UKR Journal of Medicine and Medical Research (UKRJMMR)
Homepage: https://ukrpublisher.com/ukrjmmr/
Email: submit.ukrpublisher@gmail.com
Volume 2, Issue 6, November-December 2026 ISSN: 3107-5061 (Online)

Cybersecurity Risk Awareness and Patient Data Protection among Pharmacy Students in Gregory University Uturu (GUU) and Abia State University (ABSU)

Nwitu, Sorie Pius[1]; Nweke, Emmanuel Onyekachi PhD [2] & Edozie Precious Tochi[3]

[1]Department of Pharmacy, Professor Kesley Harrison Hospital, Rivers State Hospital Management Board. https://orcid.org/0009-0006-57875125
[2]Department of Office Technology and Management, Captain Elechi Amadi Polytechnic, Rumuola, Port Harcourt, Rivers State, Nigeria. Orcid Id: http://orcid.org/000-0003-3507-2285
[3]Department of Clinical Pharmacy and Biopharmacy, College of Pharmacy, Gregory University, Uturu.

***Corresponding Author**: Nwitu, Sorie Pius
DOI: *https://doi.org/10.5281/zenodo.24040545*

Article History
Original Research Article
Received: 06 September 2026
Accepted: 15 October 2026
Published: 07 November 2026
Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial **4.0 International License (CC BY-NC 4.0),** which permits non-commercial use, sharing, and reproduction in any medium, provided the original author(s) and source are appropriately credited.
Citation: Nwitu, Sorie Pius, Nweke, Emmanuel Onyekachi PhD, & Edozie Precious Tochi. (2026). Cybersecurity risk awareness and patient data protection among pharmacy students in Gregory University Uturu (GUU) and Abia State University (ABSU). UKR Journal of Medicine and Medical Research, 2(6), 01-13.

Abstract

The study investigated cybersecurity risk awareness and patient data protection among pharmacy students in Gregory University Uturu (GUU) and Abia State University (ABSU). This study adopted the correlational research design. The study population of the study consisted of 260 students in 300-600 Levels in both universities. It adopted the stratified random technique to select 85 students from each of the two universities under review; to give a total sample size of 170. It used a questionnaire instrument tagged, Cyber Security Awareness and Patients' Data Protection Questionnaire (CSAPDPQ). Out of 170 copies of questionnaire distributed, 150 copies were duly completed and returned and the study used the returned copies for its analysis. The study used mean and standard deviation to answer the research questions at mean benchmark of 2.5 and regression to test the null hypotheses at .05 significance level. The study found that there is a significant relationship between pharmacy students at Gregory University and Abia State University, located in Uturu, Abia State cyber security awareness and patients' data protection. The study concluded that students' exposure or training on cyber security prepares their awareness on patients' data protection. That the extent of cyber security awareness relates to the extent of patients' data protection in the field. Students who are not exposed to cyber security training are bound to encounter patients' data compromise when in practice. It recommended that training institutions of Gregory University Uturu and Abia State University should embark on rigorous training programme or seminars on cyber security awareness for its Pharmacy students, among others.

***Keywords**: Cyber security, Patients, Data Protection, Students, Awareness.*

Introduction

The digital transformation of healthcare has significantly improved patient care, operational efficiency, and data accessibility. Pharmacy is a very crucial component of medical sciences which borders on ethics and observance to rules. One of such rules includes patients' confidentiality, reputation and human prestige. This study contemplates that cyber security awareness should be part of the learning component of pharmacy students. Patients' data protection involves the shielding personal information of the sick to a third party. It is also in the known that apart from confidentiality compromise, such information when exposed might also be used as a crime bait. The study establishes that it is the responsibility of the universities and the students themselves to ensure effective cyber security awareness to enable the learning or understanding of patients' data protections.

Ahmed (2022) defines cybersecurity as the strategies, procedures, tools and practices used to defend computer systems, networks and information against cyber attacks and unauthorized use. It is the preservation of digital assets, data and activities within cyberspace and maintaining the information's confidentiality, integrity and availability.

Ransomware and other types of malware, phishing, data theft, and, in recent times, cyberattacks with the help of artificial intelligence (AI) are common cybersecurity threats. A successful cybersecurity strategy creates a robust defense mechanism that prevents access, modification, deletion or destruction of an organization's systems and sensitive data, as well as those of the users.

Additionally, cybersecurity is crucial for safeguarding and preventing unauthorized entry into computer systems and digital devices that may lead to disrupting, disabling or exploiting the devices. The pharmaceutical sector has significant amounts of critical data that are used daily in their operations, making them an appealing target for cybercriminals, hackers and data breaches. Data loss is a significant cybersecurity threat as it can lead to loss of trust among stakeholders, financial losses, and legal actions. Thus, it is critical for pharmaceutical firms to adopt a comprehensive cybersecurity approach to safeguard their valuable information from such threats and ensure its security (Olanrewaju et al., 2025).

Pharma companies are facing a plethora of cybersecurity threats. However, these risks can be mitigated with the use of proper security measures such as employee awareness training, two factor authentication, data encryption, regular data backup, network segmentation and penetration testing (Fausett et al., 2021). Pharmaceutical companies should keep apprised of new cyber threats and best security practices, and should continuously conduct a surveillance program of their information systems to look for suspicious behavior. Furthermore, working closely with cybersecurity experts can assist pharmaceutical companies in creating and executing successful security strategies. These professionals can provide valuable insights into current threats and weaknesses in these systems, helping organizations to enhance their security strategies and better prepare for potential cyberattacks. Cybersecurity risks are a big challenge to the pharmaceutical industry, as a whole. As the pharmaceutical sector increasingly relies on digital technology, it becomes even more crucial to implement strong security measures to safeguard critical data and ensure the reliability and security of pharmaceutical operations.

There have been related studies relating to information technology transformation ans cyber security. (Adinarayana et al., 2025) carried out a study on data compromise in hospitals and patients identity in Nigeria. Osama, et al, (2023) equally did a study on impact of cyber breach on drug administration in health centres in Osun State. However, there has not been a study on cyber security awareness among pharmacy students and patients' data. This study is therefore geared towards closing the gap and to provide scholarship on the need to prepare pharmacy students upon graduation to use cyber facilities to protect patients' data.

Statement of Problem

The infusion of technology and digitalization into pharmacy offers significant benefits, including improved patient care and wider access to medicines through e-pharmacy, recording and verifying transactions using the blockchain, etc. With these advancements come some cybersecurity risks that threaten the confidentiality, integrity, and availability of patient data and the misuse of digital systems. Despite these risks, there is limited literature that exists in the future of pharmacy work, especially concerning technology adoption, and even less knowledge available on the risks that digitalization poses to pharmacy. There is also limited research available that assesses pharmacy students' preparedness to tackle patient-related cybersecurity challenges in Nigeria. This knowledge gap poses a threat to future pharmacists' ability to practice safely in an increasingly digital healthcare environment. The ongoing training and education of students and practitioners to keep them updated and in line with the technologies advancements in health to assure them on optimising the benefits of digital health. Pharmacy schools should be involved so that the new generation of pharmacy graduates will foster the adoption and accelerated uptake of digital health. In general, pharmacy schools have to prepare pharmacy students not just technically on some of these technologies but also on innovative and novel ways of using these for pharmaceutical care. This study would therefore to investigate the level of cybersecurity risk awareness and patient data protection among pharmacy students in Gregory University Uturu (GUU) and Abia State University (ABSU).

Aims And Objectives of Study

The primary aim of this study is to investigate the of cybersecurity risk awareness and patient data protection among pharmacy students in Gregory University Uturu (GUU) and Abia State University (ABSU), with the following specific objectives:

1. To determine level of pharmacy students' current exposure to cyber security awareness and patient data protection during their academic training and field training.
2. To find out level of pharmacy students' ability to prevent cyber threats and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU)

Research Questions

The following research questions guided the study:

1. To what extent does pharmacy students' exposure

to Cyber security awareness relates to patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU)?

2. To what extent does pharmacy students' ability to prevent cyber threats relates to patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU)?

Hypotheses Of the Study

The following hypotheses guided the study:

1. There is no significant relationship between pharmacy students' exposure to Cyber Security Awareness and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU).
2. There is no significant relationship between pharmacy students' ability to prevent cyber security threats and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU).

Literature Review

Theoretical Framework

The study is premised on the Protection Motivation Theory (PMT) first proposed by Rogers (1975; amended in 1983) which explains the situation in which individuals are driven to perform protective behaviours when faced with threat. The idea argues that two key cognitive processes, the danger appraisal and coping appraisal, determine whether or not people will defend themselves. The theory is relevant to the current investigation in that threat appraisal for an individual includes the seriousness of the threat and the probability of being affected by the threat. Coping assessment, in contrast, entails evaluating if the protective behaviour proposed is beneficial and whether the person is capable of successfully executing it, which is known as self-efficacy (Rogers, 1975).

Conceptual Clarifications

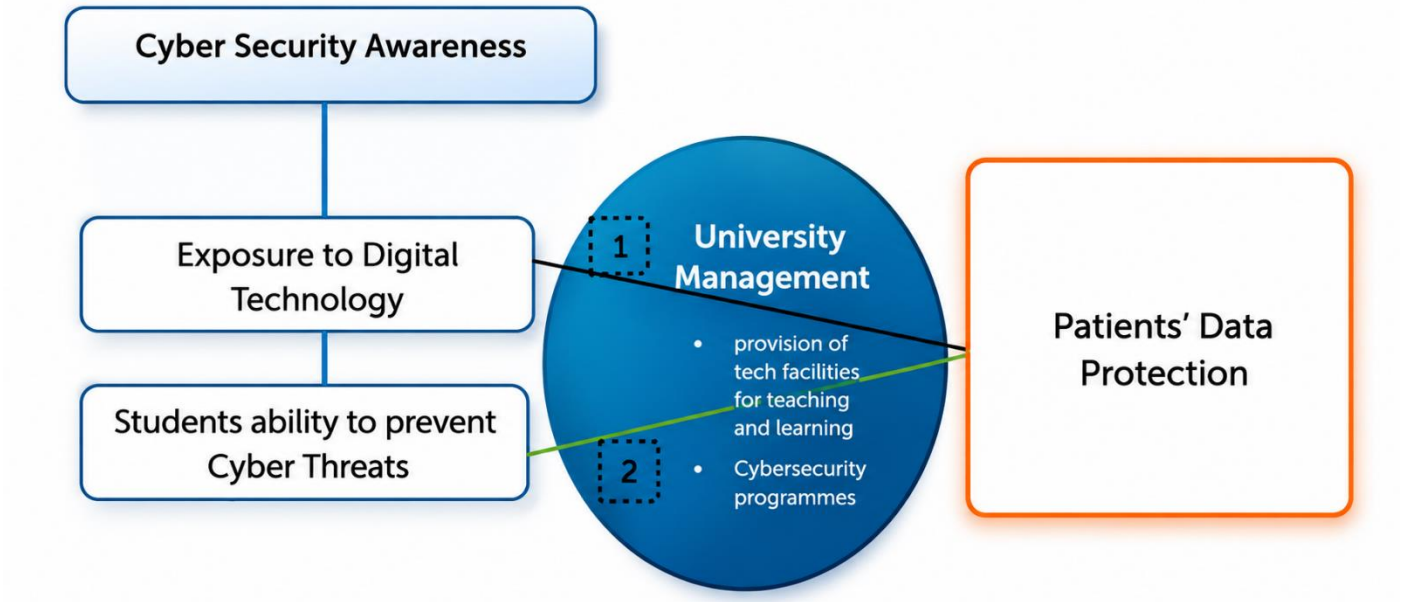

Fig. 1: Researchers' Guide, 2026

Concept of Cyber Risk Awareness

Digital technology is rapidly transforming the global pharmacy sector, enhancing efficiency, productivity, and flexibility in healthcare delivery. The integration of technologies such as automation, artificial intelligence (AI), computerization, and robotics has become increasingly important for reducing operational costs and improving the quality of pharmaceutical services (Almeman, 2024). Digital transformation refers to a process through which organizations improve their operations and outcomes by leveraging information, computing, communication, and connectivity technologies to bring about substantial changes. According to the World Health Organization (WHO, 2016), digital health is an emerging field with considerable potential to improve clinical research, reduce healthcare costs, and enhance the quality and effectiveness of healthcare services. As a multidisciplinary domain, digital health aims to strengthen patient monitoring, diagnosis, treatment, prevention, rehabilitation, and long-term care delivery (Gordon et al., 2017).

The digital pharmacy market has experienced remarkable growth and is projected to expand at an annual rate of 14.42%, reaching an estimated market value of

approximately $35.33 billion by 2026 (Shambhavi., 2022). This growth reflects the increasing adoption of digital technologies within pharmacy practice and highlights their potential to reshape healthcare delivery. Digital health technologies have also made significant contributions to improving medication adherence using text messaging services, mobile applications, virtual pillboxes, and smart medication containers. Furthermore, Internet of Things (IoT)-enabled devices, including fitness trackers, heart rate monitors, and insulin pumps, allow healthcare professionals to remotely monitor patient health indicators such as physical activity levels, blood pressure, heart rate, and medication concentrations. These technologies facilitate timely interventions and personalized treatment adjustments.

Cyber Security and Patient Data Protection

According to Ali (2025), cybersecurity's objective is to safeguard patients' data against unauthorized access, which may lead to a loss of confidence in the system and digital attacks against those who are affected. In general, Cybersecurity is the security of individuals, information systems and data from cyberattacks using appropriate technologies, processes and policies. I. H. Sarker et al. (2020) define cyber security as the security of communication and information technology systems from electronic attacks, and from various threats in the Internet. It covers a variety of aspects: it is about the measures undertaken for the protection of information technology infrastructure, data, communication systems, and the information contained in, processed and transmitted by them. The International Telecommunication Union (ITU) describes cybersecurity as “the collection of security technologies, policies, concepts, security safeguards, and guidance, risk management strategies, procedures, training, best practices, safeguards and technologies that may be applied to securing the cyber environment.” Besides defending organizational and individual assets, cybersecurity aims to ensure and maintain their crucial security features in the cyber environment against cyber risks (Quayyum et al., 2021).

Cybersecurity is quickly emerging as a technological and societal problem for governments and communities. While awareness and understanding of cyber security threats is still relatively low, it is increasing in importance. People's online actions, in particular, are not always sufficiently conscious and careful to safely use the internet (De Bruijn & Janssen, 2017). Thus, cyber-security can be defined as activities and processes to safeguard communication and information systems from exploitation, unauthorized access, and hacking attempts. Knowledge and awareness of cyber security are therefore critical for individuals to be able to identify, prevent and respond to cyber threats such as ransomware attacks (Amankwa, 2021).

Patients’ Data Protection

Ali, (2025) states that putting adequate measures in place to prevent the loss or theft of personal data is essential for maintaining the trust of patients and the public. Silva, (2002) opines that what involves patients’ data information are the nature of ailment, complaints, drug administration history, genetic histories and treatment timeline. Patients’ data protection equally includes electronic prescriptions (e-prescriptions) represent a fundamental component of digital pharmacy, modernizing the conventional prescribing process. By replacing paper-based prescriptions with digital records, they minimize errors associated with illegible handwriting and enable the secure, accurate transfer of prescription information between healthcare providers and pharmacies. Studies have shown that e-prescription systems can reduce medication errors by up to 85% while enhancing the efficiency, accuracy, and safety of medication dispensing processes. Additionally, these systems streamline pharmacy workflows, shorten patient waiting times, and support better healthcare outcomes by enabling faster, more reliable service delivery (Ali, 2025).

Free (2010) reaffirms that patients data protection covers remote pharmaceutical services which includes telepharmacy. Telepharmacy remote consultations and medication management, pharmacists can provide care without physical contact, greatly improving access to pharmacy services in rural and underserved communities. This approach enhances patient convenience, increases access to essential medications, and promotes better adherence to treatment plans, which in turn improves patient satisfaction. Research, including studies in, has shown that telepharmacy was essential in ensuring continuity of care during crisis periods, highlighting its potential to become a long-term component of healthcare delivery systems

Patients’ Cyber Security Risk and Data Protection

The CIA Triad is a fundamental model in information security that outlines the three essential principles for establishing and maintaining a robust, effective security framework (Sikder, 2023). The National Institute of Standards and Technology (NIST) identifies the CIA Triad as one of the fundamental frameworks traditionally used to evaluate the security of information and communication technology (ICT) systems. Furthermore, various professional organizations and industry bodies have endorsed the CIA Triad as a key model for assessing and rating information security practices (Shoufan & Damiani, 2017).

Confidentiality is a fundamental principle of information security that focuses on protecting sensitive information from unauthorized access, disclosure, or misuse. It requires that access to data be restricted to individuals, organizations, or systems with legitimate authorization, thereby preserving the privacy and security of information. This principle is both an ethical and legal obligation, particularly in environments where personal, financial, or organizational data are handled (Osazuwa, 2023).

Maintaining confidentiality is critical because unauthorized exposure of information can result in financial losses, reputational damage, legal liabilities, and a loss of stakeholder trust. To mitigate these risks, organizations implement various security measures that limit access to sensitive information and ensure that only approved users can view or process it (Chai & Zolkipli, 2021).

Several technological mechanisms support confidentiality. Encryption techniques, such as the Advanced Encryption Standard (AES), convert data into secure formats that can only be accessed by authorized parties possessing the appropriate decryption keys. Modern cryptographic approaches, including key aggregation methods, enable efficient management of multiple encryption keys while maintaining strong security. Access control systems further strengthen confidentiality by regulating user permissions, supporting secure data modification, preventing unauthorized activities such as replay attacks, and ensuring that users interact only with information relevant to their authorized roles (Osazuwa, 2023)

Additionally, authentication mechanisms help verify the identity of users before granting access to protected resources, thereby reducing the likelihood of unauthorized data exposure. Together, these safeguards ensure that sensitive information remains accessible only to authorized entities, reinforcing confidentiality as a core pillar of the CIA Triad and an essential requirement for secure information and network systems (Sikder, 2023).

Pharmacy Students Cybersecurity Risk Awareness

Cybersecurity risk awareness has become increasingly important for healthcare students as digital technologies continue to transform healthcare delivery. The widespread adoption of electronic health records (EHRs), telemedicine, mobile health applications, cloud computing, Internet of Things (IoT) devices, and artificial intelligence has improved the efficiency and accessibility of healthcare services. However, these technological advancements have also expanded the healthcare sector's exposure to cyber threats (World Health Organization (WHO), 2021).

Healthcare organizations are frequent targets of cyberattacks because they manage large volumes of sensitive patient information, including personal, financial, and medical data. Cyber threats such as phishing, ransomware, malware, data breaches, and social engineering attacks can compromise patient privacy, disrupt healthcare services, and result in significant financial and reputational losses (Adegoke, Achen, Foreman, Nwaobi, & Begley, 2022). Consequently, healthcare students, as future healthcare professionals, must develop adequate cybersecurity risk awareness to identify potential threats and adopt safe digital practices. Cybersecurity risk awareness also enables healthcare students to understand the importance of protecting the confidentiality, integrity, and availability of health information. By recognizing common cyber risks and their potential consequences, students are better equipped to handle patient data responsibly and comply with ethical, legal, and professional obligations related to information security (Chai & Zolkipli, 2021).

Furthermore, cybersecurity risk awareness contributes to the protection of patient privacy and helps maintain patient trust in healthcare systems. Patients are more likely to engage with digital health services when they are confident that their information is being managed securely (Adegoke, Achen, Foreman, Nwaobi, & Begley, 2022). Healthcare students who understand cybersecurity risks are more likely to follow established security protocols, such as using strong passwords, identifying phishing attempts, safeguarding mobile devices, and adhering to data protection regulations. Awareness of cybersecurity risks also supports continuity of care by reducing the likelihood of cyber incidents that could disrupt clinical operations or compromise access to critical information systems (Lupiana, 2008).

Methods

This study adopted the correlational research design. It measured the relationship between pharmacy students at Gregory University and Abia State University, located in Uturu, Abia State cyber security awareness and patients' data protection. The study focused on students in 300-600 Levels, with population of population consists of 260 registered pharmacy students in both universities who have undergone some form of field training, such as Industrial training, Externship, and Clerkship. It adopted the stratified random technique to select 85 students from each of the two universities under review; to give a total sample size of 170. It used a questionnaire instrument tagged, Cyber Security Awareness and Patients' Data Protection Questionnaire (CSAPDPQ). Out of 170 copies of questionnaire distributed, 150 copies were duly completed and returned and the study used the returned copies for its analysis. The study used mean and standard deviation to answer the research questions at mean benchmark of 2.5 and regression to test the null hypotheses at .05 significance level. The

data for the study was obtained from the registry departments of both universities. Information was obtained by a displayed students data at the registry department of both universities. The instrument was validated by an expert in Measurement and Evaluation from Niger Delta University, Wilberforce Island, Bayelsa State. The reliability of the instrument was tested using Cronbach alpha and obtained .971>.71 which showed that the instrument was reliable.

Results

Demographics of Respondents

Table 1: gender of respondents			
Gender		**Frequency**	**Percent**
	male	65	43.3
	female	85	56.7
	Total	**150**	**100.0**

Table 1 above showed that there were 65 male respondents representing 43.3%. Female respondents were 85 representing 56.7%. There were more female respondents.

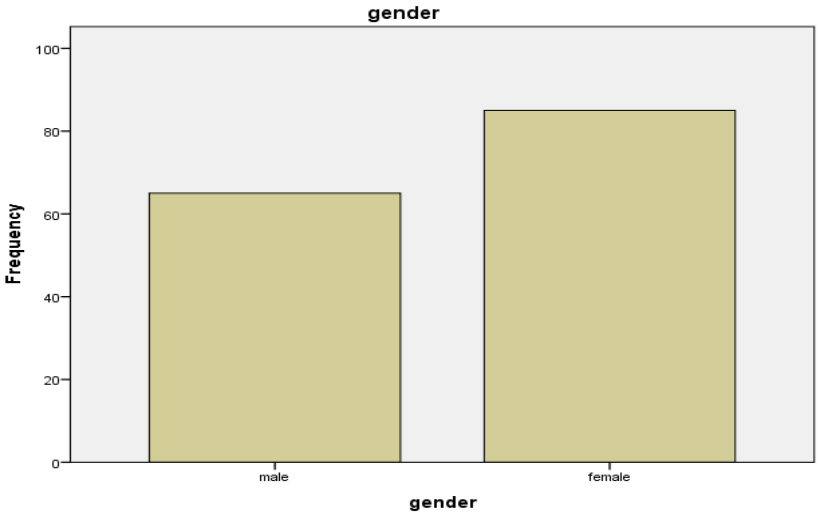

Figure 3: Bar Chart of Gender Distribution

Table 2: University of respondents			
University		**Frequency**	**Percent**
	Gregory University Uturu	71	47.3
	Abia State University	79	52.7
	Total	**150**	**100.0**

Table 2 above showed that 71 respondents or 47.3% were from Gregory University, Uturu while 79 representing 52.7% were of the Abia State University, Uturu. There were more respondents from Abia State University Uturu

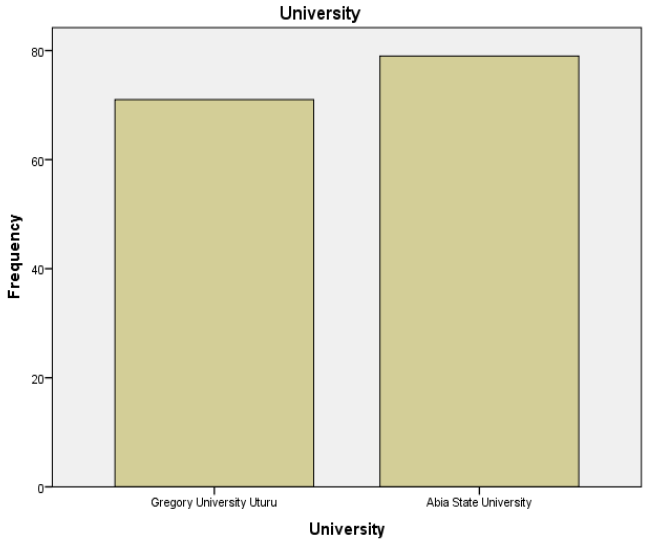

Figure 4: Bar Chart of University Distribution

Table 3: Age of Respondents			
Age of Respondents		**Frequency**	**Percent**
	18-22	52	34.7
	23-27	44	29.3
	28-32	18	12.0
	33-above	36	24.0
	Total	150	100.0

Table 3 above that age brackets 18-22 were 52 or 34.7%, 23-27 were 44 or 29.3%, 28-32 were 18 representing 12%, while 33-above were 36 or 24%. Age bracket 18-22 were predominant.

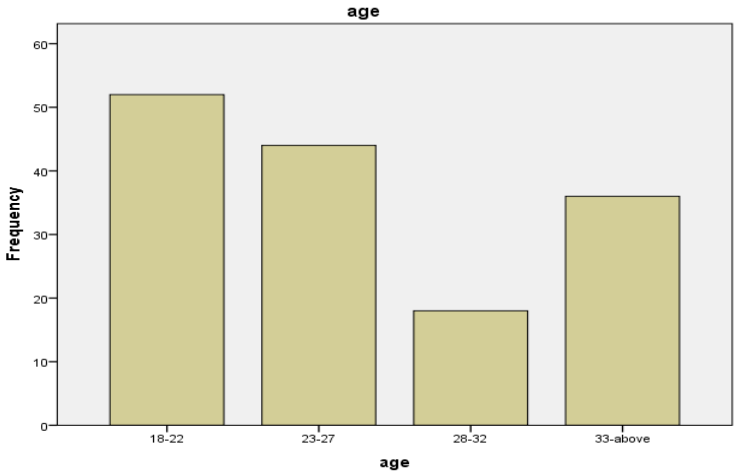

Figure 5: Bar Chart of Age Distribution

Research Question 1: To what extent does pharmacy students' exposure to Cyber security awareness relates to patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU)?

Table 4: *Mean and Standard Deviation of level of pharmacy students' exposure to Cyber security awareness and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU))*

Items	**N150**	**Mean**	**Std. Deviation**	**Remark**
1. I have used electronic systems for accessing medical or drug information		2.72	1.15	High extent
2. I have used hospital or clinical digital systems during IT training, externship, or clerkship		2.65	1.50	High extent
3. I frequently use digital platforms such as e-learning systems, hospital databases, or clinical apps during my pharmacy training		1.84	1.12	Low extent
4. I have encountered systems that store electronic patient medication records		2.63	1.12	High extent
5. I am familiar with electronic prescription systems		1.63	1.01	Low extent
6. I have attended seminars or workshops related to digital health technologies		1.56	1.20	Low extent
7. I was exposed to digital technologies as a part of my school's curriculum		2.72	1.24	High extent
8. I am aware that connecting personal devices to pharmacy networks may introduce cybersecurity risks		2.66	1.33	High extent
Grand Mean		**2.30**	**1.21**	**Low Extent**

Table 4 above showed, in item 1, a mean score of 2.72 and STD 1.152, implying that respondents' high extent that they have used electronic systems for accessing medical or drug information. Item 2 with mean score of 2.65 and an STD of 1.50, which showed high extent that respondents have used hospital or clinical digital systems during IT training, externship, or clerkship. Item 3, with a mean score of 1.84 and STD 1.12, showed respondents low extent that they frequently use digital platforms such as e-learning systems, hospital databases, or clinical apps during my pharmacy

training. Item 4, with a mean score of 2.63 and STD 1.21, implied high extent that respondents have encountered systems that store electronic patient medication records. Item 5, with a score of 1.63 and STD 1.01, implied low extent that respondents are familiar with electronic prescription systems. Item 6, with a mean score of 1.56 and an STD of 1.20, showed low extent that respondents had attended seminars or workshops related to digital health technologies. Item 7, with a mean score of 2.72 and an STD of 1.24, showed that respondents high extent that they were exposed to digital technologies as part of their school's curriculum. Similarly, item 8 with a mean score of 2.66 and STD 1.33 showed that respondents high extent that aware that connecting personal devices to pharmacy networks may introduce cybersecurity risks.

Thus, the aggregate mean score of 2.30 and STD 1.21 implied a low level of current awareness of basic cybersecurity concepts and risks among pharmacy students in Gregory University Uturu (GUU) and Abia State University (ABSU)

Research Question 2: To what extent does pharmacy students' ability to prevent cyber threats relates to patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU)?

Table 5: *Mean and Standard Deviation of extent of pharmacy students' ability to prevent cyber threats relates to patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU)*

Items	N=150	Mean	Std. Deviation	Remark
9. Electronic patient medication records are vulnerable to cyberattacks		2.18	1.37	Low extent
10. Unauthorized access to electronic prescriptions can result in medication errors		2.36	.48	Low Extent
11. Cybersecurity breaches can compromise patient confidentiality in pharmacy practice		2.90	1.22	High extent
12. Weak password practices increase the risk of unauthorized access and data theft		2.70	.40	High Extent
13. Ransomware or malware attacks can disrupt pharmacy services and delay medication dispensing		2.54	1.30	High Extent
14. Phishing emails can be used to steal healthcare login credentials		2.06	1.35	Low extent
15. Pharmacists have a professional responsibility to protect electronic patient data		2.01	1.18	Low extent
16. Poor cybersecurity practices can negatively affect patient safety		2.85	1.31	High Extent
17. Protecting patient data is as important as dispensing the correct medication		2.86	1.17	High Extent
18. Reporting suspicious digital activity is part of a pharmacist's professional duty.		3.33	.70	High Extent
19. Using one password across multiple digital systems makes the pharmacy vulnerable to cyberattacks		2.62	1.24	High Extent
Grand Mean	**150**		**2.63**	**.71 High Extent**

Table 5 above showed in item 9 a mean score of 2.18 and STD 1.37, which implies low extent that respondents that electronic patient medication records are vulnerable to cyberattacks. In item 10, the mean score of 2.36 and STD .48 equally indicates low extent that respondents that unauthorized access to electronic prescriptions can result in medication errors. Item 11, with a mean score of 2.90 and STD 1.22, showed that respondents high extent that cybersecurity breaches can compromise patient confidentiality in pharmacy practice. Item 12, with a mean score of 2.70 and STD .40, implied high extent that respondents that weak password practices increase the risk of unauthorized access and data theft. Item 13, with a mean score of 2.54 and STD 1.30, showed high extent that respondents ransomware or malware attacks can disrupt pharmacy services and delay medication dispensing. Table 14, with a mean score of 2.06 and an STD of 1.35, showed low extent that respondents phishing emails can be used to

steal healthcare login credentials. Item 15, with a mean score of 2,01 and an STD of 1.18, showed low extent that respondents pharmacists have a professional responsibility to protect electronic patient data. Mean scores of 2.85 and STD 1.17 showed high extent in item 16 that respondents have poor cybersecurity practices can negatively affect patient safety. Item 17, with a mean score of 2.86 and STD 1.17, showed that respondents high extent that protecting patient data is as important as dispensing the correct medication. Item 18, with a mean score of 3.33 and STD 1.70 implies high extent that respondents' reporting suspicious digital activity is part of a pharmacist's professional duty. Item 19, with a mean score of 2.62 and STD 1.24, showed high extent that respondents using one password across multiple digital systems makes the pharmacy vulnerable to cyberattacks.

Thus, the grand mean score of 2.63 and STD .71 implies high extent that pharmacy students' ability to prevent cyber threats relates to patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU).

Test of Hypotheses

Ho_1: There is no significant relationship between pharmacy students' exposure to Cyber Security Awareness and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU

***Table** 7: Regression Analysis of relationship between pharmacy students' exposure to Cyber Security Awareness and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU*

Regression

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.742[a]	.551	.538	.78381

a. Predictors: (Constant), exposure to Cyber Security Awareness

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	109.159	4	27.290	44.420	.000[b]
	Residual	89.081	145	.614		
	Total	198.240	149			

a. Dependent Variable: Patient Data Protection

b. Predictors: (Constant), Cyber Security Awareness

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.868	.203		4.277	.000
		.253	.070	.329	3.596	.000
		-.442	.066	-.432	-6.701	.000
		.030	.066	.029	.453	.001
		.571	.090	.505	6.355	.000

a. Dependent Variable: Patient Data Protection

Table 7 above showed in R value of .742[a] Square of .551 Adjusted R square of .538 Std error of the estimate of .78381 and p-value of .001<.05 which showed a significant relationship between pharmacy students' exposure to Cyber Security Awareness and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU. The null hypothesis is therefore rejected.

$H0_2$: There is no significant relationship between pharmacy students' ability to prevent cyber security threats and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU).

***Table 8**: Regression Analysis of relationship between pharmacy students' ability to prevent cyber security threats and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU).*

Regression

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.441[a]	.621	.638	.78241

c. Predictors: (Constant), ability to prevent cyber security threats

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	108.144	4	17.290	32.310	.000[b]
	Residual	67.071	145	.214		
	Total	185.220	149			

a. Dependent Variable: *patient data protection*

d. Predictors: (Constant), *ability to prevent cyber security threats*

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.778	.201		3.277	.000
		.433	.070	.322	3.176	.000
		-.242	.025	-.352	-7.601	.000
		.040	.029	.019	.653	.000
		.231	.070	.506	6.215	.000

a. Dependent Variable: Patient Data Protection

Table 8 above showed in R value of .441[a] Square of .621Adjusted R square of .638Std error of the estimate of .78241and p-value of .000<.05 which showed a significant relationship between pharmacy students' ability to prevent cyber security threats and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU). The null hypothesis is therefore rejected

Summary of Findings

The findings of the study, based on tested hypotheses showed thus:

1. There is a significant relationship between pharmacy students' exposure to Cyber Security Awareness and patients' data protection in

Gregory University Uturu (GUU) and Abia State University (ABSU).

2. There is a significant relationship between pharmacy students' ability to prevent cyber security threats and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU).

Discussion of Findings

The Findings of the study are discussed hereunder based on the objectives of the study:

Pharmacy Students' Exposure to Cyber Security Awareness and patient data protection

The findings of the study revealed a significant relationship between pharmacy students' exposure to Cyber Security Awareness and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU). The findings of the present study have been buttressed by the works of Ahmed (2022), stating that the cyber security programmes to students for digital health integration relates to data protection of patients. Data was collected from pharmacy schools, academics, students, and practitioners using structured questionnaires and analyzed using descriptive and inferential statistics. This implies that students' exposure to cyber security awareness would forestall the threat or danger of loss of patients' data and other comprises.

Pharmacy Students' Ability to prevent cyber security threats and patient data protection

The findings of the study revealed a significant relationship between pharmacy students' ability to prevent cyber security threats and patient data protection in Gregory University Uturu (GUU) and Abia State University (ABSU). The finding of the present study has been corroborated by Ahmed (2022), who conducted a cross-sectional survey to examine pharmacy students' awareness of cybersecurity, data privacy, and the need for cybersecurity education in digital prescription platforms. This implies that if student pharmacists are not able to prevent cyber security, has the tendency to tamper or compromise patient data in terms of confidence and even trace of medication or administration.

Conclusion

The study investigated level of cybersecurity risk awareness and patient data protection among pharmacy students in Gregory University Uturu (GUU) and Abia State University (ABSU). It found that students' exposure or training on cyber security prepares their awareness on patients' data protection. That the extent of cyber security awareness relates to the extent of patients' data protection in the field. Students who are not exposed to cyber security training are bound to encounter patients' data compromise when in practice.

Recommendations

Based on the findings of the study, the study therefore recommends the following:

1. Training institutions of Gregory University Uturu and Abia State University should embark on rigorous training programme or seminars on cyber security awareness for its Pharmacy students.
2. Pharmacy students of Gregory University Uturu and Abia State University should engage on self-awareness programmes on cyber security that has bearing with the patients' data protection.

References

1. Abernethy, A. E. (2022). The Promise of Digital Health: Then, Now, and the Future. *NAM perspectives*, pp. 10-16.
2. Adegoke, A., Achen, N., Foreman, J., Nwaobi, J., & Begley, R. D. (2022). Cyber security as a threat to health care. *Journal of Technology and Systems, 4*(1), 32–64. doi:10.47941/jts.1149
3. Adepoju, K. O., & Opele, J. K. (2023). Practice of health information management in Nigeria: Opportunities, challenges, and future directions. *Journal of Applied Information Science and Technology, 16*(2), 98–113.
4. Ahliyah, A. A. (2022). Pharmacists' Perceptions of Telepharmacy in Pharmacy Services During the Covid-19 Pandemic in Malang City. *Doctoral Dissertation, Maulana Malik Ibrahim State Islamic University*, 1-32.
5. Ahmed, N.-B. (2022). Cybersecurity in Healthcare System : Evaluation and Assessment of the Cybersecurity readiness of Mobile Field Hospital's Resilience. *Library and information sciences. IMT -MINES ALES - IMT - Mines Alès Ecole Mines - Télécom*, 1-128.
6. Al-Shourbaji, S. A.-J. (2016). A study of cyber security awareness in educational environment in the middle east. *Journal of Information & Knowledge Management, vol. 15*(no. 01), p. 1650007.
7. Alsulami, F. T. (2025). A scoping review on the impact of versatile digital health innovations on pharmacy education. *Frontiers in Medicine, 12*, 1577494. doi:10.3389/fmed.2025.1577494
8. Bernard, R., Bowsher, G., & Sullivan, R. (2020). Cyber security and the unexplored threat to global

health: A call for global norms. *Global Security: Health, Science and Policy, 5*(1), 134–141. doi:10.1080/23779497.2020.1865182

9. Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. *MIS Quarterly, 39*(4), 837–864. doi:10.25300/MISQ/2015/39.4.5

10. Chai, K. Y., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. *Journal of ICT in Education, 8*(2), 34–42. doi:10.37134/jictie.vol8.2.4.2021

11. Coventry, L., & Branley, D. (2018). Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward. *Maturitas, 113*, 48–52. doi:10.1016/j.maturitas.2018.04.008

12. Cymer, E., Szymczyk, T., Matczuk, M., & Kisała, P. (2025). Medicine Students' Cybersecurity Awareness and Its Improvement. *19th International Technology, Education and Development Conference (INTED2025)* (pp. 6684–6689). Valencia, Spain: IATED Academy. doi:10.21125/inted.2025.1727

13. Dorosti, A. M., Soheili, A., Gholizad Gougjehyaran, H., & Seyednazari, M. A. (2026). Empowering the Nursing Workforce for Cyber-Resilience: Strategic Preparedness and Care Management During Hospital Cyberattacks. *PLOS Digital Health, 5*(3), e0001291. doi:10.1371/journal.pdig.0001291

14. Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security, 31*(1), 83–95. doi:10.1016/j.cose.2011.10.007

15. Istepanian R, L. S. (2007). *M-Health: Emerging Mobile Health Systems.* New York: Springer Science + Business Media.

16. Joshi, S. (2025). 5 Major Cybersecurity Challenges Pharma Faces in 2025. *Pharma Now.*

17. Källander K, T. J. (2013). Mobile health (mHealth) approaches and lessons for increased performance and retention of community health workers in low-and middle-income countries: a review. *Journal of medical Internet research*, e17.

18. Katsantonis, N. M., Kotini, I., Fouliras, P., & Mavridis, I. (2019). Conceptual Framework for Developing Cyber Security Serious Games. *2019 IEEE Global Engineering Education Conference (EDUCON)* (pp. 872–881). Dubai, United Arab Emirates: IEEE. doi:10.1109/EDUCON.2019.8725125

19. Kay, M. S. ((2011). Health: new horizons for health through mobile technologies. *World Health Organization*, 7;64(7):66-71.

20. Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for Academia. *Information*, 417.

21. Labrique, V. L. (2013). Health innovations as health system strengthening tools: 12 common applications and a visual framework. *Global health: science and practice*, 1;1(2):160-71.

22. Lupiana, D. (2008). *Development of a Framework to Leverage Knowledge Management Systems to Improve Security Awareness.* Dublin: Dublin Institute of Technology.

23. M. Bada, A. M. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* arXiv preprint arXiv.

24. O'Brien, N., Martin, G., Grass, E., Durkin, M., Darzi, A., & Ghafur, S. (2020). *Cybersecurity in Healthcare: Comparing Cybersecurity Maturity and Experiences Across Global Healthcare Organizations.* SSRN. doi:10.2139/ssrn.3688885

25. Olanrewaju Ogundojutimi, E. A. (2025). Predicting Cybersecurity Risk in Healthcare Pharmacy Infrastructures. *Global Journal of Cyber Security (GJCS)*, pp. 1-20.

26. Organization, W. H. (2016). *Monitoring and Evaluating Digital Health Interventions: a Practical Guide to Conducting Research and Assessment.*

27. Osazuwa, O. M. (2023, December). Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature. *International Journal of Innovative Science and Research Technology, 8*(12), 1946–1955. doi:10.5281/zenodo.10464076

28. Peltoniemi T, S. R. (2021). Electronic prescription as a driver for digitalization in Finnish pharmacies. *BMC Health Services Research*, 1-9.

29. Porterfield, A. e. (2014). Electronic prescribing: improving the efficiency and accuracy of prescribing in the ambulatory care setting. *Online Research Journal Perspectives in Health Information Management*, 1-5.

30. Rathore AS, B. R. (2010). Process analytical technology (PAT) for biopharmaceutical products. *Analytical and Bioanalytical Chemistry.*, 137-154.

31. Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology*, 93–114.

32. Salama, R., Altrjman, C., & Al-Turjman, F. (2024). Healthcare cybersecurity challenges: A look at current and future trends. In R. Salama, C. Altrjman, & F. Al-Turjman, *Computational Intelligence and Blockchain in Complex Systems* (pp. 97–111). Elsevier. doi:10.1016/B978-0-443-13268-1.00003-0

33. Santo K, R. S. (2016). Mobile phone-based interventions to improve medication adherence in hypertension and cardiovascular disease: Systematic review and meta-analysis. *European Heart Journal – Quality of Care and Clinical Outcomes*(ISSN: 2058-1742 (Print), 2058-5225 (Online)), 2(4):237-249.

34. Shoufan, A., & Damiani, E. (2017). On Inter-Rater Reliability of Information Security Experts. *Journal of Information Security and Applications, 37*, 101–111. doi:10.1016/j.jisa.2017.10.004

35. Sikder, A. S. (2023). Cybersecurity Framework for Ensuring Confidentiality, Integrity, and Availability of University Management Systems in Bangladesh. *International Journal of Imminent Science & Technology*, 3006-3116.

36. Silva, R. d. (2022). Digital pharmacists: the new wave in pharmacy practice and education. *International journal of clinical pharmacy, vol. 29*, 1421-1431.

37. Sophos. (2024). *The State of ransomware in healthcare 2024.* Sophos Ltd. Retrieved from https://news.sophos.com/en-us/category/sophos-state-of-ransomware/

38. Tarhan, N. (2022). Digital data security awareness: A Study with Pharmacy Students. *FABAD Journal of Pharmaceutical Sciences, 47*(2), 193–200. doi:10.55262/fabadeczacilik.1134564

39. Tariq RA, V. R. (2024). *Medication Dispensing Errors and Prevention.* Treasure Island (Florida): StatPearls Publishing. Retrieved from https://www.ncbi.nlm.nih.gov/books/NBK519065/

40. *dicine, 10*(2). doi:10.1371/journal.pmed.1001382

41. U.S. Food and Drug Administration. (2020). *What is digital health?* Silver Spring, MD: Digital Health Center of Excellence, FDA. Retrieved from https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health

42. World Health Organization (WHO). (2021). *Global Strategy on Digital Health.* Geneva, Switzerland: World Health Organization.

43. Yalçınkaya, T., Tuncer, M., Tuncer, G. Z., Erol, A., & Yücel, S. Ç. (2025). Nursing students' cybersecurity practices and perceptions and cybersecurity crime awareness: A cross-sectional study. *Nurse Education Today, 153*, 106818. doi:10.1016/j.nedt.2025.106818

44. Zapata BC, F.-A. J. (2015). Empirical studies on usability of mHealth apps: A systematic literature review. *Journal of Medical Systems, 39*(2), 1–19. doi:10.1007/s10916-014-0182-2