SN Computer Science (2024) 5:257
https://doi.org/10.1007/s42979-023-02589-0

ORIGINAL RESEARCH

Identifying the Software Quality Attributes that Affect Patient Portal Adoption in Trinidad and Tobago

Marcus Rawlins[1] · Xuejun Yu[1]

Received: 20 November 2021 / Accepted: 28 December 2023

Abstract

Trinidad and Tobago's public health sector currently uses paper records, posing challenges for both patients and healthcare providers. Transitioning to an electronic health record system with a patient portal is vital. Identifying and highlighting user requirements is crucial for this improvement, promising better healthcare services and data accessibility. With that being said, this study aims to identify key functional user requirements for a patient portal in Trinidad and Tobago, assess potential adoption barriers, and define credibility attributes for the credibility evaluation framework. The research question is focused on understanding user expectations and factors that may hinder adoption. The research methodology consisted of three main steps. First, a comprehensive review of existing standards, guidelines, and journals on patient portals was conducted to gather insights into best practices and key software credibility attributes. Second, an online survey was designed to collect data from 390 citizens of Trinidad and Tobago aged 18 years and over. The survey focused on gathering user preferences, expectations, and concerns regarding the implementation of patient portal adoption. Lastly, the survey responses were analyzed to identify key functional user requirements for the system. The results of the study revealed 16 key functional user requirements for the electronic health records system, providing insights into the features and functionalities expected by users. Among the identified adoption barriers, resistance to change and inadequate cybersecurity laws were found to be significant factors that may hinder the successful implementation of the system. Additionally, 15 credibility attributes were selected based on the use'r requirements to establish the system's reliability and trustworthiness. Understanding user requirements and addressing adoption barriers are crucial for developing an effective patient portal system in Trinidad and Tobago's public health sector. The identified credibility attributes will guide the evaluation framework, enhancing the system's adoption and contributing to improved patient and provider care.

Keywords Patient portal · Electronic health records · Software credibility · Software quality · Adoption

Introduction

Trinidad and Tobago's healthcare system is two-tiered (private and public), where public healthcare is available to all citizens for free and offers a wide variety of services [1]. The record management system currently implemented within the public healthcare sector is primarily paper-based. Each health facility contains its own system for the filing of records and patients generally have to go to that particular health facility to access their records (personal communication, August 1st, 2021). Paper-based record management systems have many inefficiencies that not only affect patient care but also provider care. These issues may include inconsistent templates, limited security, lack of scalable storage, inadequate audit trails, errors in patient records, and duplication of records [2, 3].

To mitigate some of these challenges, digital record management systems have been developed and implemented in healthcare through the use of Electronic Health Records. An Electronic Health Record (EHR) is a digitized version of a patient's medical history but is also not limited to medical tests, X-rays/imaging, and long-term medical history [4, 5]. EHRs are usually utilized by healthcare providers and have been widely adopted throughout many countries such as Finland [6], Sweden [5] and the United States of America [7], providing healthcare providers with proper management of patient records [4, 8]. One of the key features of EHR

✉ Marcus Rawlins
marcusraw@hotmail.com

[1] School of Software, Beijing University of Technology, Beijing, China

Published online: 09 February 2024

systems is the ability to allow patients to be able to access their health records online, primarily with the assistance of a patient portal.

A patient portal is a secure online system offered by healthcare providers to allow patients to access their health records as well as provide additional functionalities such as appointment creation, prescription, and consolation requests [9, 10]. Patient portals can be standalone or an added functionality of EHR software. This system carries many benefits including improved focus on patient care, better patient communication, easy access to health records, streamlined patient registration and administrative tasks and improved clinical outcomes [11]. Epic's MyChart, athenaOne, Finland's My Kanta, and Estonia's e-Health Patient Portal are among some of the patient portals utilized worldwide [12, 13].

Although patient portals carry many benefits, patients may not be as inclined to utilize such a system for a variety of reasons. Lack of knowledge on how to use the system [9], lack of trust in the security, integrity and confidentiality of information [8, 14], and resistance to change [10], are among the factors as to why users many not be inclined to use or adopt such a system. Age has also shown to have some influence on the user's trust as older users may not be as inclined to use such a system [5, 10]. As part of the requirements process of the software development cycle (SDLC), it is important to consider these factors to develop a system that meets the user's requirements. Using a software credibility evaluation model throughout the development of the SDLC can ensure that all aspects of the system are met and the credibility of the software is maintained.

Software credibility can be defined as a process that is used to determine if the actual behavior of the application corresponds with the expected result [15]. This process is completed by analyzing the software using various methods throughout the development lifecycle [16].

Figure 1 shows an overview of the credibility framework which consists primarily of testing between the software development life cycle (SDLC) and the credibility evaluation model. The model was developed based on research conducted by previous studies [15, 17, 18]. The first process of the framework begins with the requirements analysis phase of the SDLC where the credibility attributes are defined based on the functional requirements and the behavior declaration files are generated based on the credibility attributes. As the life cycle enters the testing phase, the behavioral declaration files are assessed and credibility testing is performed to evaluate the credibility of the system. This system is continually evaluated even after implementation has been completed. Based on the credibility test evaluation, the events are logged and a response is sent to the main system where the results of the test are analyzed. The behavior declaration files are then regenerated as the system is updated or if the requirements are changed during maintenance.

As Trinidad and Tobago do not currently have a patient portal system implemented, it was considered as a good subject to identify the factors that can affect patient portal adoption and also identify the functional requirements for a patient portal health records system. In this paper, we aim to: (i) identify the key functional user requirements for a potential electronic health records system in Trinidad and Tobago; (ii) assess potential adoption barriers; and (iii) define the credibility attributes based on the functional requirements as the first phase of the credibility evaluation model. This research will be conducted using quantitative research tools such as a survey for data collection. As part of the results, key functional user requirements will be identified, potential barriers will be assessed, recommendations will be provided

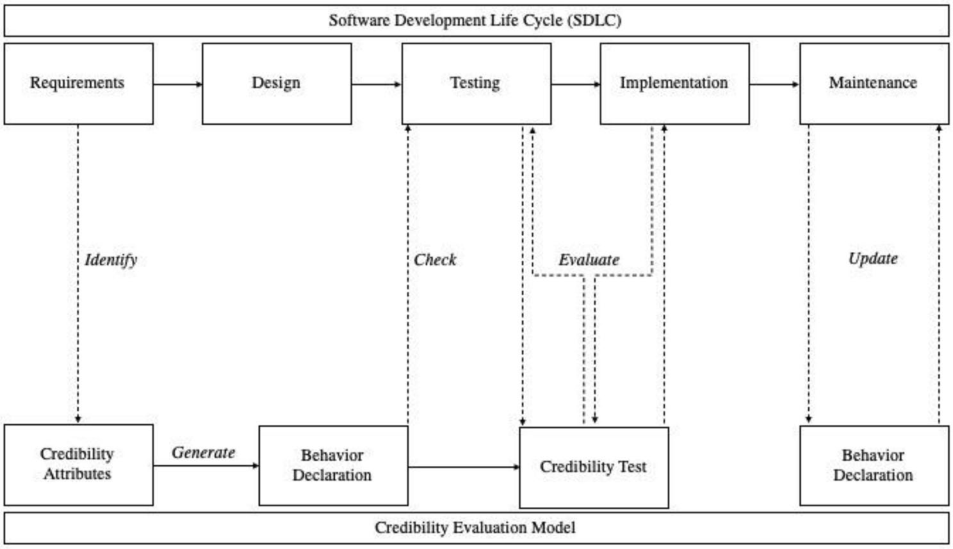

Fig. 1 Overview of the credibility evaluation framework

and the credibility attributes for the evaluation model will be defined.

Literature Review

Several studies have been conducted with regard to software credibility and how it is applied in various applications. Yu and Dan [19] developed a credibility demand analysis method that focused on reviewing the credibility of risk-driven mobile application software. Xu and Tang [17] developed a calculation method to determine the user's behavior based on trust. Rodriguez-Perez et al. [20], conducted a study on the reproducibility and credibility of empirical software engineering (ESE) which consisted of reviewing publications that use the Sliwerski, Zimmermann and Zeller (SZZ) algorithm. Yu and Xiao [15] proposed a credibility evaluation model based on the application behavior declaration (ABD) which is generated throughout the entire software development life cycle. The model is based on a "WORD" and "DEED", where the "WORD" defines what the system should do and the "DEED", represents the actual behavior of the system. Yang and Yu [18] proposed a credibility evaluation model, used to evaluate the cloud end user's behavior. They identified the evaluation indicators of the user behavior credibility based on behavioral data analysis. Yu and Wang [21] proposed a model for generating credibility test cases based on the immune algorithm. Fang et al. [16], developed a credibility evaluation model based on simulation systems by exploring simulation models.

Overall Methodology

This project's overall methodology includes an organized approach with numerous essential components. The first step is to undertake an extensive study on patient portal gidelines and standards to help identify the key software quality attributes, which will serve as the foundation for the succeeding phases. Once the essential guidelines and standards have been defined, the following stage is to create a survey that will be used to collect user answers from Trinidad and Tobago individuals.

After collecting survey responses, the attention focuses on examining and analyzing the data. This stage is critical in determining the most important and relevant functional user needs to the users. Concurrently, survey results are utilized to establish credibility qualities that will assure the solution's dependability, security, usability, and overall performance.

The responses are used to help identify some of the key functional user requirements and develop credibility attributes based on the requirements identified. The process of identifying the credibility attributes is based on the credibility evaluation model proposed by Yu and Xiao where the evaluation model is integrated into the different phases of the Software Development Life Cycle starting from the requirements gathering phase [15]. By incorporating credibility evaluation early on, we prioritize the trustworthiness of the solution and maintain the highest standards of quality throughout the development process.

Reviewal of Standards and Guidelines on Patient Portals

To identify some of the key software attributes utilized by patient portals, we have conducted research on some standards and guidelines that patient portals should contain.

The International Organization for Standardization (ISO) and the Health Insurance Portability and Accountability Act (HIPAA) provide a variety of standards and guidelines for the protection of information in regard to security, integrity, confidentiality and availability. The ISO/IEC 27799:2016 [22] extends from the ISO/IEC 27002:2013 [23] which highlights the importance of security as well as the need for security controls to be implemented at various levels to ensure the protection and effectiveness of data with special emphasis on confidentiality, integrity and availability which are crucial in ensuring the preservation of information. Health information is considered to be among the most confidential information which helps to ensure that privacy is maintained. The guidelines further state that integrity is an important component of the protection of health information by ensuring that the information is accurate and auditable. Health information should be available and remain operational in the event of system failures and attacks as well as natural disasters.

The HIPAA of 1996 [24], provides a level of standards and rules that companies and associates called covered entities should develop to provide effective safeguards that will ensure the integrity, confidentiality and availability of electronic protected health information (e-PHI) such as patient portals. Some HIPAA-compliant patient portal software include EPIC MyChart and Athenahealth [25, 26].

Related Studies on Patient Portals

Research on various elements of patient portals have been undertaken. Following a study of the guidelines and standards, we decided to look at studies that primarily focus on software quality elements such as availability, integrity, security, and confidentiality.

Moll et al. [5], studied the patients' experiences of accessing their EHRs using the Swedish National patient portal. Focusing primarily on the availability of information, they were able to identify the reasons why users accessed the system and also why it was important for this information to be available to them. The results showed that users were more inclined to use the system if key features such as the ability to view records online, prescription requests and appointment management were available.

A study conducted by Keshta and Odeh [27] highlighted that security is among the most important factors to be considered when implementing and utilizing patient portals. They have found that healthcare professionals and patients are generally concerned about the safety of the information and have proposed measures that can be utilized to help improve the system. These measures included technical and administrative safeguards to protect the records from unauthorized use. Security is among one of the key attributes that can influence a user's adoption of the system. Users are generally concerned about the safety of their information; therefore, it is important to have strong security protocols implemented [28].

Techapanupreed and Kurutach [29] defined integrity as one of the key aspects to ensure that data remain confidential and safe. Information stored online should be safeguarded and protected from allowing unauthorized users access to manipulate the information. Medical information should be accessed primarily by the healthcare practitioner but additional personnel such as admin staff may also have access to view this information. Users may not feel safe if the information is modified by other personnel other than healthcare personnel. If unauthorized personnel access the records, this can lead to potential data breaches [8].

Some users may not want to have certain types of information available online as they may fear those additional personnel such as may be privy to this information or fear of information being breached. Users should have the option to choose what kind of sensitive information they want to be able to access online as users are generally concerned about who has access to their information [8]. Confidentiality of information is one of the key aspects with regard to healthcare. If confidentiality and trust are broken, it can affect the user's trust in the system as well as affect the security and integrity of information.

Selection of Software Quality Attributes for a Patient Portal

Based on a review of ISO standards [22, 23], HIPAA requirements, and prior research, we were able to identify and describe critical software quality features to consider when designing a patient portal, as shown in Table 1. These characteristics include availability, security, integrity, and confidentiality.

Design of Survey

The survey was developed based on the software quality attributes identified in Table 1. Following the research practice of the guidelines and frameworks, the survey was designed to cover six key areas:

- *Demographics*: consisted of 10 questions—age, gender, educational background, location, access to the internet, devices available and purposes for accessing the internet.
- *Availability*: consisted of 7 questions—types of information available, frequency of accessing the system and also preferred choice to access the information.
- *Security*: consisted of 6 questions—security measures such as multifactor authentication, access control and security policies.
- *Integrity*: consisted of 4 questions—user notification of account access and authenticity of information entered by various healthcare personnel.

Table 1 Description of software quality attributes based on HIPAA requirements, ISO standards, and prior research

Attribute	Description
Availability	• Information should be available to users in various forms such as using websites or mobile applications • Patients should be able to do basic functionalities such as: view medical records, make appointments and or prescription requests, test records and request consultation [8] • Information should always be readily available for the user to access at any time of the user's convenience
Security	• Traditional security measures consist of a secure username and password • Additional security measures such as multifactor authentication (SMS/email authentication), 3rd party authentication, one-time password (OTP), should be adopted to provide advanced protection to the system • Security protocols such as password requirements and change policies should also be implemented [36] • Access control should also be considered to ensure the unauthorized access of users [29]
Integrity	• Information should be entered only by authorized personnel • Records should be accessed only by the user and authorized personnel [8] • Audit trails are also an important asset that keeps a log of record access • Users should be notified when their accounts have been accessed or information has been modified
Confidentiality	• Personal health information should remain confidential • Information such as sexual health, family history, doctors' consultations and prescriptions are among the most type of sensitive information [8] • Users should have the option to select who can access their health information

- *Confidentiality*: consisted of 3 questions—types of confidential information and non-medical personnel access to confidential information.
- *Adoption:* consisted of 3 questions—opinion of patient portal adoption and factors.

Distribution of the Survey

Before the distribution of the survey, 15 participants were invited to complete the survey, provide feedback on how the survey could be improved, advise on if additional content to be added and also identify potential errors. 12 participants completed the survey and the feedback was impactful in the restructuring of questions regarding security and confidentiality. Additional feedback from the group led to the development of an additional section of the survey which focused on adoption and consisted of 3 questions, focusing on the preparedness of a patient portal system and also additional factors that can potentially hinder adoption of such a system. The sample group was then asked to retake the survey with the new changes.

The survey was administered as an electronic survey using Survey Monkey, consisting of 6 sections with a total of 33 questions. The survey was distributed via the main social media platforms used in the country which included Facebook, WhatsApp, Instagram and LinkedIn. The survey was posted on the author's social media platforms and also sent to family and friends, who later shared the survey on their social media platforms, as this was the most effective way of distributing the survey. The survey was voluntary and no incentives were provided for completed surveys.

The survey was tailored toward the citizens and residents of Trinidad and Tobago, 18 years and older who had internet access. Approximately 79% or 1.085 million citizens are considered to be of adult age and with an internet penetration of 77% or an average of 838,705 citizens had access to the internet [30, 31]. Using Slovin's formula [32], the minimum sample size of the survey was calculated with a confidence level of 95% and a margin of error of 5% which equaled to 384 participants. Only responses from Trinidad and Tobago residents were taken into consideration.

Results

Analysis of Survey Results

The results of the survey were collected over 3 weeks. A total of 484 responses were recorded. Approximately 390 respondents completed the survey, resulting in a completion rate of 81%. Only completed responses are analyzed and the results are analyzed based on the format of the survey. The sample test group accounted for about 3% (12/390) of the survey. The results are analyzed using a combination of descriptive statistics, Kruskal–Wallis testing for Likert-scale questions and chi-squared testing to understand the significance between variables. IBM SPSS was used to conduct the statistical tests.

Table 2 Age range and gender of respondents ($n = 390$)

Age range	Male	Female	Other	Total (n)	Total (%)
18–24	17	23	1	41	11
25–34	65	71	2	138	35
35–44	38	60	0	98	25
45–54	16	38	0	54	14
55–64	12	27	0	39	10
65 +	7	13	0	20	5
Total	155	232	3	390	100%

Table 3 Educational background of respondents ($n = 390$)

Educational level	Male	Female	Other	Total (%)	Total (n)
Primary School	0	2	0	1	2
Secondary School	24	37	2	16	63
Undergraduate	80	119	1	51	200
Postgraduate	44	57	0	26	101
PhD	5	4	0	2	9
Other (please specify)	2	13	0	4	15
Total	155	232	3	100%	390

Demographics

The demographic section focused on key aspects of the respondents such as age, gender and educational level. Table 2 shows the varying age groups compared with the gender. Approximately 59% (232/390) respondents identify as female, 40% (155/390) as male and 1% (3/390) as other. The results show that 71% (277/390) of the respondents are within the age range of 18–44 and 55% (154/277) of that range identify as female. This shows that a majority of respondents who identify as female are within the age range of 18–44 and account for 66% of the overall female respondents. A similar trend is shown for those who identify as male with the majority of male respondents between the range of 18–44 (120/155, 77%). A chi-test was conducted to determine if there is a relationship between age and gender and the results showed that there is no statistically significant relationship between gender and the age range ($\chi^2(10) = 11.5$, $P = 0.313$).

Table 3 shows the results of the educational level based on gender with over 79% (310/390) of the respondents having at least an undergraduate degree or higher. This is similar to the results of the test group where 92% (11/12) of the respondents have an undergraduate degree or higher. This also shows that the majority of respondents in the study are well educated.

Availability

Prior to this research, 58% (228/390) of respondents had not heard of a patient portal while 42% (162/390) had some knowledge about the system. Of the 390 responses, 96% (373/390) respondents would like the ability to access their electronic health records online with a majority of the respondents between the age of 25 and 34 (131/373, 35%), followed by the 35–44 (95/373, 25%) age range.

Figure 2 shows various types of information that users would like to have access to via the patient portal. Test results 91% (354/390), medical history 88% (344/390), appointments and billing 84% (329/390) and prescriptions 83% (322/390) are among the most populous types of information that users would like to access.

Security

Figure 3 shows the results of which personnel users will feel comfortable allowing access to their accounts. The results show that respondents will feel safer allowing their healthcare physician (285/369, 77%) to have the most access to their accounts while respondents felt very unsafe allowing their friends to have access (102/365, 28%). The weighted average for each personnel is as follows: primary healthcare physician = 3.94, nurse = 3.26, healthcare administrator = 3.12, receptionist = 2.25, family = 2.95 and friends = 3.01. The Kruskal–Wallis test showed that there is no significant difference between the age and the ratings of the different healthcare personnel ($P = 0.467$).

Figure 4 focuses on the various security mechanisms that are available for users to choose. Results show that respondents will feel the safest accessing the patient portal using traditional security measures along with multifactor authentication and also using traditional security measures in addition to security questions. Table 4 shows the key multifactor mechanisms that were chosen by respondents are SMS

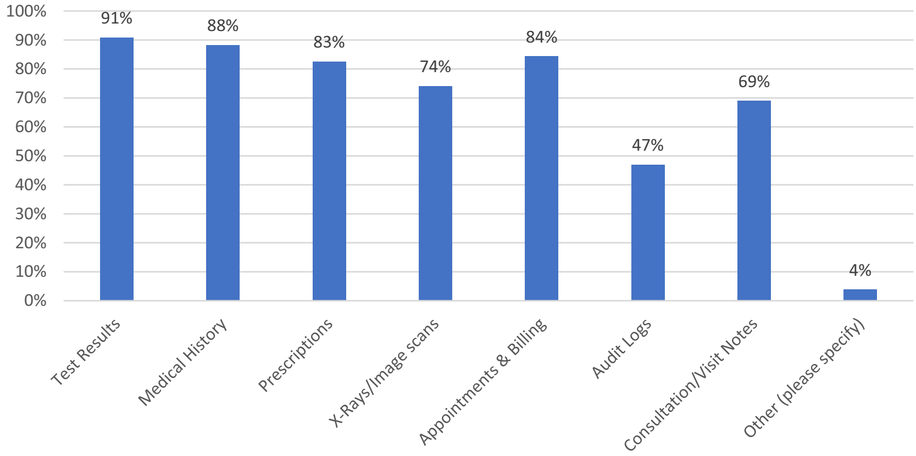

Fig. 2 Types of available information ($n = 390$)

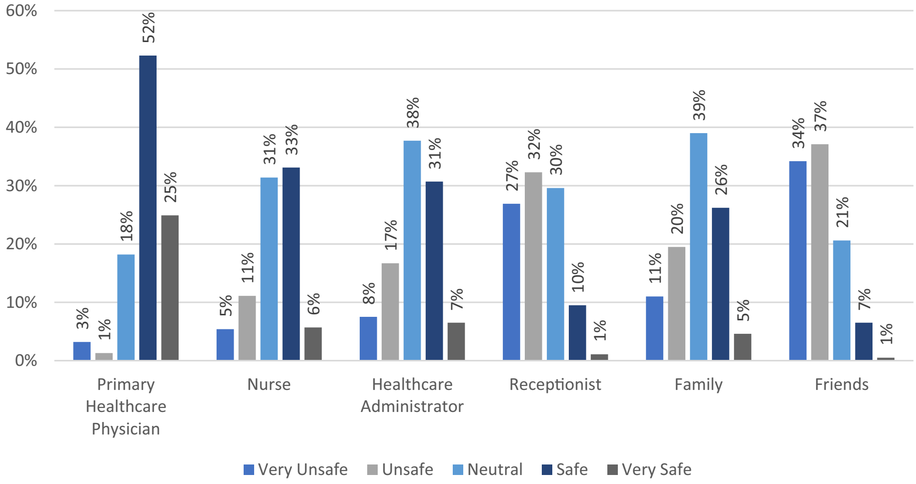

Fig. 3 The stakeholders that respondents feel comfortable accessing their health care information ($n = 369$)

Fig. 4 Access to the patient portal using various security mechanisms ($n=369$)

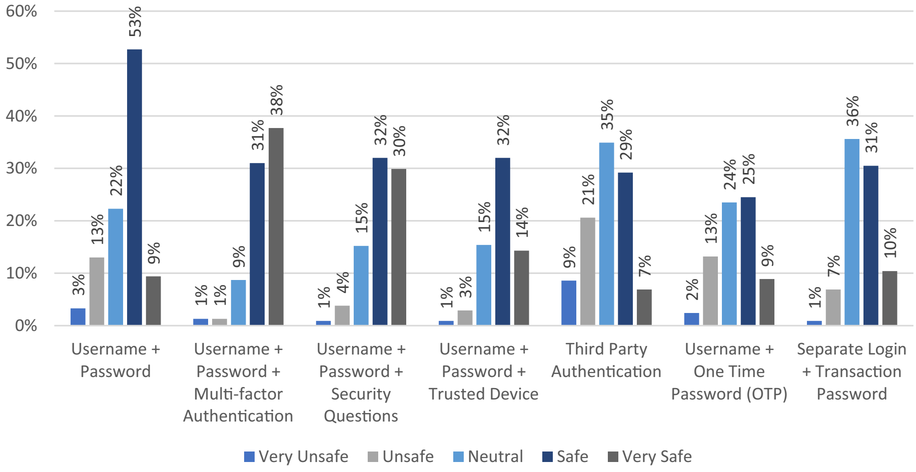

Table 4 Multifactor authentication security mechanisms using SMS and email authentication ($n=379$)

	18–24	25–34	35–44	45–54	55–64	65 +	Total
SMS authentication							
Yes	27	94	59	29	18	8	235
	7%	25%	16%	8%	5%	2%	63%
No	11	40	37	24	21	11	144
	3%	11%	10%	6%	6%	2%	39%
Email authentication							
Yes	24	78	53	33	26	11	225
	6%	21%	14%	9%	7%	3%	60%
No	14	56	43	20	13	8	154
	4%	15%	11%	5%	3%	2%	40%

Table 5 Notification of account access when health records have been accessed ($n=390$)

Condition	Total (%)	Total (n)
Yes	99	389
No	1	1
Total	100%	390

authentication (235/379, 62%) and email authentication (225/379, 59%). Between the two options, the main respondents were between the 25 and 34 age range followed by the 35–44 age range. A chi-test was performed and the results show that there is a relationship between age and SMS authentication ($\chi^2(5)=13.6$, $P=0.018$), where younger respondents were more accepting of SMS authentication than older respondents. There was no relationship between age and email authentication ($\chi^2(5)=2.05$, $P=0.842$).

Integrity

The results of Table 5 show that 99% of the respondents prefer to be notified if their account has been accessed. Respondents were in favor of being notified immediately via email, SMS, or other Messaging platforms (319/390, 86%) which shows a positive response from respondents in regard to audit tracing.

The data in Fig. 5 show the responses based on the level of trust in accepting information that has been entered by the various medical personnel. Healthcare physicians received a high rating with most respondents (320/369, 87%) placing a high level of trust in information inputted by them. Nurses and Lab technicians also received high levels of trust with almost similar statistics of (225/367, 61%) and (228/367, 62%) respectively. As these are the three main parties that users are likely to interact with regarding health information, it is understandable that users would rather trust information entered by these personnel. The Kruskal–Wallis test showed that there is no significant difference between the various personnel and the age of the respondents ($P=0.139$).

Cofidentiality

Table 6 shows the choices of who should be able to access the various forms of information that have been uploaded to the patient portal. Across the 12 categories of information, over 90% of respondents prefer to allow their primary healthcare physician access to their information. Several

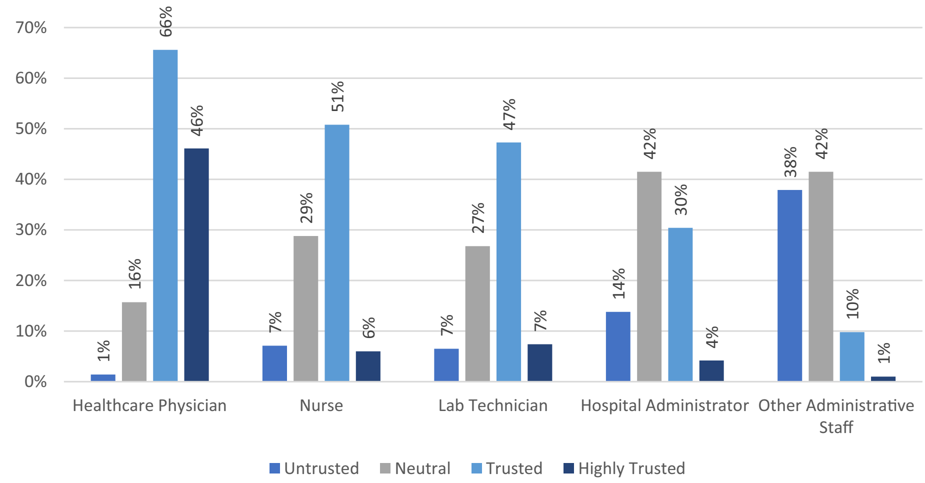

Fig. 5 User trust of the information entered by the various healthcare personnel

Table 6 Categories of information personnel should be able to access ($n=369$)

Type of information	PHP	Nurse	HA	Receptionist	Family	Friends
Contact information	356	244	237	198	210	108
	97%	66%	64%	54%	57%	29%
Address	335	208	239	201	220	114
	91%	56%	65%	55%	60%	31%
Visit history	351	260	218	169	121	27
	95%	71%	59%	46%	33%	7%
Upcoming appointments	337	252	240	274	145	26
	91%	68%	65%	74%	39%	7%
Medical history	362	227	155	34	109	11
	98%	62%	42%	9%	30%	3%
Doctors/consultation notes	359	221	128	30	89	8
	97%	60%	35%	8%	24%	2%
Sexual health	360	162	84	9	44	5
	98%	44%	23%	2%	12%	1%
Prescriptions	356	261	159	79	114	20
	97%	71%	43%	21%	31%	5%
Lab test results	363	222	134	37	89	10
	98%	60%	36%	10%	24%	3%
X-ray/imaging scans	362	230	148	48	102	15
	98%	62%	40%	13%	28%	4%

PHP primary healthcare physician, *HA* healthcare administrator

Kruskal–Wallis tests were conducted to determine the differences between the age and various categories of information. With the exception of X-ray ($P=0.012$), all other categories of information do not show any statistical differences.

Adoption

With regards to the adoption of a patient portal in Trinidad and Tobago, the results show in Table 7 that of the 377 responses, 51% of the respondents believe that Trinidad and Tobago is ready for the adoption of a patient portal, 25% do not believe Trinidad and Tobago is ready for the adoption of a patient portal and 24% are unsure. Most of the respondents who are ready for adoption are between the age of 25 and 54 (150/193, 78%) with the 25–34 age group holding the majority of votes. Using the chi-squared test, the results show that there is no association between age and the readiness factor ($\chi^2(10)=12.22$, $P=0.270$).

Table 8 highlights the respondents' beliefs on the factors that can hinder patient portal adoption in Trinidad and Tobago. The 3 main factors that respondents highlighted are lack of trust in ensuring the integrity, confidentiality and security of information on the patient portal 70% (265/379), lack of adequate cybersecurity laws and regulations 65%

Table 7 Readiness of patient portal adoption in Trinidad and Tobago ($n=377$)

	18–24	25–34	35–44	45–54	55–64	65+	Total
Yes	14	74	46	30	22	7	193
	7%	38%	24%	16%	11%	4%	51%
No	13	27	28	8	9	8	93
	14%	29%	30%	9%	9%	9%	25%
Unsure	11	31	22	15	8	4	91
	12%	34%	24%	16%	9%	5%	24%

Table 8 Factors that hinder the adoption of a patient portal in Trinidad and Tobago. ($n=379$)

	18–24	25–34	35–44	45–54	55–64	65+	Total
Resistance to change							
Yes	22	88	46	34	23	11	224
	6%	24%	12%	9%	6%	3%	60%
No	17	45	50	19	16	8	155
	4%	12%	13%	5%	4%	2%	40%
Lack of digitization of information							
Yes	17	81	39	24	17	8	186
	5%	21%	10%	6%	5%	2%	49%
No	22	52	57	29	22	11	193
	6%	14%	15%	8%	6%	2%	51%
Lack of adequate cybersecurity laws and regulations							
Yes	20	87	64	30	30	16	247
	5%	23%	17%	8%	8%	4%	65%
No	19	46	32	23	9	3	132
	5%	12%	9%	6%	2%	1%	35%
Lack of internet access for citizens							
Yes	10	41	28	17	11	7	114
	3%	11%	7%	4%	3%	2%	30%
No	29	92	68	36	28	12	265
	8%	24%	18%	10%	7%	3%	70%
Lack of trust in ensuring the integrity, confidentiality and security of information on the patient portal							
Yes	21	83	76	38	32	15	265
	6%	22%	20%	10%	8%	4%	70%
No	18	50	20	15	7	4	114
	5%	13%	5%	4%	2%	1%	30%
Lack of infrastructure and financial resources to implement the system							
Yes	15	60	33	18	6	8	140
	4%	15%	9%	5%	2%	2%	37%
No	24	73	63	35	33	11	239
	6%	19%	17%	9%	9%	3%	63%
Lack of education on the usage of technology							
Yes	17	55	23	15	11	4	125
	4%	15%	6%	4%	3%	1%	33%
No	22	78	73	38	28	15	254
	6%	21%	19%	10%	7%	4%	67%
Resistance to having personal information shared online							
Yes	10	58	44	30	18	11	171
	3%	15%	11%	8%	5%	3%	45%
No	29	75	52	23	21	8	208
	8%	20%	14%	6%	5%	2%	55%

(247/379), and resistance to change 59% (224/3379). Using chi-testing to analyze the key leading factors, results show that there is no relationship between age and resistance to change ($\chi^2(5) = 8.40$, $P = 0.135$), and also age and lack of adequate cybersecurity laws and regulations ($\chi^2(5) = 10.53$, $P = 0.061$). There is, however, a strong statistical relationship between age and lack of trust in ensuring the integrity, confidentiality, and security of information on the patient portal ($\chi^2(5) = 15.81$, $P = 0.007$).

Functional User Requirements

Following careful analysis of the results from the survey, we were able to identify some of key the functional user-centered requirements based on the responses of the participants and also from the previous studies conducted. The requirements are based on the characteristics of security, availability, integrity, and confidentiality. The requirements are described in Table 9 below based on the four attributes: security, availability, integrity, and confidentiality.

Respondents were found to be in favor of advanced login security measures aside from traditional login measures (username + password), with multifactor authentication (MFA) among the most populous. This coincides with the ISO Health Informatic guidelines which encourage the adoption of MFA. Among the two MFA measures highlighted in this study, the preferred choice for respondents aged between 18 and 44 is SMS authentication, and email authentication is favored among all age groups. This is expected as not everyone may understand the dynamics of SMS authentication and, therefore, both SMS and email authentication should be an available option for all users. Additional security measures for the system performance may include firewall protection, data encryption and security permissions can also improve how information is stored and accessed. System events can be logged and the patient should be immediately notified via email if their record has been accessed.

Information should also be categorized in different tiers which only certain personnel will have access to. The user should also be given the option to choose who they are willing to grant access to certain types of information as not everyone may feel comfortable sharing information such as sexual health and lab tests results. These requirements are selected based on the responses of the participants. Though this does not fully reflect the entire nation, it can be used as a census to highlight what users may expect from such a system. The patients will be the primary users of this type of system; therefore, it is important to ensure their needs are met.

Selection of Credibility Attributes

As part of the first phase of the credibility evaluation framework [18, 21], the software credibility attributes are defined based on the functional requirements and categorized into four key indicators shown in Table 10. These indicators include the credibility of user access, the credibility of information access, the credibility of information and overall credibility of the system. The attributes identify key requirements that the system should perform to provide a trustworthy and credible system.

The credibility of user access indicator comprises two attributes and focuses on the user's behavior when accessing the system or performing system functions. The user is expected to perform certain functions when accessing their account which includes authenticating their identity using SMS or email authentication and should also reset their password after some time. This is to ensure that the user

Table 9 User-centered functional requirements

Attribute	Functional requirement
Security	1. Login using their email address or ID Number 2. Confirm login identity using email or SMS authentication 3. Reset their password every 45–90 days 4. Control who has access to their health records 5. Notified if an account has been accessed
Availability	6. View and edit basic contact information 7. View medical information 8. Perform functions such as making appointments, processing billings and requesting prescriptions 9. Contact their healthcare provider via the patient portal for consultation or support 10. Download medical information from the portal 11. Use a PIN to access downloaded documents 12. View a log of system events
Integrity	13. Information should be entered only by authorized personnel 14. Information should be signed by the primary physician to confirm the authenticity of the personnel who entered the information 15. User accounts should only be accessed by authorized personnel
Confidentiality	16. Ability to control what kind of information should be accessible to the healthcare provider

Table 10 The selection of the credibility attributes

Indicator	Attribute	Function
The credibility of user access	User login	The user logs into the system using a username and password and is confirmed using a form of multifactor authentication such as SMS or email authentication
	User password policy	The system prompts the user to resets their password every 90 days and confirms their identity using SMS or email authentication and security questions
The credibility of information access	Information access	Authorized personnel should confirm their identity using their ID number, password and SMS authentication to be granted access to patient information
	Security permissions	Personnel has access to patient records based on various security tiers Tier 1: Read-only access Tier 2: Write access only Tier 3: Read and write access
	Data entry	The information must be validated and signed by the healthcare physician to ensure the integrity of information
	Data encryption	Information entered should be encrypted and using various techniques such as AES, RSA, Triple DES, etc
The credibility of information	Information categories	Information is categorized based on different tiers of security and will require additional measures to access some of that information
	Security tiers	Tier 1: Read-only access Tier 2: Read and write access Tier 3: Read-only access and the user has to authenticate identity using multifactor authentication Tier 4: The user should contact the healthcare provider to be granted access to this information
	Information display	Information can be viewed only using the web browser or mobile application where copy and paste functions are disabled
	Downloading information	Information will only be available to download using encrypted PDF documents and will require a 4 PIN code to unlock the document. The PIN will be requested by the user
The credibility of the system	System timeout	The system will timeout after a certain period of time if the user is inactive
	Account suspension	The system will suspend the user's account if the user fails to properly authenticate their identity
	Hashing	Passwords and other security measures inputted should be hashed to protect the integrity of the information; MD5, SHA
	User flagged	The system will flag a user who tries to access information without proper clearance
	Audit log	All system events should be logged and stored as a backup

is who they are by providing the system with the necessary information to confirm their identity.

The credibility of information access indicator comprises of four attributes and is based on access and input of the patient information by the hospital personnel. To ensure the integrity of information entered by healthcare personnel, the personnel is expected to provide the same level of authentication as the user. Hospital personnel will be able to access patient information based on the access that is provided to their account. If the personnel does not have permission to access the patient's record, they will be denied access to the patient's record. All data should, therefore, be signed by the corresponding personnel to ensure the validation of the information and should be encrypted in the database using various encryption techniques.

The credibility of information indicator has 4 attributes and focuses on the categorization of information and how information will be viewed and downloaded. Information will be required to be categorized based on 4 different security tiers, which will be chosen based on the requirements of the healthcare institution. This indicator also reviews how information should be viewed and downloaded.

The credibility of the system indicator comprises of 5 attributes and includes various functions that the system is expected to perform regardless of the operation in progress. These attributes include the timing out of the system, suspension of accounts, hashing of confidential information, flagging of unauthorized users and performing an audit of system events.

Discussion

The study reveals a significant issue of distrust among citizens concerning the security of a patient portal system. This distrust can have a profound impact on the system's adoption, as users may be reluctant to share their sensitive medical information online unless they are assured of its security and confidentiality. To address this concern, it is crucial to focus on enhancing security measures to improve the overall trustworthiness of the system. Interestingly, the study's findings align with those of other research studies, which also emphasize the need for bolstered security protection to instill confidence in users [5, 27, 29, 33].

These consistent findings underline the urgency of implementing robust cybersecurity measures and patient confidentiality laws. By doing so, patients' rights will be better protected, and individuals may be more inclined to share their information online and with healthcare personnel.

The survey results revealed mixed responses regarding granting access to patient records by additional personnel beyond primary healthcare physicians and nurses. Notably, some respondents were hesitant to allow receptionists access to their records, despite the receptionists' vital role in managing administrative tasks and facilitating patient care. This hesitation may indicate a lack of trust between patients and certain healthcare personnel. To build trust, hospital personnel needs to be held accountable in case of data breaches or unauthorized access. Implementing clear protocols and consequences for data breaches will reinforce the system's security and demonstrate the commitment to protecting patient information.

Reviewing and applying international standards and legislation requirements such as ISO and HIPAA are techniques to ensure robust cybersecurity and data protection. These standards give essential guidance and best practices for protecting sensitive data. However, it is important to remember that rules and regulations differ from country to country, and Trinidad and Tobago's legal system will have its own set of laws. As a result, the implementation of cybersecurity and patient confidentiality regulations should be customized to the individual needs and environment of the country. Another barrier to adoption identified in the study is resistance to change, particularly among elderly users. Technology advances rapidly, and some users may be hesitant to adopt new systems that require them to learn new approaches. This resistance might also be influenced by cultural factors and the belief that the current system, despite its shortcomings, is sufficient. To conquer this barrier, it is crucial to develop the patient portal system with a user-friendly interface, ensuring that users of all ages can easily access and utilize the platform. Providing comprehensive user training and ongoing support will also be critical in increasing adoption among older users and others who are unfamiliar with technology.

In conclusion, addressing the issue of distrust, enhancing security measures, as well as taking into account the needs of elderly users are critical elements to enable the effective implementation of a patient portal system in Trinidad and Tobago. The healthcare industry can establish a more accessible and trustworthy digital environment for patients, healthcare providers, and other stakeholders by prioritizing cybersecurity, implementing patient confidentiality legislation, and focusing on user-friendly design.

Views on patient portal implementation vary significantly among nations, with examples from Sweden, the United States, and the United Kingdom providing valuable insights. In Sweden, significant government, patient centric approach and data security have led to a successful patient portal adoption [5, 33]. In the United States, substantial growth in patient portal usage due to government initiatives and an increased demand for patient-centered care, despite challenges related to data security and user friendliness [7, 11, 24]. In the United Kingdom, the National Health Service (NHS) has played a key role in promoting patient portals, and government support has facilitated widespread adoption [34, 35].

In comparison to Trinidad and Tobago, both the US and the UK encounter issues with patient portal deployment. Adoption hurdles in Trinidad and Tobago include mistrust of security and concerns about data confidentiality. Similar concerns have been expressed in the United States and the United Kingdom. Furthermore, every sector emphasized data security and patient privacy as key factors for successful adoption. In Sweden, the United States, and the United Kingdom, government intervention has been critical in increasing patient portal adoption. Assistance from the government may also be required in Trinidad and Tobago to stimulate adoption.

While there are a several similarities in terms of challenges and considerations, the success of patient portal adoption in Sweden, the United States, and the United Kingdom illustrates the potential of digital health solutions to improve patient engagement and healthcare delivery. Data security, privacy concerns, and accessibility are universal themes for successful patient portal deployment across the world.

Limitations

The study presented herein is a valuable contribution to understanding the user requirements and credibility attributes for a patient portal in the context of Trinidad and Tobago's healthcare system. However, it is essential to recognize and address the study's inherent limitations to ensure a comprehensive understanding of its findings and implications.

One significant disadvantage of this study is the shortage of reference data regarding Trinidad and Tobago's healthcare system. As a result of the limited pool of recently published literature and data available for examination, the study's content and depth may be limited. Despite the researchers' best attempts to collect relevant information, the study's conclusions may have been biased by the lack of comprehensive data. Furthermore, the online survey approach used in this study can generate biases and restrictions. While online surveys provide advantages such as lower costs and wider reach, they may not adequately capture the thoughts and perspectives of all age groups, especially those with limited access to or experience with internet platforms. As a result, the survey findings may skew toward particular age categories, perhaps overlooking the preferences and demands of older individuals who may have distinct wishes and expectations for a patient portal. Combining online surveys with other data-gathering methods, such as in-person interviews or focus groups, could assist in overcoming this limitation and offer an improved understanding of the population's various perspectives.

Finally, it is critical to acknowledge that studies on healthcare and technology adoption in Latin America, particularly Trinidad and Tobago, may be restricted in comparison to more widely examined regions. As a result, the study's conclusions may not completely represent all of the region's nuances and complexities. Researchers should be careful not to overgeneralize their results and should take into account any cultural and contextual changes that may impact user requirements and credibility attributes particular to the location. Despite these constraints, the research gives valuable insight into the functional user requirements and credibility specifications for a patient portal in Trinidad and Tobago. Researchers can determine the foundation for future studies that dive further into understanding the complexity of the region's healthcare system and its influence on technology adoption by recognizing and resolving these constraints. Incorporating other research approaches and expanding the study's duration can also improve the study's validity and broaden the scope of user preferences in this case.

Conclusion

In conclusion, this study has made substantial progress in identifying the factors that influence the adoption of a patient portal system in the Trinidad and Tobago healthcare sector. Valuable insights have been gathered to inform future advancements in the sector through the identification of functional user requirements, the defining of credibility attributes based on these requirements, and the assessment of adoption barriers. The study emphasizes the importance of security, integrity, availability, and confidentiality in successfully implementing a patient portal system. These requirements serve as the foundation for the selection of credibility attributes, which are critical in ensuring the system's confidence among users. The credibility evaluation method proposed in this study can be used to guide the design and implementation of patient portal systems not only in Trinidad and Tobago but also in other similar situations.

One of the primary conclusions of this study is that the residents of Trinidad and Tobago are skeptical about the security, integrity, and confidentiality of information in a patient portal system. Addressing these concerns is critical for increasing favorable adoption rates, as many people may be hesitant to embrace the technology if they consider it to be missing in these areas. As a result, in the creation of the patient portal system, steps to improve security, maintain data integrity, and ensure confidentiality must be prioritized. The study also identifies two major barriers to adoption: opposition to change and insufficient cybersecurity laws. Overcoming these obstacles is critical for a successful deployment. Change approaches management should be prioritized for patient portal system implementers to simplify the transition and achieve acceptance from both users and stakeholders. Furthermore, advocating for effective cybersecurity laws will establish a strong legal framework to protect patient information and instill trust in the system. Data openness and accountability are emphasized to maintain the patient portal system's long-term success. Holding responsible individuals accountable in the event of a breach demonstrates a commitment to preserving the system's integrity and protecting patient data. Furthermore, there are significant opportunities for further research in the development of patient portal systems for Trinidad and Tobago in the future. Exploring additional constraints, such as infrastructure limits and information digitization, can provide useful insights into adapting the system to the region's specific needs. Continuous research will be critical in optimizing the patient portal system and guaranteeing its relevance and efficiency as the healthcare sector advances.

Finally, this research has established the framework for the advancement of patient portal systems in Trinidad and Tobago and abroad. We can pave the path for accessible, reliable, and user-friendly healthcare technology that improves patient care and experiences by addressing the specified criteria, credibility attributes, and adoption barriers.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s42979-023-02589-0.

Acknowledgements A special acknowledgement to Associate Professor Yu for her guidance and support on this paper. A special thank you to my family for their continued support.

Data availability All relevant data supporting the findings of this study are available upon request. Please see the following link for access to the data https://doi.org/10.1007/s42979-023-02589-0.

Declarations

Conflict of Interest The authors declare that there is no conflict of interest.

Ethical Approval The procedure of the Beijing University of Technology concerning collecting information was followed. Survey templates were reviewed by the supervising body, and participants' oral permission was obtained for the survey.

Informed Consent Informed consent was obtained from all individual participants included in the study.

References

1. Services. Ministry of Health—Trinidad and Tobago. (n.d.). https://health.gov.tt/services
2. Mutshatshi TE, Mothiba TM, Mamogobo PM, Mbombi MO. Record-keeping: challenges experienced by nurses in selected public hospitals. Curationis. 2018. https://doi.org/10.4102/curationis.v41i1.1931.
3. Yang X, Li T, Pei X, Wen L, Wang C. Medical data sharing scheme based on attribute cryptosystem and blockchain technology. IEEE Access. 2020;8:45468–76. https://doi.org/10.1109/access.2020.2976894.
4. Katehakis DG. Electronic medical record implementation challenges for the National Health System in Greece. Int J Reliable Qual E-Healthcare. 2018;7(1):16–30. https://doi.org/10.4018/ijrqeh.2018010102.
5. Moll J, Rexhepi H, Cajander Å, Grünloh C, Huvila I, Hägglund M, Åhlfeldt R. Patients' experiences of accessing their electronic health Records: National Patient Survey in Sweden. J Med Internet Res. 2018. https://doi.org/10.2196/jmir.9492.
6. Kujala S, Hörhammer I, Väyrynen A, Holmroos M, Nättiaho-Rönnholm M, Hägglund M, Johansen MA. Patients' experiences of web-based access to Electronic Health Records in Finland: cross-sectional survey. J Med Internet Res. 2022. https://doi.org/10.2196/37438.
7. Grossman LV, Choi SW, Collins S, Dykes PC. Implementation of acute care patient portals: recommendations on utility and use from six early adopters. Am Med Inf Assoc. 2017;25(4):370–9. https://doi.org/10.1093/jamia/ocx074.
8. Exceline C, Norman J. Existing enabling technologies and solutions to maintain privacy and security in healthcare records. Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions. 2019; 155–182. https://doi.org/10.1049/pbhe020e_ch7
9. Nahm E, Son H, Yoon JM. Older adults use of patient portals: experiences, challenges, and suggestions shared through discussion board forums. Geriatr Nurs. 2020;41(4):387–93. https://doi.org/10.1016/j.gerinurse.2019.12.001.
10. Sakaguchi-Tang DK, Bosold AL, Choi YK, Turner AM. Patient portal use and experience among older adults: systematic review. JMIR Med Inf. 2017. https://doi.org/10.2196/medinform.8092.
11. Otokiti A, Williams KS, Warsame L. Impact of digital divide on the adoption of online patient portals for self-motivated patients. Healthcare Inf Res. 2020;26(3):220–8. https://doi.org/10.4258/hir.2020.26.3.220.
12. Health record—e-estonia. e. (2022, November 23). https://e-estonia.com/solutions/healthcare/e-health-records/
13. Simola S, Hörhammer I, Xu Y, Bärkås A, Fagerlund AJ, Hagström J, Holmroos M, Hägglund M, Johansen MA, Kane B, Kharko A, Scandurra I, Kujala S. Patients' experiences of a national patient portal and its usability: cross-sectional survey study. J Med Internet Res. 2023. https://doi.org/10.2196/45974.
14. Pramanik PK, Pareek G, Nayyar A. Security and privacy in remote healthcare. New York: Telemedicine Technologies. Elsevier; 2019. p. 201–25. https://doi.org/10.1016/b978-0-12-816948-3.00014-3.
15. Yu X, Xiao R. Research on Application's Credibility Test Method and Calculation Method Based on Application Behavior Declaration. Lecture Notes in Electrical Engineering Frontier Computing. (2019). pp. 1–10. https://doi.org/10.1007/978-981-13-3648-5_1
16. Fang K, Zhou Y, Ma P, Yang M. Credibility evaluation of hardware-in-the-loop simulation systems. 2018 Chinese Control And Decision Conference (CCDC). 2018. https://doi.org/10.1109/ccdc.2018.8407782
17. Xu Y, Tang Y (2019) A user behavior credibility calculation method based on behavior co-occurrence. Proceedings of the 2nd International Conference on Big Data Technologies—ICBDT2019. https://doi.org/10.1145/3358528.3358573
18. Yang R, Yu X (2017) Research on Building the Credibility Evaluations Indicator System of Cloud End User's Behavior. 2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS). https://doi.org/10.1109/bigdatasecurity.2017.23
19. Yu X, Feng D. Research on credible demand analysis method based on risk driven mobile application software. Wireless Pers Commun. 2018;103(1):785–96. https://doi.org/10.1007/s11277-018-5477-z.
20. Rodríguez-Pérez G, Robles G, González-Barahona JM. Reproducibility and credibility in empirical software engineering: a case study based on a systematic literature review of the use of the SZZ algorithm. Inf Softw Technol. 2018;99:164–76. https://doi.org/10.1016/j.infsof.2018.03.009.
21. Yu X, Wang J. A preliminary study of automatic generation of credibility test cases based on immune algorithm. Clust Comput. 2018;22(S6):14867–75. https://doi.org/10.1007/s10586-018-2427-1.
22. https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-2:v1:en. (n.d.). Health informatics—Information security management in health using ISO/IEC 27002.
23. ISO/IEC 27002:2013. ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security controls. (2022, February 15). https://www.iso.org/standard/54533.html
24. (OCR), O. for C. R. (2023) Regulatory initiatives. Regulatory Initiatives. https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/index.html
25. Athenahealth. Cloud-Based Healthcare Products and Services. (n.d.). https://www.athenahealth.com/
26. Epic Research. Epic. (n.d.). https://www.epic.com/
27. Keshta I, Odeh A. Security and privacy of electronic health records: concerns and challenges. Egypt Inf J. 2021;22(2):177–83. https://doi.org/10.1016/j.eij.2020.07.003.
28. Hongwei T, Yixiang C, Hengyang W, Rumei D. A survey of software trustworthiness measurements. Int J Perform Eng. 2019;15(9):2364. https://doi.org/10.23940/ijpe.19.09.p9.2364237.
29. Techapanupreed C, Kurutach W. Enhancing transaction security for handling accountability in electronic health records. Security Commun Netw. 2020;2020:1–18. https://doi.org/10.1155/2020/8899409.

30. Population statistics Trinidad and Tobago. Central Statistical Office. (2023). https://cso.gov.tt/subjects/population-and-vital-statistics/population/
31. Trinidad and Tobago | Data—World Bank Data. Trinidad and Tobago. (n.d.). https://data.worldbank.org/country/Trinidad%20and%20Tobago
32. Slovin's formula: What is it and when do I use it? Statistics How To. (n.d.). https://www.statisticshowto.com/probability-and-statistics/how-to-use-slovins-formula/
33. Leysan Nurgalieva ÅC (n.d.). 'I do not share it with others. No, it's for me, it's my care': On sharing of patient accessible electronic health records—Leysan Nurgalieva, Åsa Cajander, Jonas Moll, Rose-Mharie Åhlfeldt, Isto Huvila, Maurizio Marchese, 2020. Retrieved from https://journals.sagepub.com/doi/full/https://doi.org/10.1177/1460458220912559
34. Kuppanda PM, Jenkins J. Evaluation of experiences and attitudes of patients towards patient portal enabled access to their health information or medical records—a qualitative study. (2022) https://doi.org/10.1101/2022.07.23.22277951
35. Tewolde S, Costelloe C, PowelI J, Papoutsi C, Reidy C, Gudgin B, Shenton C, Greaves F. An observational study of uptake and adoption of the NHS app in England. Br J Gen Pract. 2022. https://doi.org/10.1101/2022.03.16.22272200.
36. Kim L. Cybersecurity matters. Nurs Manage. 2018;49(2):16–22. https://doi.org/10.1097/01.numa.0000529921.97762.be.

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