SLJoAS Sri Lankan Journal of Applied Sciences

Research Article

www.sljoas.uwu.ac.lk/index.php/sljoas

Exploring Privacy and Security Concerns in Sri Lankan Telemedicine Systems: A Patient-Centric Self-Assessment

Sugandima Vidanagamachchi [a,*], Sasanka Mallikarachchi [b]

[a] Department of Computer Science, University of Ruhuna, Sri Lanka

[b] IFS R&D International (Pvt) Ltd, Colombo, Sri Lanka

***Corresponding author email address:** smv@dcs.ruh.ac.lk

(Received 8th April 2024; Accepted 29th August 2024)

Abstract

As a consequence of rapid technological advancements, the field of telemedicine has experienced widespread acceptance within the community. While telemedicine initiatives were introduced several decades ago, significant challenges were encountered to gain prominence due to the prevailing availability of traditional healthcare facilities and a lack of mental preparedness for embracing digital health solutions. However, the recent years, particularly amid the COVID-19 pandemic, have witnessed resurgence in telemedicine practices, becoming the most reliable option for medical care. In an era where individuals are intricately intertwined with technology, especially when it comes to sensitive health-related information, it becomes imperative to possess a foundational understanding of security vulnerabilities and strategies for mitigating associated risks. Consequently, it becomes essential to undertake a comprehensive investigation focused on recognizing the privacy and security concerns inherent in Sri Lankan Telemedicine Systems compared to other developed countries and their standards to protect confidential patient health information. In pursuit of this objective, we have meticulously formulated a comprehensive questionnaire encompassing various facets of telemedicine practices considering the Sri Lankan telemedicine context. In order to ensure the credibility and applicability of our findings, our study enlisted real-world users of telemedicine applications from Sri Lankan hospitals as the sample population. Following an exhaustive phase of data collection, we subjected the gathered information to rigorous analysis, culminating in essential insights. These insights serve as a pivotal privacy and security guide and a self-assessment compatible for all users of telemedicine applications, especially Sri Lankan patients, offering them direction to enhance their practices based on the state-of-the-art techniques, thereby fostering a reliable healthcare service that is both secure and dependable.

Keywords: Telemedicine, Security, Privacy, Self-assessment, Sri Lanka

1. Introduction

Telehealth encompasses a broader range of remote healthcare services and technologies compared to telemedicine, which can be seen as a subset of telehealth. Telemedicine specifically pertains to delivering healthcare services and educational resources across distances. The emergence of the various information technologies have facilitated the extensive utilization of telemedicine to provide high-quality healthcare services, especially in situations where physical access to healthcare is challenging. This was particularly evident during the recent COVID-19 pandemic, where telemedicine played a pivotal role in offering healthcare services to individuals who were hesitant to visit medical facilities in person.

Across various countries such as China, the USA, Italy, India, and WHO Eastern Mediterranean (EMR) region, telemedicine experienced widespread adoption during the pandemic [18,5,6,10,3,2,16,14,12]. The Centers for Disease Control and Prevention (CDC) reported a staggering 154% increase in remote telemedicine visits in March 2020 compared to the same period in 2019. Even in lower-middle-income countries like Sri Lanka, the government's proactive investment in essential infrastructure encouraged and motivated citizens to embrace telemedicine. Further, it was available in some private sector health care centres for a long time.

However, despite the numerous benefits, some individuals remain skeptical about engaging in telemedicine-based healthcare due to concerns related to data breaches and unfavorable experiences. Although the government has issued policies regarding digital data handling, these policies often lack specificity in the context of telehealth and telemedicine. This leads to policy gaps and vulnerabilities in Sri Lanka, leaving patients at risk. Therefore, before formulating policies or advancing telemedicine facilities, it is imperative to enhance public awareness and understanding of telemedicine systems.

To achieve this, it is crucial to gauge people's knowledge about digital data privacy and security policies within healthcare systems. Recognizing security and privacy as pivotal factors in telemedicine and telehealth applications [1,4,17], our study aims to meticulously analyze the existing

security and privacy considerations prevalent in other countries. Our main objective is to explore how to scrutinize the present security and privacy concerns specific to Sri Lanka's context, with the intention of devising a comprehensive self-assessment mechanism. This self-assessment would support patients to determine the level of security of a health care application as it is tailored for the Sri Lankan telemedicine systems.

The primary goal of our study is to formulate a set of insightful interview questions. These questions will target seven critical domains within both telemedicine and cybersecurity. Each subtopic will be accompanied by clear, concise explanations to evaluate Sri Lankans' comprehension of privacy and security concerns in telemedicine systems. Given the evident technical divide within Sri Lankan society, we intend to create and validate distinct interview questionnaires for diverse groups, accounting for different demographics and ethnic backgrounds. Further, we expect more reliable and trustworthy telemedicine services in the future by addressing the analyzed security and privacy shortcomings.

2. Literature Review

Ensuring the security and privacy of telemedicine applications stands as a critical imperative to safeguard patients' sensitive information [18, 17, 25]. A pivotal responsibility lies with healthcare providers, who play a pivotal role in preserving patient privacy and establishing a secure communication infrastructure.

In the realm of privacy and security within telehealth systems, an extensive systematic review was undertaken by Watzlaf V.J.M. et al. in 2017 [17]. This study, however, focused exclusively on privacy and security concerns within the United States. The review underscored the need for enhanced support for telehealth providers concerning privacy and security matters [17]. It examined the utilization of various privacy and security standards, encompassing entities like HIPAA, HL7, and ATA guidelines. A systematic review on privacy and security risk factors were conducted by Houser et al [8], recently in 2020 and they have identified three factors : environmental, technology and operational . However, there is no such standard guideline is available in the Sri Lankan context yet.

A seminal contribution by John C. P. et al. (John et al., 2013) identified a range of security threats intrinsic to telemedicine systems. This included potential vulnerabilities such as Denial of Service (DoS) attacks, identity spoofing, data tampering, repudiation issues, information disclosure, and unauthorized privilege elevation - all incorporated within the STRIDE threat model [24]. To the best of our knowledge, there is no threat model or a self-assessment utilized by the telemedicine applications utilized in Sri Lankan context.

Further innovation emerged with the work of Fatemeh et al. [4], who devised an effective security solution catering to user mobility and anonymity within telemedicine systems. Another noteworthy development was the creation of a telemedicine system specifically tailored to address the Covid-19 scenario. This design took into account both the pandemic situation and the security facets of telemedicine systems, grounded in a service-oriented architecture [15].

A privacy and security self-assessment mechanism aligned with the government audit protocol HIPAA was formulated to guide telehealth providers [13]. Iterative refinement of the questionnaire was undertaken based on the feedback from telehealth providers regarding their preliminary draft [13].

Though there are a few reviews on telehealth security within the Sri Lankan context [21] and experiences on implementations (without considerations of privacy and security aspects) [22], no such patient-centric feedback analysis has been conducted (from the perspectives of patients), despite security being a paramount concern in telemedicine.

Consequently, both telehealth providers and patients remain susceptible to varying degrees of security and privacy breaches, posing a tangible risk of unauthorized access to confidential and sensitive information.

3. Methodology

Our methodology unfolds through three distinct phases, each meticulously designed to ensure the comprehensive achievement of our study objectives. Initially, we crafted a set of well-structured interview questions accompanied by pertinent case scenarios. This was followed by the meticulous selection of potential study participants—users of telemedicine applications. There are 100 participants were selected from different regions in Sri Lanka. The intention was to gather their valuable responses to the formulated interview questions, a critical element of our research. Subsequently, the amassed data was subjected to rigorous analysis to derive meaningful insights and conclusions. We thoroughly referred to the HIPAA while preparing the questionnaire was and it has been refined based on the local security and privacy context (in both Sinhala and English languages). Further, this refinement was carried out repeatedly with several technical and non-technical scientists in Faculty of Science, University of Ruhuna, Sri Lanka and separate case studies were developed for the non-technical users.

- Literature Review

The groundwork for our study involved an exhaustive exploration of previous undertakings related to telemedicine practices within the Sri Lankan context. This was complemented by a comprehensive examination of the prevailing security mechanisms associated with these practices. Our review extended to encompass established questionnaires and interview question structures that pertained to security concerns inherent in telemedicine applications. This thorough analysis informed the criteria underpinning our proposed research endeavor.

- Draft Interview Question Formulation

Building upon the insights gleaned from the literature review, we developed preliminary iterations of interview questions aligned with existing telemedicine regulations. These draft questions were synthesized from the collective wisdom of previous questionnaires and interviews discovered during the review process. Subsequent rounds of scrutiny and refinement enabled us to distil the draft questions into a final, polished set that precisely addressed our research objectives.

- Clarity Enhancement

To ensure that the interview questions were easily comprehensible and relevant to the participants, we categorized them according to the predefined evaluation criteria established in the initial phase. These categorizations facilitated a streamlined and understandable framework for participants. Prior to finalizing the interview questions, we sought feedback from potential participants to refine and enhance their clarity further.

A user-friendly web platform was developed to render the interview questions and their accompanying explanations readily accessible to potential participants [20]. This platform allowed for seamless distribution of the interview questions via a provided link and it provides an embedded scoring for the questionnaire. As the study advanced, the same platform was ingeniously repurposed to disseminate the knowledge acquired during the course of the study, thus fostering a continuous cycle of learning and engagement.

- Participant Identification and Recruitment

Given the pivotal role of participant feedback, identifying willing and enthusiastic individuals was paramount. Participants were recruited through various channels including physical encounters, telephone communication, and email correspondence. This step was instrumental in constructing the robust foundation upon which our study rests.

Table 1:
Results of the Questions on Privacy

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Mean
I have read the agreed privacy policies of the telemedicine application	5	30	19	32	14	3.2
I have read the agreed security policies of the telemedicine application	4	30	19	35	12	3.21
My health provider asks me to consult specific outside organizations such as laboratories and clinics	12	47	16	21	4	2.58

- Conducting Interviews and Thorough Evaluation

The refined interview questions were methodically distributed to the participants via our dedicated web platform. Subsequently, the collected responses underwent meticulous statistical analysis, thereby enabling us to conduct a comprehensive evaluation of our study's findings. This phase stood as a critical juncture in extracting meaningful insights from the accumulated data.

Through this carefully orchestrated process, our study endeavors to shed light on crucial aspects of telemedicine application security and privacy, effectively bridging gaps in understanding and contributing to the broader knowledge landscape.

4. Results, Discussion and Evaluation

After receiving 100 responses from potential participants, we analyzed the gathered information on previously identified subtopics. Furthermore, it is also possible to conduct separate study on single response to analyze the acknowledgment level of the corresponding participant and suggest the areas which needs to be more focused.

By looking at the Table 01 and Fig. 1 approximately 70% of the participants have not read the privacy and security policies of the telemedicine provider before getting a service. Also, it is noteworthy that nearly 60% of the participants have experienced that their telemedicine provider asking them to consult outside organizations such as laboratories and clinics. By looking at the above figures there is self-evident risk that majority is not reading the privacy and security policies and the meantime majority is experiencing sharing their data with third parties. In addition to this less than 40% of the population has gone through the well-recognized privacy policies related to health and the internet such as HIPAA-Health Insurance Portability and Accountability Act or GDPR-General Data Protection Rules. This proves very clearly that patients are already vulnerable and don't aware of any mitigation strategies.

By analyzing the responses, we gathered on questions on storage scenario, we concluded that nearly two-thirds of the population is not aware with the capacity of the files that they share among telemedicine application and doesn't even consider the storage capacity limitations of the application as well. Every time we share something via online methods if accidentally, we shared unnecessary files we can't guarantee that we will recover it forever as its not physical and copies can be generated so easily. There's a possibility

Table 2: Results of the questions on Storage – Part I

	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Mean
I know the average size of documents or images which I share via the telemedicine application	6	30	19	40	5	3.08
I consider the size of documents or images before sending them to the doctors or nurses	13	29	18	33	7	2.98
I received notifications from telemedicine application regarding data backup plans	3	39	26	26	6	2.93

of preventing that if we are aware about the size of the files to be sent and what we are sending.

Maintaining back-up is also important as handling sensitive data in all the sectors. Although data baking-up is not in the hands of the users it is required to know about whether it is provided and other must know facts such as how often it is getting back-ups, does it have a limit or is it free etc. But by looking at the results we obtained, less than 50% of the participants were aware of the backing-up plans of the telemedicine application they are using.

In Table 01 and Fig. 01 we noticed that majority is not familiarized with the well-recognized privacy policies related to health and the internet such as HIPAA or GDPR. In such situation nearly one-third of the sample population is neither agree nor disagree to asking their consent before taking their pictures or video recordings.

Based on the Table 02 and Fig. 02 most of the telemedicine application users don't know about the sizes of the application data which keeps in the storage and the transferring. However, most of the users have received notification of back-up process once it is planned. It is good to know about the back-up process as it helps keeping the past records (including sensitive data) of patients and they can be utilized later for further clinical activities. Also, we added a different type of question to capture what their action in case of emergency which will be is in Table 03 and Fig. 03. They show the actions taken by application users whenever they lost their mobile device which has been used for telemedicine appointments with medical professionals. Regretfully majority is not aware of the best methods in data security spectrum. As the consent has to be taken from each and every patient before keeping the sensitive data used via telemedicine communication, the consent was considered in this analysis. Figure 04 and Table 04 show the further details of this of current usage of patients' applications.

The main purpose using encryption is to provide data security for sensitive information. Encryption methods convert our data into a format which can be readable only for authorized parties. Therefore, users of any telemedicine application or any other application which deals with sensitive data should have a basic understating of these mechanisms. Although above mentioned each method has its own advantages and disadvantages, it goo to witness they have heard about at least one mechanism. Through case studies presented in both Sinhala and English, this analysis aims to determine whether participants in the questionnaire had any familiarity with popular encryption standards (Table 05 and Figure 05).

By looking at the Table 06 and Fig 06 it is clearly evident that majority of the sample population is conscious about the authentication strategies. Specially compared to other categories "Agree" choice scores the highest. Hence, we can notice patients are well aware and correctly using authentication and access control methods (i.e. at least the simple authentication using credentials).

Due to the rapid advancement of technology sometimes having any password is not enough as hackers and intruders are also evolving with the latest technology. Hence having an unbreakable password is important. So, we added a question to analyze understanding of password strength. Table 7 and Fig 07 presents that 86% of the sample is able to recognize the strongest password among the given.

Authorization focuses on determining a user or service's level of access. We use authorization to provide users or services permission to access data or conduct a particular action. When it comes to telemedicine, patient's medical records are only accessible for the respective doctors and nurses, and they should not be accessible to other patients or other staff members. Given that it is good to observe that almost 50% of the sample is acknowledged that the application they are using is capable of such functionalities. Also mean value reported as 2.84 stating majority is not with disagreeing (see Table 08 and Figure 08).

Finally, we wanted to observe the acknowledgement level of network security as lack of proper web security measurements always welcome outside attacks and could cause severe damages to a web application. Here for most of the questions we obtained mean value of 2.5- 2.75 which lies between agreeing and being neutral. It can be considered as a positive point and further it states that population is willing to get to know about network security (see Table 09 and Figure 09).

Table 3: Results of the questions on Storage – Part II

Question	Inform police	Inform ISP	Don't know
This is first action I would take when your mobile device (which you used for medicine treatments) get stolen or lost	23	22	52

Table 4: Results of the questions on Consent

Question	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Mean
My telemedicine application asks for consent while recording and takes pictures while handling treatment sessions	4	32	38	*22*	*4*	*2.9*
My telemedicine system allows me to get tested from outsiders (Clinicals/ Laboratories)	*2*	*39*	*30*	*27*	*2*	*2.88*

Fig. 1. Questions on privacy/ security

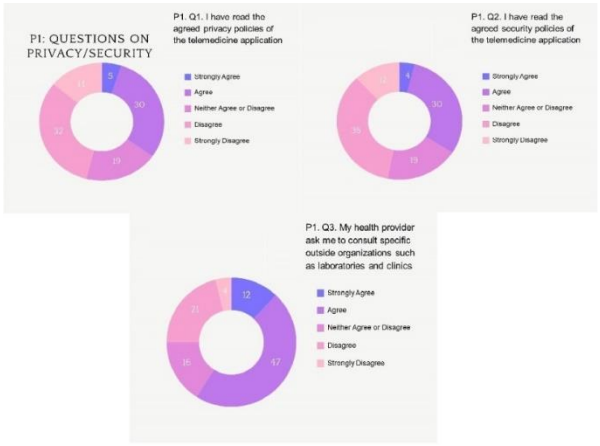

Fig. 2. Questions on storage

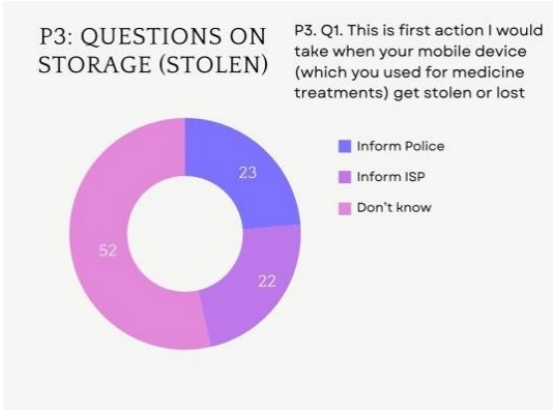

Fig. 3. Questions on storage (stolen) used for telemedicine

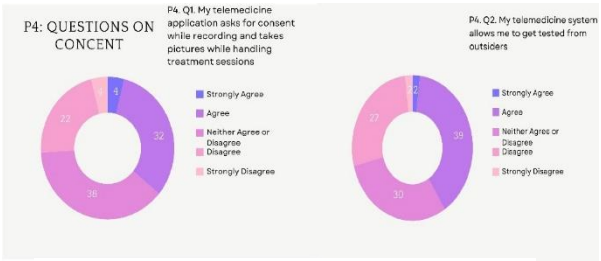

Fig. 4. Questions on consent

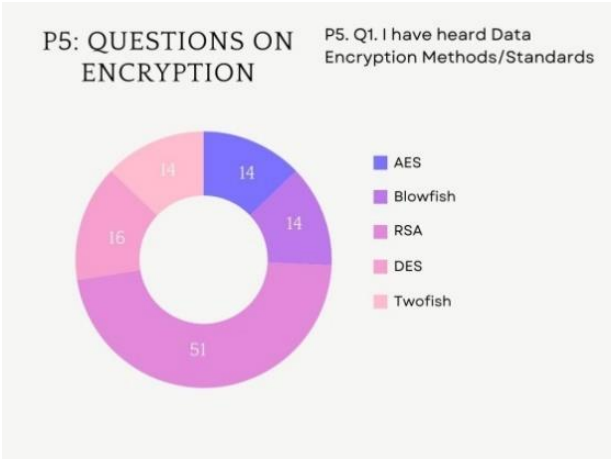

Fig. 5. Questions on encryption

Table 5: Results of the questions on encryption

Question	AES	Blowfish	RSA	DES	Twofish
I have heard following's (Data Encryption standard), AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) security, Blowfish, Twofish	14	14	51	16	14

Table 6
Consent Results of the Questions on Authentication/ Access Control Part I

Question	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Mean
My telehealth system requires Passwords, OTPs, fingerprint scanning before logging into the telehealth session	16	49	14	18	3	2.43
If I don't use the telemedicine application for a while (10-15 minutes), I have to log-in again using user credentials	15	16	44	25	0	2.51

Table 7
Results of the questions on Authentication/ Access control Part II

Questions	hospital*	Hospital	Hospital123	Hospital@123
This is the strongest password among following	6	4	4	86

Table 8
Results of the questions on Authorization

Question	Strongly Agree	Agree	Neither agree or disagree	Disagree	Strongly disagree	Mean
The telemedicine system have certain functionalities which are not accessible for patients but for doctors or nurses. (Disabled buttons, non-editable text fields)	4	43	18	35	0	2.84

Table 9
Results of the questions on Secure Network

Question	Strongly Agree	Agree	Neither Agree or Disagree	Disagree	Strongly Disagree	Mean
My telemedicine system requires passwords or OTPs before opening or sending PHI-Personal Health Information related documents	10	54	12	24	0	2.5
I have installed anti-virus, anti-malware programs on the device which is used to logging into telemedicine system	9	35	26	30	0	2.77
I have used/ visited government blocked or unavailable websites for my region	0	30	24	38	8	3.24
I am aware about data restoring options	5	46	25	18	6	2.74

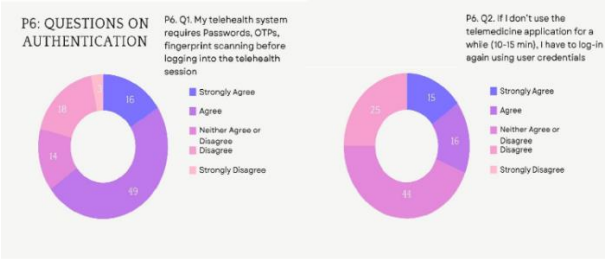

Fig. 6. Questions on authentication

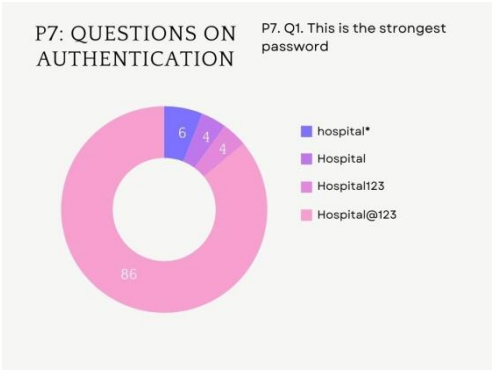

Fig. 7. Questions on authentication- strength of the password

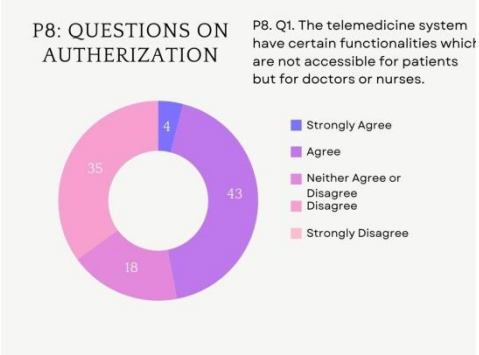

Fig. 8. Questions on authorization

Fig. 9. Questions on secure network

5. Conclusion and Future Work

In summary this self-assessment questionnaire can be considered as a very balanced and versatile questionnaire as it is covered broad scope in privacy and security concerns of Telemedicine systems in Sri Lanka. Also, it could be considered as a reliable questionnaire as the participants have actively engaged and by looking at the answers it reflects questions were simple and specific. Generally sample was acknowledged the risk mitigation and preventing step related to privacy and security, access control while they don't consider about storage and network security spectrum. Hoping this study illustrates the current privacy and security concerns of Telemedicine systems in Sri Lanka. Further, this study can be utilized to guide all the telemedicine application users to improve their practices for a more secure and reliable healthcare service in the future. Moreover, the establishment and dissemination of a comprehensive framework of standards for telemedicine professionals and users in Sri Lanka is imperative, given that only a preliminary draft of regulations was identified at the time of this article's submission. This initiative necessitates the involvement of both security specialists from the academia, industry and healthcare practitioners.

Conflicts of Interest

No conflict of interest to be declared.

Acknowledgments

We express our gratitude to the University of Ruhuna, Faculty of Science, Sri Lanka for the grant awarded under reference number RU/SF/RP/2022/06.

Ethical Clearance

Secured ethical approval for the project from the Faculty of Science's Ethical Review Committee at the University of Ruhuna in Matara, Sri Lanka.

References

[1] Almathami H.K.Y., Win K.T., Vlahu-Gjorgievska E. 2020 Barriers and Facilitators That Influence Telemedicine-Based, Real-Time, Online Consultation at Patients; Homes: Systematic Literature Review. J Med Internet Res. 22 2

[2] Bhaskar S., Bradley S., Chattu V. K., et al. 2020 Telemedicine Across the Globe-Position Paper From the COVID-19 Pandemic Health System Resilience PROGRAM (REPROGRAM) International Consortium (Part 1). Frontiers in Public Health.

[3] Byrne M.D. 2020 Telehealth and the COVID-19 Pandemic. J Perianesth Nurs. 35 5

[4] Fatemeh R., Yi M. 2018 Practical and secure telemedicine systems for user mobility. Journal of Biomedical Informatics. 78

[5] Galle A., Semaan A., Huysmans E., et al. 2021. A double-edged sword—telemedicine for maternal care during COVID-19: findings from a global mixed-methods study of healthcare providers. BMJ Global Health.

[6] Gillman-Wells C.C., Sankar T.K., Vadodaria S. 2021 COVID-19 Reducing the Risks: Telemedicine is the New Norm for Surgical Consultations and Communications. Aesthetic Plast Surg. 45 1

[7] Hale T. M., and KvedarJ. C. 2014 Privacy and Security Concerns in Telehealth. AMA Journal of Ethics, Virtual Mentor. 16 12

[8] Houser S.H., Flite C.A., Foster S.L. 2023 Privacy and Security Risk Factors Related to Telehealth Services - A Systematic Review. Perspect Health Inf Manag. 20 1

[9] John C.P., Karen H., Ranganathan C., Venkatakrishnan V.N. 2013 A Threat Table Based Appr able Based Approach to Telemedicine Security. Transactions of the Intrnational Conference on Health Information Technology Advancement. 2 1

[10] Monaghesh, E., Hajizadeh, A. 2020 The role of telehealth during COVID-19 outbreak: a systematic review based on current evidence. BMC Public Health. 20.

[11] Removing regulatory barriers to telehealth before and after COVID-19. Available: https://www.brookings.edu/articles/removing-regulatory-barriers-to-telehealth-before-and-after-covid-19/ (Accessed on 30th August 2023)

[12] Parkes P., Pillay T.D., Bdaiwi Y. et al. 2022 Telemedicine interventions in six conflict-affected countries in the WHO Eastern Mediterranean region: a systematic review. Confl Health. 16.

[13] Pendergrass J. C., Heart K, Ranganathan C., and Venkatakrishnan, V.N. 2023 A Threat Table Based Approach to Telemedicine Security. Transactions of the International Conference on Health Information Technology Advancement 38.

[14] Omboni S. 2020 Telemedicine During the COVID-19 in Italy: A Missed Opportunity? Telemed J E Health. 26 8.

[15] Shaikh A., Reshan M.S., Sulaiman A., Alshahrani H., Asiri A. 2022 Secure Telemedicine System Design for COVID-19 Patients Treatment Using Service Oriented Architecture. Sensors. 22.

[16] Tatti P., Galiero R., Pafundi P. C. et al. 2020 The Importance of Telemedicine during COVID-19 Pandemic: A Focus on Diabetic Retinopathy. Journal of Diabetes Research.

[17] Watzlaf V.J.M., Zhou L., Dealmeida D.R. 2017 Hartman LM. A Systematic Review of Research Studies Examining Telehealth Privacy and Security Practices used by Healthcare Providers. Int J Telerehabil. 9 2.

[18] Weiquan W., Li S., Tao L. & Tian L. 2022 The use of E-health during the COVID-19 pandemic: a case study in China's Hubei province. Health Sociology Review. 31 3

[19] Zhou L., Thieret R., Watzlaf V., Dealmeida D., Parmanto B. 2019 A Telehealth Privacy and Security Self-Assessment Questionnaire for Telehealth Providers: Development and Validation. Int J Telerehabil. 11 1

[20] Siriwardhana V. T. N. S., Mallikarachchi P. S., Vidanagamachchi S. M. 2023 Embedded scoring methodology for the self - Assessment of the privacy and security concerns in telemedicine systems in Sri Lanka, Proceedings of the International Conference on Applied and Pure Sciences 3 120

[21] Ranwala, R. A. D. L. M. K. 2019 Review of literature for health information security on Sri Lankan health, Sri Lanka Journal of Bio-Medical Informatics

[22] Kumarasinghe, M., Karunarathne, W.,Karunapema, P., Irfaan, S. 2022 Opportunity for Innovation: Experiences in Implementing Telehealth Services to Enhance Access to Healthcare during COVID-19 Pandemic in Sri Lanka: A Case Study. Asian Journal of Advanced Research and Reports. 16.

[24] Kohnfelder, L., Garg, P. 1999 The threats to our products. Microsoft Interface. Retrieved 20 December 2022.

[25] Timothy M. H., and Joseph C. K. 2014 Privacy and Security Concerns in Telehealth, American Medical Association Journal of Ethics, 16 12