with your supervisor about the situation	24 (28.24)	9 (40.91)	
• Talk to the person who is disclosing health information (Correct)	58 (68.24)	12 (54.55)	
• Confront the participant	3 (3.53)	1 (4.55)	
Two researchers are eating lunch at a busy restaurant and discussing a research participant's case that involves confidential health information regarding the participant. What should they do?			0.139
• They should not mention the name of the participant	38 (44.19)	14 (63.64)	
• Ask others what they think	1 (1.16)	1 (4.55)	
• Move to a private location (Correct)	46 (53.49)	7 (31.82)	
The rules and regulations that help protect the security and privacy of patient's health information are required to be followed by?			0.25
• Healthcare providers	4 (4.65)	3 (13.64)	
• Medical and/or clinical researchers	2 (2.33)	0	
• All of the above (Correct)	80 (93.02)	19 (86.36)	

Table 5. National Committee of Bioethics (NCBE) knowledge of survey respondents

Questions	Nonphysicians (n = 86; 79.63%)	Physicians (n = 22; 20.37%)	p value
The National Committee of Bioethics is defined as?			0.59
• A committee that monitors compliance with biomedical research ethics and requirements (Correct)	76 (88.37)	19 (86.36)	
• A committee decides which drugs will appear on that entity's drug formulary	3 (3.49)	0	
• An executive body of the council that is responsible for the direct supervision over the health insurance industry	7 (8.14)	3 (13.64)	
NCBE is related to one of the following?			0.13
• Saudi Commission for Health Specialties	22 (25.58)	2 (9.52)	
• Saudi Food and Drug Authority	7 (8.14)	4 (19.05)	
• Research Center (Correct)	57 (66.28)	15 (71.43)	
Institute Review Board (IRB)/Institutional Research Ethics Committee (REC) is a representative committee in each institute, appointed by NCBE and is responsible for ____.			0.05
• Approval of new drug to formulary	3 (3.49)	3 (13.64)	
• Providing approval for the principal investigator for conducting any research studies (Correct)	81 (94.19)	17 (77.27)	
• Supervising and evaluating training programs	2 (2.33)	2 (9.09)	
Research participants have the right to withdraw at any point during or after the research project as mandated by ____.			0.73
• Saudi Health Council	10 (11.63)	3 (13.64)	
• Council of Cooperative Health Insurance	6 (6.98)	2 (9.09)	
• National Committee of Bioethics (Correct)	70 (81.40)	17 (77.27)	
NCBE committee rules and regulations are applied to ____.			0.007
• Foreign and Saudi researchers (Correct)	68 (80)	17 (77.27)	
• Only Saudi researchers	17 (20)	2 (9.09)	
• Only foreign researchers	0	3 (13.64)	
NCBE rules and regulations are ____.			0.04
• Optional for HCPs conducting research	37 (43.02)	6 (27.27)	
• Applicable only to research in hospital settings	24 (27.91)	3 (13.64)	
• Law mandated by a royal decree (Correct)	25 (29.07)	13 (59.09)	

indicates improved HIPPA knowledge for those who had experience with clinical research (β : 1.16 [95% CI: 0.52–1.81]; $p = 0.001$).

NCBE Knowledge

Table 5 lists the six broad questions included in the survey to determine respondents' familiarity with the NCBE, including inquiries regarding the NCBE's definition, the area it primarily influences, and the individuals to whom its rules and regulations are applied. The survey demonstrated that more than 50% of the survey respondents from the physician group correctly answered all six questions. In the nonphysician group, five out of the six questions in this section were correctly answered by more than 50% of the survey respondents. The median score of correct answers was 5 (4–5) in

nonphysicians and 5 (4–6) in physician groups ($p = 0.517$). Factors increasing the score were working on a research project (β : 0.87 (95% CI: 0.35–1.39); $p = 0.001$), and years of work experience (β : 0.35 (95% CI: 0.12–0.58); $p = 0.003$), while increased age was associated with lower score (β : –0.28 (95% CI: –0.54 to –0.01); $p = 0.04$).

Interview Design

Theme 1: Factors Influencing Variability in Defining Patients' Data Privacy and Security

• Nature of the Research

Participants mentioned that privacy is more secure in research than in practice. Physicians mentioned that they are more careful, as there is somebody following the process, unlike in practice:

“...for example, in practice, a patient comes to you asking for a doctor’s number. You can give him ..., but the research is much less.” (FG 1)

Furthermore, the nature of the research affected privacy violations, such as variability in sample size and nature of communication. For instance, some research contained a small sample number and for a very long time compared to other research where there are hundreds of patients:

“As Dr. (...) said, it depends on the type of researcher, especially dentistry... For example, you must be part of the research, and you will not pay anything, so I will start to pressure you to accept. However, we, as pharmacists, if, for example, a research questionnaire ... and he refused, I will go to another participant, no condition that I would pressure him to accept.” (FG 1)

- Junior versus Senior Researchers

Participants discussed that they noticed privacy violations when the primary investigator involved an inexperienced research assistant:

“... in general, (researchers) who know research procedures, how to do research and ethical aspects will not do that ... but I’m talking about the participants who are with us, for example, data collectors ... they must have an ethical guide, or study points that were taken in the past and not violate the data.” (FG 3)

Theme 2: Underlying Factors Contributing to Unauthorized Use of Patients’ Data Privacy and Security in Clinical Research

- Slip-Up Error

Participants discussed that the reason might be a human mistake, similar to any other error:

“... pressure causes a medical error, so this might happen... work pressure puts pressure on all people... no doubt it affects.” (FG 1)

- Local Research Culture

Interviewees discussed that the Saudi culture and nature of the communication might have contributed to such behavior, as the following interviewee mentioned:

“... I stay for an entire hour (with the patients), I sit with him and talk ... and I have his number. We are in culture as long as someone I sit with and talk to in private. They become friends, and we do not need to set boundaries ... Compared to other countries, we are definitely more. Saudi Arabia, for example, this is the norm!” (FG 1)

Furthermore, the problem of using personal mobile phones for planning recruitment and other research arrangements might aggravate it:

“Perhaps this is one of the mistakes that can happen in research. (communication) is not through a phone designated for work ... so violation happen... besides I am not supposed to keep them (the patients’ contacts) ... but what happens is not like that ...” (FG 3)

Theme 3: Enhancing Patients’ Data Privacy and Security: Recommendations from HCPs

- Continuous Education

HCPs mentioned that the matter is that protecting privacy depends on the researcher’s knowledge and that there is no dedicated education the healthcare provider received:

“... , it is certainly (was) part of the curriculum in the college. ... after this, no one teaches you or provides you instructions ... ” (FG 3)

- A Reminder

Participants discussed that an application for research that sends reminders might help:

“For me, I see that it is not easy at all, in a kind of difficulty to remember these things, you need a tool or something that reminds you that.” (FG 1)

- Limit Researchers’ Number and Access to Data

Interviewees mentioned that the limiting number of researchers who access patients’ data is vital:

“I think that according to the number of data collectors ... it is very important that two or three data collectors are allowed with the patient and not more ... do not assign more people.” (FG 3)

“The most important, I think, for example, was to set a password, and this password had an expiration date, and it would be granted by the head of the department. This is among the things that help.” (FG 1)

“... (a password) for a certain period, it was three months, and the password changed from time to time, and you could only open it from inside the hospital, the internal internet.” (FG 1)

Integration between Survey and Interview Components of Our Research

The integration of a mixed methods study, specifically by incorporating a qualitative design to enhance the understanding of the quantitative component, is a valuable approach in research that we undertook in our study [14]. By utilizing both qualitative and quantitative methods, researchers can gain a more comprehensive and nuanced understanding of the phenomenon under investigation. The interview study provided context, depth, and richness to the survey data, offering insights into the underlying reasons, motivations, and perceptions that

may not be captured through survey study alone. This integration aligns with the transformative mixed methods research framework proposed by Creswell and Plano Clark [15] which emphasizes the complementary nature of qualitative and quantitative methods in addressing research questions. Furthermore, the use of a qualitative design within a mixed methods study can also help in the interpretation of quantitative results, as qualitative data can elucidate the meaning and significance of quantitative findings. This integration is supported by the work of Tashakkori and Teddlie [16], who advocate for the synergistic use of qualitative and quantitative methods to capitalize on their respective strengths and offset their individual limitations. More discussion about the explanation of the survey component by the interview components is presented in the discussion section.

Discussion

Privacy and security of patients' data in clinical research have crucial value [17]. Previous report demonstrated that HCPs may lack sufficient knowledge to maintain patients' privacy [18]. There are limited data on the knowledge of national (NCBE) or international (HIPAA) guidelines for patients' data privacy and security in clinical research for HCPs in Saudi Arabia. Therefore, we performed this study to assess the awareness, knowledge, and attitude toward patients' data privacy and security in clinical research among HCPs, by utilizing the guidelines of the Health Insurance Portability and Accountability Act (HIPAA) and the National Committee on Bioethics (NCBE). The approach used was both quantitative and qualitative in nature, to assist not only in understanding and assessing the awareness, knowledge, and attitude (the what) but also, the why within the context of this study. To paint a better picture of HCP's awareness, knowledge, and attitude toward patients' data privacy and security in clinical research, a deeper and better understanding of the description and comprehension was needed by implementing a mixed methods design to produce stronger conclusions than each methodology alone. The findings in this study revealed varying levels of awareness among HCPs in reference to guidelines mentioned previously (HIPAA and NCBE), which was a crucial aspect of the study's objective to assess knowledge in this domain. Furthermore, the study delved into the attitudes of HCPs toward patient's data privacy and security, uncovering significant insights that align with our initial objective of understanding HCP

perspectives in the context of clinical research. These insights are instrumental in identifying gaps and formulating strategies for improving compliance and ethical conduct in clinical research, directly linking to the study's primary objectives. This study consisted of two components: the survey study and the interview study. The survey study included 108 participants (86 nonphysicians and 22 physicians). Despite the difference in the baseline characteristics and research experience, most participants agreed about their perceptions of the impact of the IRB/REC rules and regulations for protecting health information and their knowledge about HIPAA and NCBE. The survey has showed that physicians and nonphysicians have acceptable awareness of the HIPAA; however, this was significantly better in HCP who had participated in clinical research. The results also indicated the necessity to improve the knowledge of HCPs about data privacy and security in clinical research. Factors associated with better knowledge were prior participation in research, working on research projects, work experience, and younger age.

Utilizing an interview study in conjunction with survey results offered the added benefit of more understanding of the findings. Based on the interview study, several factors were identified that could impact patients' privacy and security in clinical research. Participants expressed concerns about the nature of the research, particularly in cases where the research involved sensitive health information. They emphasized the need for stringent measures to safeguard patient privacy, especially when inexperienced individuals were involved in data handling and management. Additionally, human errors were highlighted as a significant concern, with participants expressing apprehensions about the potential for data breaches due to inadvertent mistakes.

Furthermore, in response to these concerns, participants suggested various improvements to the data privacy and security process. This included limiting access to sensitive data to a specific number of authorized personnel, thereby reducing the risk of unauthorized exposure. Continuous education initiatives were also recommended to ensure that all individuals involved in clinical research, especially those handling patients' data, were well-versed in privacy protocols and best practices. Furthermore, participants stressed the importance of regular reminders about the rules and regulations governing data privacy and security to mitigate the likelihood of oversight or complacency.

The perception of HIPAA privacy rules was evaluated in other studies. A sample of 1,527 epidemiologists

in the USA were asked questions about the positive and negative potential effects of the HIPAA privacy rules. A measurement approach was used to determine the influence of the HIPAA privacy rules on health research. Only a quarter of epidemiologists agreed that the rule increased participants' confidentiality and privacy. The rule also negatively affected the IRB submission process, including approval delays and increased costs [19]. Furthermore, a cross-sectional survey of HCPs working in the training and research hospital aimed to determine the HCP's attitudes toward the privacy and confidentiality of the patients. The sample consisted of 174 nurses and 183 physicians. The study identified that at the highest, 40.8% of nurses and 26.8% of physicians reported that they were well aware of patient rights, and at their lowest, 2.9% of nurses and 8.2% of physicians reported that they were uninformed of patients' rights [20].

A cross-sectional study assessed the knowledge, perceptions, and practices toward medical ethics of 128 physician residents in three teaching hospitals. The results showed that most residents (98.0%) experienced ethical issues during their practice, which indicated a lack of knowledge and the ability to solve ethical problems among physician residents [21]. A study focused on the information system was also conducted in Saudi Arabia. The study aimed to assess the application of HIPAA regulations using a qualitative assessment approach to examine security information systems in two main Saudi healthcare institutions. A survey was used to examine the security and safeguarding of information. As a result, the scores from the two health security information systems in both institutions were relatively close. Thus, it was suggested that the Saudi Ministry of Health should construct a national policy for health information security based on the HIPAA model [22].

Mohammad Nejad et al. [23] conducted a cross-sectional study to measure nurses' awareness of patients' rights in a teaching hospital. The study used a two-part validated questionnaire. The study showed that out of 156 nurses, 58% had good awareness, 39% had medium awareness, and the remaining 2.5% had poor awareness. A significant relationship exists between nurses' awareness and work experience. The study recommended that special measures and strategies should be considered to promote nurses' awareness of patients' rights [23].

Our research findings unveil noteworthy distinctions from the literature reviewed, particularly in the realm of gender, age groups, and educational levels among phy-

sicians and nonphysicians. Unlike the existing literature, we identified significant differences in these demographic variables, suggesting that contextual factors specific to our study population may influence these disparities. A key similarity, however, emerges concerning physicians' perspectives on research rules, where half of the respondents agreed that the regulations facilitated the research process but simultaneously extended the time required for study completion. Similarly, HCPs acknowledged the pivotal role of IRB/REC in upholding data privacy and security, aligning with the existing literature. On the other hand, our research diverges notably in terms of participant numbers and methodological approaches.

The findings from this study underscore the importance of enhancing HCPs understanding and adherence to patients' data privacy and security, particularly concerning HIPAA and NCBE guidelines in Saudi Arabia. As previously noted by the interviewees, they recommended improvements to data privacy and security protocols. One recommended policy change is the implementation of mandatory HIPAA certification for all healthcare providers. This certification process should be designed to ensure that every HCP, regardless of their role or level of experience, possesses a thorough understanding of HIPAA regulations and the importance of patients' data privacy and security in clinical practice. The certification program could include comprehensive training modules covering various aspects of HIPAA, including patient rights, data handling procedures, and the legal implications of data breaches. Additionally, regular recertification, perhaps on an annual or biennial basis, could be mandated to ensure that healthcare providers stay current with any changes or updates in HIPAA regulations. This policy change would not only enhance the overall compliance with patient data protection standards but also foster a culture of continuous learning and vigilance among HCPs, ultimately leading to improved patient trust and safety in healthcare settings. Also, ongoing training sessions and assessments are crucial to keeping HCPs abreast of the latest developments in data privacy and security, potentially through online modules, workshops, or continuing education credits. Establishing a culture of compliance within healthcare institutions is also vital, promoting a proactive approach toward data protection, including regular audits and feedback mechanisms. Furthermore, collaboration with IT experts is necessary to develop secure data systems, especially with the increasing use of technology in healthcare.

Implications of the Study

This study explored the knowledge and perception of HCPs about patients' data security and privacy in clinical research and factors that could improve data privacy and security. Prior publications and participation in clinical research were associated with improved knowledge of HIPAA and NCBE rules and regulations. These data could be used to develop targeted educational programs for HCPs to improve HCP knowledge and awareness and to enroll them in more clinical research projects to enhance their knowledge about the rules and regulations. Raising the awareness of data privacy and security among HCPs could help promote public trust in clinical research. Several factors could affect the privacy and security culture [24], and new technologies are being developed to enhance healthcare security [25]. Future studies are required to evaluate factors that influence data privacy and security in clinical research and evaluate the methods that can be used to enhance privacy and security culture and systems.

Study Limitations

The study has several limitations. The research was limited by the sample size and demographics and affiliation to a single institution; therefore, generalization of the findings to other HCPs in different centers could be an issue. The study is cross-sectional, and a causal effect cannot be established. Additionally, using an online questionnaire could have introduced selection bias. Also, the limited number of publications by the survey participants may be a source of bias in interpreting the results. The accuracy of self-reported data is another issue. HCPs may be reluctant to participate or report their knowledge because of concerns about their professional competence.

Conclusions

Patients' data privacy and security remain vital to clinical research. Identifying factors that could compromise data privacy and security, enhancing HCP knowledge, and fostering a culture of data privacy can

ultimately enhance the integrity of clinical research. HCPs realize the role of IRB/REC to maintain data privacy and security. Enrollment of HCPs in clinical research and continuous education could improve HCP knowledge of regulatory rules.

Statement of Ethics

The questionnaire was distributed only after receiving approval from the Research Ethics Committee of Prince Sultan Military Medical City Research Council Number 1407. Participants were informed of the aim and content of the study. No identifiable information was collected from the participants, i.e., names, ID numbers, or contact information. Written informed consent was obtained from all study participants for participation in the study.

Conflict of Interest Statement

The authors have no conflicts of interest to declare.

Funding Sources

Funding was not received for this study.

Author Contributions

Monirah A. Albabtain, Dalal Alotaibi, Nourah Almazial, and Haneen Mohammed Alghosoon conceptualized the quantitative part of the research designed. Nouf Aloudah conceptualized the qualitative part of the research designed. All authors contributed to the writing of the proposal and final manuscript and approved the final manuscript. Amr A. Arafat analyzed the data and wrote the results.

Data Availability Statement

The data that support the findings of this study are not available publicly due to institutional regulations but will be made available upon justifiable request from the corresponding author and after approval of the institution's IRB to release the data. Further inquiries can be directed to the corresponding author.

References

- 1 Nair SC, Ibrahim H. Assessing subject privacy and data confidentiality in an emerging region for clinical trials: United Arab Emirates. *Account Res.* 2015;22(4):205–21. <https://doi.org/10.1080/08989621.2014.942452>.
- 2 Allen AL. Coercing privacy. *Wm Mary L Rev.* 1998;40:723.
- 3 Turn R, Ware W. Privacy and security issues in information systems. *IEEE Trans Comput.* 1976; 100(12):1353–61. <https://doi.org/10.7249/p5684>.
- 4 Gostin LO, Lazzarini Z, Neslund VS, Osterholm MT. The public health information infrastructure: a national review of the law on health information privacy. *JAMA.* 1996;275(24):1921–7. <https://doi.org/10.1001/jama.275.24.1921>.

- 5 Almutairi SS. A modified technology acceptance model (TAM) for implementation of privacy in health information systems in Saudi Arabia (Doctoral dissertation. Rutgers University-School of Health Related Professions.
- 6 Asiri HA. Health information privacy laws and policies: do we need more policies in the arab world? *J Health Inform Developing Countries*. 2013;7(2).
- 7 Rockwern B, Johnson D, Snyder Sulmasy L; Medical Informatics Committee and Ethics Professionalism and Human Rights Committee of the American College of Physicians. Health information privacy, protection, and use in the expanding digital health ecosystem: a position paper of the American College of Physicians. *Ann Intern Med*. 2021;174(7):994–8. <https://doi.org/10.7326/M20-7639>.
- 8 Gayler BW. HIPAA regulations. *J Am Coll Radiol*. 2005;2(2):200–2. <https://doi.org/10.1016/j.jacr.2004.12.003>.
- 9 NCBE- standards and regulations. 2013. Available form: <https://ncbe.kacst.edu.sa/en/standards-and-regulations/>.
- 10 May R, Denecke K. Security, privacy, and healthcare-related conversational agents: a scoping review. *Inform Health Soc Care*. 2022;47(2):194–210. <https://doi.org/10.1080/17538157.2021.1983578>.
- 11 Oh SR, Seo YD, Lee E, Kim YG. A comprehensive survey on security and privacy for electronic health data. *Int J Environ Res Public Health*. 2021;18(18):9668. <https://doi.org/10.3390/ijerph18189668>.
- 12 Atkins L, Francis J, Islam R, O'Connor D, Patey A, Ivers N, et al. A guide to using the Theoretical Domains Framework of behaviour change to investigate implementation problems. *Implement Sci*. 2017;12(1):77–8. <https://doi.org/10.1186/s13012-017-0605-9>.
- 13 Saldaña J. The coding manual for qualitative researchers. In: *The coding manual for qualitative researchers*; 2021; p. 1–440.
- 14 Adarmouch L, Felaefel M, Wachbroit R, Silverman H. Perspectives regarding privacy in clinical research among research professionals from the Arab region: an exploratory qualitative study. *BMC Med Ethics*. 2020;21(1):27–6. <https://doi.org/10.1186/s12910-020-0456-9>.
- 15 Creswell JW, Plano Clark VL. Designing and conducting mixed methods research. In: *Department of family medicine*. 3rd ed. University of Michigan: Sage Publications; 2022.
- 16 Tashakkori A, Teddlie C. *SAGE handbook of mixed methods in social & behavioral research*. 2nd ed. Thousand Oaks, CA: SAGE Publications, Inc.; 2010.
- 17 Tariq RA, Hackert PB. Patient confidentiality. *StatPearls*.
- 18 Karasneh R, Al-Mistarehi AH, Al-Azzam S, Abuhammad S, Muflih SM, Hawamdeh S, et al. Physicians' knowledge, perceptions, and attitudes related to patient confidentiality and data sharing. *Int J Gen Med*. 2021;14:721–31. <https://doi.org/10.2147/IJGM.S301800>.
- 19 Ness RB; Joint Policy Committee, Societies of Epidemiology. Influence of the HIPAA privacy rule on health research. *JAMA*. 2007; 298(18):2164–70. <https://doi.org/10.1001/jama.298.18.2164>.
- 20 Demirsoy N, Kirimlioglu N. Protection of privacy and confidentiality as a patient right: physicians' and nurses' viewpoints. *Biomed Res*. 2016;27(4):1437–48.
- 21 Mohamed AM, Ghanem MA, Kassem AA. Knowledge, perceptions and practices towards medical ethics among physician residents of University of Alexandria Hospitals, Egypt. *East Mediterr Health J*. 2012;18(9):935–45. <https://doi.org/10.26719/2012.18.9.935>.
- 22 Alrajeh NA. HIPAA based healthcare information security qualitative assessment application of information security for Saudi hospitals. In: *IADIS International Conference e-Health 2010 (part of MCCSIS 2010)*. 2010. p. 199–204.
- 23 Mohammad Nejad E, Begjani J, Abotaleb G, Salari A, Ehsani SR. Nurses awareness of patients rights in a teaching hospital. *J Med Ethics Hist Med*. 2011;4:2.
- 24 Salih SA, Abdelkader Reshia FA, Bashir WA, Omar AM, Ahmed Elwasefy S. Patient safety attitude and associated factors among nurses at Mansoura University Hospital: a cross sectional study. *Int J Africa Nurs Sci*. 2021;14:100287. <https://doi.org/10.1016/j.ijans.2021.100287>.
- 25 Khan S, Saravanan VN, Lakshmi TJ, Deb N, Othman NA. Privacy protection of healthcare data over social networks using machine learning algorithms. *Comput Intell Neurosci*. 2022:2022.