




Attitudes of Covid-19 patients toward sharing their health data: A survey-based study to understand security and privacy concerns

Khadijeh Moulaei¹  | Elnaz Iranmanesh² | Parasto Amiri¹  | Leila Ahmadian³ 

¹Student Research Committee, Kerman University of Medical Sciences, Kerman, Iran

²Department of Information Technology Engineering, Faculty of Sciences, Islamic Azad University, Kerman, Iran

³Department of Health Information Sciences, Faculty of Management and Medical Information Sciences, Kerman University of Medical Sciences, Kerman, Iran

Correspondence

Leila Ahmadian, Department of Health Information Sciences, Faculty of Management and Medical Information Sciences, Kerman University of Medical Sciences, Haft-bagh Hwy, PO Box 7616911313, Kerman, Iran.
Email: l.ahmadian@kmu.ac.ir and ahmadianle@yahoo.com

Abstract

Background and Aims: Many people around the world, especially at the time of the Covid-19 outbreak, are concerned about their e-health data. The aim of this study was to investigate the attitudes of patients with Covid-19 toward sharing their health data for research and their concerns about security and privacy.

Methods: This survey is a cross-sectional study conducted through an electronic researcher-made questionnaire from February to May 2021. Convenience sampling was applied to select the participants and all 475 patients were referred to two to Afzalipour and Shahid Bahonar hospitals were invited to the study. According to the inclusion and exclusion criteria, 204 patients were included in the study and completed the questionnaire. Descriptive statistics (frequency, mean, and standard deviation) were used to analyze the questionnaire data. SPSS 23.0 was used for data analysis.

Results: Participants tended to share information about “comments provided by individuals on websites” (68.6%), “fitness tracker data” (64.19%), and “online shopping history” (63.21%) before death. Participants also tended to share information about “electronic medical records data” (36.75%), “genetic data” (24.99%), and “Instagram data” (24.99%) after death. “Fraud or misuse of personal information” (4.48 [±1.27]) was the most common concern of participants regarding the virtual world. “Unauthorized access to the account” (4.38 [±0.73]), “violation of the privacy of personal information” (4.26 [±0.85]), and “violation of the patient privacy and personal information confidentially” (4.26 [±0.85]) were the most of the unauthorized security incidents that occurred online for participants.

Conclusion: Patients with Covid-19 were concerned about releasing information they shared on websites and social networks. Therefore, people should be made aware of the reliability of websites and social media so that their security and privacy are not affected.

Khadijeh Moulaei and Elnaz Iranmanesh contributed equally to this work as first authors.

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.

© 2023 The Authors. *Health Science Reports* published by Wiley Periodicals LLC.

KEYWORDS

attitude, COVID-19, data sharing, privacy, security, survey

1 | INTRODUCTION

So far, a huge amount of health data has been collected and shared digitally, which has recently increased greatly with the outbreak of the Covid-19 pandemic. As the biggest challenge of the last century, this disease has disrupted public health in the world.^{1,2} Moreover, Covid-19 has threatened lives, destabilized businesses, damaged daily life, induced stress and anxiety in people, and stunned the global economy.^{3,4} To deal with this pandemic, the use of face-to-face healthcare services has been reduced.³ For this reason, the use of social media (such as WhatsApp, Telegram, and Instagram) as a platform of updated information related to Covid-19 increased significantly.⁵ The spread of information about this disease through social media was shared faster than the disease around the world.⁶ The World Health Organization (WHO) and the United Nations called this unprecedented release of information “infodemic.”⁷ Governments, for reasons such as social media's use of personal data for financial value, have become increasingly concerned about protecting the privacy and security of people's information.⁸ Meanwhile, the shift from in-person visits to telemedicine that occurred during the Covid-19 pandemic has increased cybersecurity and protection of individual and organizational information resource concerns.⁹ Gerke et al.,¹⁰ pointed out that in the healthcare sector, the vulnerability to cyber-attacks has greatly increased, and these incidents can lead to suboptimal care or harm to individuals and breach of their privacy and security.

By looking beyond data collection and usage, during the Covid-19 pandemic, much personal data are shared without individual consent. To inform others who may be at risk, the South Korean government publicly disclosed private information about victims of the disease, including demographic information, employment, location, and social contacts.¹¹ In Singapore, the government also disclosed places related to patients, such as accommodation, workplace, and other places they had visited.¹² Using data from patients with Covid-19 may lead to online abuse, invasion of privacy, social stigma, and even an increased risk to their physical safety.^{13,14} On the other hand, access to information and information sharing helps researchers to seek solutions to control patients, gain accurate knowledge about patients and sometimes inform the public and prevent gossip.¹⁵ To this end, several studies have examined the privacy and security of personal data during the outbreak of Covid-19.^{16–18} Iran was also one of the most affected countries in the world at the time of the outbreak of Covid-19.⁷ People share a lot of information on social media without knowing that their information may reflect their health information. On the other hand, their willingness to share their information for various purposes, especially research, is unclear. So, the aim of this study is identifying the individual's opinions and concerns about the misuse of shared health data, privacy and data security in the use of data for the management of the Covid-19 crisis.

To our knowledge, this is the first study to identify data security and privacy concerns for patients with COVID-19. Also, in this study, we identify the types of data that can be shared and received feedbacks on sharing health data with health researchers. However, other studies have focused on identifying interventions to ensure safety and review best practices and regulatory requirements for privacy and security during the outbreak of Covid-19,¹⁰ providing a blockchain-based security and privacy protection plan for COVID-19 medical records,¹⁹ determining privacy of COVID-19 contact tracing apps,^{12,20} and identifying top 10 cybersecurity threats that had and could take place during the pandemic.³

2 | MATERIALS AND METHODS

The present cross-sectional study was conducted using an electronic researcher-made questionnaire. This questionnaire was designed by reviewing related studies^{1–3,5,7,8,12–14,20–27} and sample questionnaires related to security and privacy.^{15–18} Also, the opinions of two medical informatics specialists and two software engineers with at least 5 years of experience in the information technology department of medical centers were used to design a questionnaire. Then, the questionnaire was created in 8 sections and 67 questions: Demographic information (4 questions), different sources of knowledge and information about health (9 questions), types of data shared with researchers before and after death (26 questions), received feedbacks on sharing health data with health researchers (5 questions), sharing data with researchers and health organizations (6 questions), tendency to share information and knowledge extracted from personal health data analysis with individuals or organizations (7 questions), concerns about the virtual world (5 questions), and unauthorized security incidents occurring online (5 questions). Four questions in the “demographic information” section were defined as open-ended (for age and education level) and two scales (for detection of Covid-19 infection method and treatment method). The score of each question was different based on the answers to each question. In other hand, Questions were defined as multi options, and participants could select more than one answer. For example, in the “Different sources of knowledge and information about health” section, we have listed all the sources of knowledge and information about health in response to this question. Therefore, the patient could choose more than one source to answer this question.

To evaluate face validity, both qualitative and quantitative methods were applied. In this section, questions were asked about the “relevance,” “ambiguity,” and “difficulty” of the items. Then, based on the answers given, changes were made in the initial questionnaire. For quantitative section, the face validity of the questionnaire was confirmed by two medical informatics specialists and two software

engineers. For the quantitative section, the same four individuals were asked to evaluate the questionnaire and rate the importance of each item on a 5-point Likert scale to calculate the "item impact score" (impact score = frequency [%] × importance). An impact score of 1.5 or higher was considered satisfactory.²⁸ A minimum score of 1.5 was obtained for all questionnaire questions.

Content validity ratio (CVR) was used to determine the content validity of the questionnaire. To calculate CVR, the questionnaire was given to three infectious diseases specialists and three medical informatics experts. These people had the experience of research work in the field of security and privacy of patients. To determine CVR, we asked the panel of experts to answer each question based on a three-point scale (necessary, useful but not necessary, and not necessary).^{29,30} Then CVR was calculated using the following formula:

$$\text{CVR} = \frac{n_e - N/2}{N/2}$$

Where, n is the number of experts who selected the "necessary" option and N is the total number of experts.

According to Lawshe's decision table for CVR, if the number of expert panel members is six, the minimum acceptable value for each case will be 0.99.³⁰ In this research, the minimum acceptable value of CVR for each question (according to experts) was 1.00. In addition, the total CVR ratio was also calculated at 0.99. The reliability of the questionnaire was calculated after completing the questionnaire by 50 patients with Covid-19. The reliability of the questionnaire based on Cronbach's alpha and Kuder–Richardson formulas for four-option and two-option questions was 0.831% and 0.85%, respectively. After confirming the validity and reliability, the questionnaire was designed electronically with Google Form tool.

The study population included patients with Covid-19 in Kerman city. To include patients in the study, we used the following inclusion criteria and exclusion criteria. The inclusion criteria were: At least 18 years old, at least a diploma, infection with Covid-19 (with any level of disease), and a resident of Kerman city. Moreover, refuse to accept informed consent and having severe dementia, severe blindness, deafness, or cognitive impairment defined as the exclusion criteria.

During the study period (from February to May 2021), a total of 475 patients with Covid-19 were referred to two to Afzalipour and Shahid Bahonar hospitals affiliated to Kerman University of Medical Sciences (KUMS). At the time of the present study, these two hospitals were the only hospitals that provided medical services to patients with Covid-19 in Kerman. Moreover, these governmental hospitals are educational therapy centers that patients with various diseases can refer to. After submitting the approval obtained from the ethical committee of KUMS to these two hospitals, the phone numbers of all 475 patients were given to the researchers. Their phone numbers were extracted from the patients' medical records. Then, sampling was conducted by convenience method based on inclusion criteria and all 475 patients were invited to the study. It should be noted that convenience sampling is a type of nonrandom or non-probability sampling in which members of the target population

who meet certain practical criteria such as easy accessibility, availability at a given time, geographic proximity, or willingness to participate are included for the aim of the study.³¹ It is also referred to the researching subjects of the population that are easily available to the researcher and all these subjects can be included in the study.³¹

To invite patients, an invitation was sent through social networks (WhatsApp or Telegram), as well as Email. We used the fotojet website (<https://www.fotojet.com/features/photo-card/invitation.html>) to design the invitation. A total of 305 patients accepted our invitation. Finally, according to the inclusion and exclusion criteria, 204 patients were included in the study.

Before sending the questionnaire link to the participants, to estimate the exact time of completing each questionnaire, eight patients completed the questionnaire and recorded the approximate time. The approximate time was estimated between 15 and 20 min. Then, the questionnaire link was sent to patients through social networks (WhatsApp and Telegram) as well as Email from May 1 to 30, 2021. By June 21, 2021, all patients had completed the questionnaires. Along with the link, a help file in PDF format about the questionnaire's content and how to complete it was sent to the participants. It should be noted that since we had defined all the questions in the questionnaire as "required" (patients must answer each question to finally submit the questionnaire to the researchers), all 204 participants answered all the questions.

Frequency and percentage were used to analyze patients' demographics. Also, descriptive statistics (percentage, mean, standard deviation) were used to analyze other parts of the questionnaire. Analyzes were performed using SPSS 23.0.

2.1 | Ethical considerations

Ethics approval (IR.KMU.REC.1401.459) was obtained from the Ethics Committee of Kerman University of Medical Sciences. Before participating in the study, the study's objectives were explained to the participants, and informed consent was obtained from them. Patients' participation in the study was voluntary, and they could be excluded from the study at any stage of the study.

3 | RESULTS

A total of 204 patients was recruited for this study, and all 204 patients completed the questionnaires. Table 1 shows the demographic information of the patients participating in the study. Most participants were aged 38–47 (36.3%) and had a diploma (34.3%). About half of the participants' disease (58.8%) were diagnosed with laboratory tests, and most were treated through home quarantine (82.8%).

According to the participants (56.3%), health websites, Instagram (53.9%), and WhatsApp (49%) are the most used different sources for

gaining knowledge and information about health, respectively. Also, Snapchat (2.4%), Email accounts (4.9%), and Twitter (23.5%) were the least used sources for gaining knowledge and information about health (Figure 1).

The third part of the questionnaire was related to sharing of 22 different types of data with researchers before and after death by participants. To share data before death, participants were willing to share data with researchers on "comments provided by individuals on websites" (68.6%), "fitness tracker data" (64.19%), and "online shopping history" (63.21%). Also, among these 22 types of data, patients were less likely to share "electronic medical records data" (3.92%), "bank card billing information"

(2.45%), "tax and income history" (2.45%), and "genetic data" (0.98%) with researchers.

Moreover, for postmortem data sharing (Table 2), "electronic medical records data" (36.75%), "genetic data" (24.99%), and "Instagram data" (24.99%) were the most postmortem data donated by participants, respectively. Data related to "medication records" (7.84%), "Geographic data (GPS from phone or computer)" (7.35%), and "online shopping history" (5.88%) were the least important data that could be donated postmortem by the participants.

Also, out of 204 participants, 86 (42.4%) stated that they would donate "all health data" to health organizations and institutions after death. Sixty-two participants (30.38%) stated that they would donate "only some health data" to health organizations. Also, 36 participants (17.46%) stated that they would not donate their health data after death, and 20 participants (9.8%) stated that they were "not unsure," respectively.

The most common feedbacks that participants wanted to receive when sharing their electronic data with health researchers were "identify potential risk factors for personal health" (4.70 [2.36]), "comparing people's data with each other to compare their health status and diseases with other patients" (4.53 [1.68]), and "information about the impact of individual habits on people's health," respectively (3.93 [0.96]) (Table 3).

Among the 204 participants, 87 participants (42.6%) believed that others could use their data for various purposes. Also, 36 participants (17.6%) were likely to benefit from their data for various purposes. A total of 81 participants (39.7%) stated that others would not benefit from their data. Ninety-nine participants (48.5%) were concerned about giving their electronic information to researchers in the future. One hundred and five participants (51.5%) said they were not worried about giving their electronic information to researchers in the future and would share their information with researchers.

TABLE 1 Demographic information of the participants.

Variable		n (%)
Age	18–27	28 (13.7)
	28–37	62 (30.4)
	38–47	74 (36.3)
	48–57	26 (12.7)
	≥58	14 (6.89)
Education level	Diploma	70 (34.3)
	Associate	20 (9.8)
	Bachelor	61 (29.9)
	Master	47 (23.0)
	PhD	6 (2.99)
Detect Covid-19 infection	By symptom	84 (41.16)
	By laboratory tests	120 (58.8)
Treatment method	Home quarantine	169 (82.8)
	Hospitalization	35 (17.15)

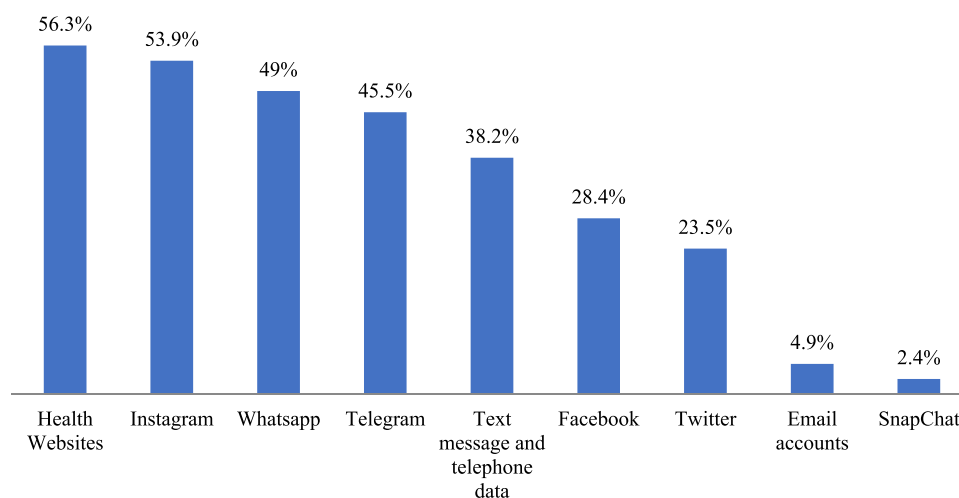


FIGURE 1 Different sources of knowledge and information about health. Participants could select more than one resource.

TABLE 2 Types of data shared with researchers before and after death.

Types of data that can be shared with researchers and their methods of sharing	Before death n (%)	Postmortem data n (%)
Comments provided by individuals on websites	140 (68.6)	24 (11.76)
Fitness tracker data (Fitness, Apple Watch, etc.)	131 (64.19)	20 (9.8)
Online shopping history	129 (63.21)	12 (5.88)
Website ranking information	120 (58.8)	17 (8.33)
Search history	118 (57.82)	33 (16.17)
Music playback data	115 (56.35)	15 (7.35)
Internet taxi history	110 (53.9)	18 (8.82)
WhatsApp data	101 (49.49)	35 (17.15)
Telegram data	100 (49)	34 (16.66)
Facebook data	78 (38.22)	18 (8.82)
Instagram data	75 (36.75)	70 (24.99)
Email History (Gmail, Yahoo, etc.)	69 (33.81)	17 (8.33)
Snapchat data	63 (30.87)	17 (8.33)
Twitter data	55 (26.95)	17 (8.33)
Geographic data (GPS from phone or computer)	53 (25.97)	15 (7.35)
Medication records	50 (24.5)	16 (7.84)
History of voting or campaigning	25 (12.25)	18 (8.82)
Text message and telephone data (telephone calls and SMS)	20 (9.8)	23 (11.27)
Electronic medical records data	8 (3.92)	75 (36.75)
Bank card billing information	5 (2.45)	24 (11.76)
Tax and income history	5 (2.45)	19 (9.31)
Genetic data	2 (0.98)	51 (24.99)

Note: Participants could select more than one data type.

TABLE 3 Received feedbacks on sharing health data with health researchers.

Received feedbacks	Mean (standard deviation)
Identify potential risk factors for personal health	4.70 (2.36)
Comparing people's data with each other to compare their health status and diseases with other patients	4.53 (1.68)
Information about the impact of individual habits on people's health	3.93 (0.96)
Analysis of health data to find out the status of individual health	3.50 (1.12)
Information on improving eating and exercise habits	3.41 (0.49)

Note: Participants could choose from more than one feedback.

According to Table 4, 190 participants (93.1) were willing to send themselves the information and knowledge extracted from the analysis of personal health data. Also, 185 participants (90.6%) and 170 participants (83.3%) wanted this information and knowledge to be provided to “physician or healthcare provider,” and “family,” respectively.

The most common concerns of participants regarding the virtual world were “fraud or misuse of personal information” (4.48 [1.27]), “unauthorized disclosure of online information shared with friends” (4.42 [1.38]), and “disclosure of personal information by companies or online websites without the consent of individuals” (4.30 [1.35]), respectively (Table 5).

Most of the unauthorized security incidents that occurred online for participants were related to “unauthorized access to the account” (4.38 [0.73]), “violation of the patient privacy and information confidentially” (4.26 [0.85]), and “victim of fraud and identity theft” (4.20 [0.71]) (Table 6).

TABLE 4 Tendency to share information and knowledge extracted from personal health data analysis with individuals or organizations.

Sharing information and knowledge extracted from health data analysis	n (%)
Myself	190 (93.1)
Physician or healthcare provider	185 (90.6)
Family	170 (83.3)
People with a patient-like health condition	160 (78.4)
Health organizations	152 (74.4)
Other researchers	48 (23.52)
All people who want to get information	10 (4.9)

Note: Participants could choose more than one answer.

TABLE 5 Concerns about the virtual world.

Concerns about the virtual world	Mean (standard deviation)
Fraud or misuse of personal information	4.48 (1.27)
Unauthorized disclosure of online information shared with friends	4.42 (1.38)
People you only know through the internet are not what they say	4.30 (1.35)
Disclosure of personal information by companies or online websites without the consent of individuals	3.32 (1.25)
Companies and online websites misuse individuals' information to achieve their own goals without providing privacy policies and laws	3.30 (1.26)

Note: Participants could choose more than one answer.

TABLE 6 Unauthorized security incidents occurring online.

Unauthorized security incidents occurring online	Mean (standard deviation)
Unauthorized access to the account	4.38 (0.73)
Violation of the patient privacy and information confidentially	4.26 (0.85)
Victim of fraud and identity theft	4.20 (0.71)
Gaining an unpleasant experience by providing information online to people	3.80 (0.73)
Negatively affecting people's reputation	3.40 (0.77)

Note: Participants could choose more than one answer.

4 | DISCUSSION

This study examined the attitudes of patients with Covid-19 toward sharing their digital health data and their concerns about the security and privacy of this data. The results of this study showed that most of the participants emphasized that only their families and doctors had access to their health data. Most participants wanted to share all or part of their digital health data after death. Participants were less inclined to share electronic health records, especially before death, due to concerns. Participants stated that the purpose of sharing health data with researchers was to “identify potential risk factors for personal health” and to “comparing people's data with each other to compare their health status and diseases with other patients.” Participants were more concerned about scams by Internet users and unauthorized disclosure of their information. Most of the security incidents that people faced included unauthorized access to their accounts, privacy breaches, and identity theft. However, the results of this study showed that people continue to use websites and social media to gain knowledge and information about their health and exchange information through these media.

According to the results of this and other studies, security threats are not specific to one technology or one social media, and any health technology may be subject to cyber-attacks inside or outside the organization. In the 2015 survey by Healthcare Information and Management Systems Society, two-thirds (68%) of surveyed healthcare organizations in the United States reported having recently experienced a significant security incident. Reported security incidents came both from external threats (63.6% of healthcare organizations) and insider threats (53.7%).³² These statistics of IT-related security breaches in the healthcare sector are alarming, and the reality may be even bleaker when one views that many security incidents remain undiscovered or are not properly evaluated, as well as the tendency of organizations to underreport security incidents. Studies show that security breaches in healthcare settings can be expensive. Absolute Software Corporation reported cases of healthcare data breaches that cost hospitals \$250,000 to \$2.5 million in settlement payments.³² Security and privacy concerns may prevent patients and healthcare providers from using information technology to perform medical processes. Enhancing HIT security and privacy

practices is an important step forward for delivering and receiving effective healthcare services.

In our study, participants were willing to share different types of digital data with researchers, both before and after death. In the study by Seltzer et al.,³³ study patients were significantly more like to share their personal digital data with researchers. "Vivli" is an example of a data-sharing initiative for clinical research data during a Covid-19 pandemic. "Vivli" will link existing data-sharing platforms and communities, while hosting the data from investigators who aspire to share data but don't have the resources to do so.³⁴ In addition, many articles today have dealt with the effective relationship of digital data on improving health outcomes and the use of healthcare.²⁴⁻²⁷ Collecting and analyzing digital health data as it has been useful for monitoring various diseases in the past,^{12,15,16} now it will also be effective for monitoring, prevention and control of Covid-19 disease.

According to the findings of the present study, it was stated that almost half of the participants use health websites, Instagram, and WhatsApp to obtain health-related knowledge and information. According to a systematic review of social media-based surveillance systems for healthcare, Twitter is the most widely used social media platform for sharing information related to disease surveillance and individual disease outbreaks.³⁵ Chen et al.,³⁶ showed that almost half of the individuals use health websites, Instagram, and WhatsApp to acquire health-related knowledge and information. Moreover, another study³⁷ also showed that most individuals obtained the news of COVID-19 through social media platforms such as WhatsApp, Telegram, Instagram, radio, and television. With the increasing use of social media, people share their personal information, even highly personal information. For this reason, some are concerned that social media is a tool for government surveillance, but people need to be convinced that the data available on social media may be used by governments for actions such as influencing policies to control the Covid-19 pandemic.^{38,39} On the other hand, although very inaccurate, wildly inaccurate, harmful, dangerous, and fake information may be present on websites and social media, it is still used by most people on a regular basis.⁴⁰ To remove wrong information about Covid-19, the WHO formed a team to cooperate with social media such as Twitter, YouTube, and Facebook.⁴¹ For this purpose, researchers and healthcare providers can also do their part to combat misinformation by using reliable and engaging methods to disseminate accurate information. In addition to these, social media can provide a communication platform for stakeholders during a disease outbreak. Government social media accounts may embellish as official information sources that provide timely outbreak content to local agencies and journalists.^{42,43}

According to the other findings of our study, the online collection of user information leads to many new era problems such as misinformation, fake news, identity fraud, hacking, and general information security.⁴⁴ This is why many people around the world, for fear of compromising their privacy, oppose sharing their private data, but today many people refuse to oppose this issue to curb the Covid-19.⁴⁵ Numerous studies have reported positive changes in people's use of social media, especially in patients with Covid-19, during Covid-19.⁴⁶⁻⁴⁸ The majority of participants (93.1%) in the present study also stated that the information and knowledge extracted from the analysis of personal health data should be

made available to the "physician or healthcare provider" and the "family." Huang et al.,⁴⁹ mentioned that users create and share information through social media around the world. Sharing information on social media can prevent the further spread of the Covid-19 epidemic in social environments and promote and educate healthcare. Other studies^{35,37,42} have also shown that social media has several advantages over other media when used to disseminate health information. Social media are the fastest available channels for sharing warnings and updates about disease outbreaks.⁴² Moreover, social media allows using different forms of media to engage the public. For example, by incorporating links, social media posts can direct the public to different online resources for more health information.³⁶ Health institutions and organizations can also share podcast audio files and YouTube videos on various social media platforms to provide health information.⁵⁰

Today, a large number of health professionals and organizations are constantly involved in social networks.⁵¹ On the other hand, the cost-effectiveness of using social media has made it easier to share news or information.⁵² Therefore, the possibility of disseminating health data through these media is increasing day by day. Zhou et al.,⁵³ showed that the widespread adoption of new technologies such as telemedicine systems, social networks, and mHealth applications make security and privacy issues in healthcare more challenging and urgent, since patients can easily share the confidential health information, they receive from healthcare providers without knowing the security risks. In this study, participants were most concerned about "scams by Internet users or the misuse of their personal information," "unauthorized disclosure of information shared online with friends by these people," and "people you only know through the Internet, they are not what they say they were." Armitage et al.,⁵⁴ reported that unauthorized access and dissemination of data, especially in the field of health, bring chaos to the community. SO, managers of social networks can gain the trust of users by improving the features of the platforms such as security and privacy policies, ease of use, and improving the quality of information. Gerke et al.,¹⁰ suggested that during a public health emergency, healthcare providers, and technology companies should make sure to comply with HIPAA and protect the individual's privacy as much as possible.

According to the results of this study and other studies,⁵⁵ the role of social media as an opportunity to share information has created a positive image in the view of their users. So that people use them to search for information, discuss and exchange personal experiences, and interact with other users about their problems.⁵⁶ The occurrence of unauthorized security incidents in them doesn't only frighten people, but can also tarnish their good image⁵⁷ and undermine their use.^{39,58} After a security flaw that led to the accidental release of Facebook users' personal information in 2010, the possibility of unauthorized security incidents became clear to the public.^{59,60} Among the most unauthorized security incidents that happened to the participants of the present study were "unauthorized access to the account," "violation of the patient privacy and information confidentially," and "victim of fraud and identity theft." Although there is a lot of talk about privacy, there is no clear answer. These concerns may lead individuals to use social media less.⁶¹ Of course, individual's concern

about their privacy online depends a lot on their level of trust in the platform they are using.⁶²

In this study, the participants preferred to share online shopping history, bank card billing, music playback data, and tax and income history data before or after their death. It seems that due to the decrease in life expectancy during the spread of COVID-19 worldwide, this disease can affect the interactions and daily activities of patients such as shopping, paying bank bills, income and paying taxes of COVID-19 patients. Schöley et al.⁴¹ showed that COVID-19 has caused an unprecedented increase in mortality and reduced life expectancy worldwide. Also, the decrease in life expectancy has affected various aspects of patients' lives. Other study,⁶³ also showed that the outbreak of Covid-19 has changed the way of life. For example, shopping patterns have changed from traditional to online, because the fear of contracting this disease has always existed in people. However, people are concerned about personal data privacy and security in their online shopping transactions. Khan et al.³ also pointed out that hackers, attackers and fraudsters usually take advantage of emergency situations, especially when people are scared, desperate, and vulnerable. Therefore, it should be said that during the outbreak of a disease, not only the dimensions related to maintaining the physical and mental health of patients should be considered, but also the concerns related to the security and privacy of patients' data. The concerns and stress of patients about how to maintain the security and privacy of data can effect on the physical, mental, emotional, and spiritual health of the patients.⁶⁴

Many of the most popular social media and websites are emerging and have started operating in the last decade. Collect and store digital health data that is not typical, collected in electronic health records and sometimes it may not be shared with service providers such as walking, calorie counting, and so forth can play an important role in people's health and lead to better health services for people in the future. During the Covid-19 pandemic, given the growing trend of the relationship between digital activities and people's health, it is necessary to increase people's trust in social media. This requires technical, operational and political commitments from governments at all levels. For this reason, governments around the world are revising their data usage laws. Recently, the United States' National Institute of Health Data Sharing Policy and the European Union's General Data Protection Regulation have been established to protect the privacy and security of digital health data in the world.^{65,66} Also, health policymakers should understand people's concerns regarding the privacy and security of their health data in social media to determine what challenges make it difficult to take necessary measures to manage and control information related to Covid-19.

5 | STRENGTHS AND LIMITATIONS OF THE STUDY

To our knowledge, no study has been conducted to identify the security and privacy concerns of patients with Covid-19. Therefore, our study is the first to identify these concerns and challenges. This study identified different sources of knowledge and information

about health, types of data that can be shared with researchers before and after death, and received feedbacks on sharing health data with health researchers. Another strength of our study was determining with whom participants were willing to share their health data. Moreover, in our study, concerns about the virtual world and unauthorized security incidents occurring online were identified.

Our study has limitations that need to be considered. The first limitation of our survey was related to the location (Kerman province). For this reason, the results of this study cannot be generalized to the Iranian people. To do this, more extensive research needs to be done at the national level. The second limitation was that due to the spread of the Covid-19, the researchers distributed the questionnaire among patients online and through social networks. Therefore, patients who were not members of social networks or individuals who had low digital literacy were not included in the study. Also, because the participants are probably more aware of technology than the general population, there is a risk of response bias in the results. Therefore, in other studies, these data collection biases should be considered. Despite the limitations mentioned, the data were collected through a self-report that individual reports are used due to biases such as the ability to internalize constraints. To reduce the effect of this, the instructions for completing the questionnaire were provided to the patients to correctly understand the questions of the questionnaire. We recommend that future researchers conduct this study at the national level because examining the patients' attitudes with Covid-19 toward sharing their digital health data across the country will yield very interesting results that can help policymakers.

Also, the study used the convenience sampling method, in which the sample may not be representative of all Covid-19 patients in Iran. Future studies should consider randomized samples with regions other than the Kerman city, where the study had been conducted.

6 | CONCLUSION

The analysis of the present study showed that although people with Covid-19 in Kerman province use websites and social media to share their health data, they are also concerned about the privacy and security of their health data. Therefore, managers of social networks, officials of universities, institutions, and health organizations to effectively deal with this epidemic must increase people's awareness of the behavior and reliability of websites and social media. It should also enable people to have a better understanding of websites and social media and encourage them to use these programs properly so that their security and privacy are not compromised. The results of the present research can be considered as the starting point for the implementation of the policies and national strategies for control and prevention of Covid-19 by technology.

AUTHOR CONTRIBUTIONS

Khadijeh Moulaei: Conceptualization; data curation; formal analysis; investigation; methodology; project administration; resources; software; supervision; validation; visualization; writing—original draft;

writing—review & editing. **Elnaz Iranmanesh**: Conceptualization; data curation. **Parasto Amiri**: Methodology; writing—original draft; writing—review & editing. **Leila Ahmadian**: Conceptualization; writing—original draft.

ACKNOWLEDGMENTS

The authors would like to thank all patients who participated in this study. This study was supported by Kerman University of Medical Sciences (Grant: 401000847). The funder had no roles in study design, data gathering, and analysis.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ETHICS STATEMENT

All methods of the present study were performed following the relevant guidelines and regulations of the ethical committee of Kerman University of Medical Sciences. Participation was voluntary, the consent was verbal, but all participants responded via email or text message to approve their participation. Participants had the right to withdraw from the study at any time without prejudice.

TRANSPARENCY STATEMENT

The lead author Leila Ahmadian affirms that this manuscript is an honest, accurate, and transparent account of the study being reported; that no important aspects of the study have been omitted; and that any discrepancies from the study as planned (and, if relevant, registered) have been explained.

ORCID

Khadijeh Moulaei  <http://orcid.org/0000-0002-5730-3972>

Parasto Amiri  <https://orcid.org/0000-0002-5654-1987>

Leila Ahmadian  <http://orcid.org/0000-0002-6487-2209>

REFERENCES

- Hussein MR, Shams AB, Apu EH, Mamun KAA, Rahman MSJ. Digital surveillance systems for tracing COVID-19: privacy and security challenges with recommendations. 2020.
- Jalali MS, Landman A, Gordon WJ. Telemedicine, privacy, and information security in the age of COVID-19. *J Am Med Informatics Assoc: JAMIA*. 2021;28(3):671-672.
- Khan NA, Brohi SN, Zaman N. Ten deadly cyber security threats amid COVID-19 pandemic. 2020.
- Kazemi-Arpanahi H, Moulaei K, Shanbehzadeh M. Design and development of a web-based registry for coronavirus (COVID-19) disease. *Med J Islam Repub Iran*. 2020;34:68.
- Mahncke RJ, Williams PA. Secure transmission of shared electronic health records: a review. 2006.
- Sowmiya B, Abhijith V, Sudersan S, Sakthi Jaya Sundar R, Thangavel M, Varalakshmi PJS. A survey on security and privacy issues in contact tracing application of COVID-19. *SN Computer Sci*. 2021;2:1-11.
- Sun R, Wang W, Xue M, Tyson G, Camtepe S, Ranasinghe DJ. Vetting security and privacy of global covid-19 contact tracing applications. *arXiv preprint arXiv*. 2020;10933(2020):1-14.
- Trestian R, Xie G, Lohar P, et al. Privacy, privacy in a time of covid-19: How concerned are you? *IEEE Security Privacy*. 2021;19(5):26-35.
- Alammary A, Alshaikh M, Pratama AR. Awareness of security and privacy settings in video conferencing apps among faculty during the COVID-19 pandemic. *PeerJ. Computer Sci*. 2022;8:e1021.
- Gerke S, Shachar C, Chai PR, Cohen IG. Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. *Nature Med*. 2020;26(8):1176-1182.
- Undale S, Kulkarni A, Patil H. Perceived eWallet security: impact of COVID-19 pandemic. 2021;18(1):89-104.
- Wen H, Zhao Q, Lin Z, Xuan D, Shroff N. A study of the privacy of covid-19 contact tracing apps, security and privacy in communication networks: 16th EAI International Conference, SecureComm, Washington, DC, USA, October 21-23, 2020, Proceedings, Part I 16 Springer: 2020; pp. 297-317.
- Williams P, Mahncke R. A new breed of risk: electronic medical records security. 2005.
- Yang W-Y, Tsai C-H. Democratic values, collective security, and privacy: Taiwan people's response to COVID-19. 2020;8(3):222-245.
- Zhou L, Thieret R, Watzlaf V, DeAlmeida D, Parmanto B. A telehealth privacy and security self-assessment questionnaire for telehealth providers: development and validation. *Int J Telerehabil*. 2019;11(1):3-14.
- Oh S-R, Seo Y-D, Lee E, Kim YG. A comprehensive survey on security and privacy for electronic health data. *Int J Environ Res Public Health*. 2021;18(18):9668.
- Papoutsis C, Reed JE, Marston C, et al. Patient and public views about the security and privacy of electronic health records (EHRs) in the UK: results from a mixed methods study. *BMC Med Inform Decis Mak*. 2015;15:1-15.
- Hartigan L, Cussen L, Meaney S, O'donoghue K. Patients' perception of privacy and confidentiality in the emergency department of a busy obstetric unit. *BMC Health Serv Res*. 2018;18:978.
- Tan L, Yu K, Shi N, Yang C, Wei W, Lu H. Towards secure and privacy-preserving data sharing for COVID-19 medical records: a blockchain-empowered approach. *IEEE Transactions Net Sci Eng*. 2022;9(1):271-281.
- Borra S. COVID-19 apps: privacy and security concerns. *Intelligent Systems and Methods to Combat Covid-19*. Springer; 2020:11-17.
- Arifeen MM, Al Mamun A, Kaiser MS, Mahmud M. Blockchain-enable contact tracing for preserving user privacy during COVID-19 outbreak. 2020.
- Azad MA, Arshad J, Akmal SMA, et al. A first look at privacy analysis of COVID-19 contact tracing mobile applications. 2020.
- Emami-Naeini P, Francisco T, Kohno T, Roesner F. In understanding privacy attitudes and concerns towards remote communications during the {COVID-19} pandemic, seventeenth symposium on usable privacy and security (SOUPS), 2021; pp 695-714.
- Ferrag MA, Shu L, Choo K-KR. Fighting COVID-19 and future pandemics with the internet of things: security and privacy perspectives. *IEEE/CAA J Automatica Sinica*. 2021;8(9):1477-1499.
- Golec M, Ozturac R, Pooranian Z, Gill SS, Buyya R. iFaaSBus: a security and privacy based lightweight framework for serverless computing using IoT and machine learning. 2021.
- Sowmiya B, Abhijith V, Sudersan S, Sundar RSJ, Thangavel M, Varalakshmi PJS. A survey on security and privacy issues in contact tracing application of Covid-19. 2021;2(3):1-11.
- Undale S, Kulkarni A, Patil HP. Perceived eWallet security: impact of COVID-19 pandemic. 2020.
- Naderimaghani S, Niknami S, Abolhassani F, Hajizadeh E, Montazeri A. Development and psychometric properties of a new

- social support scale for self-care in middle-aged patients with type II diabetes (S4-MAD). *BMC Public Health*. 2012;12(1):1035.
29. Ayre C, Scally AJ. Critical values for Lawshe's content validity ratio: revisiting the original methods of calculation. *Measurement Evaluation Counseling Develop*. 2014;47(1):79-86.
 30. Wilson FR, Pan W, Schumsky DA. Recalculation of the critical values for Lawshe's content validity ratio. *Measurement Evaluation Counseling Development*. 2012;45(3):197-210.
 31. Etikan I, Musa SA, Alkassim RS. Comparison of convenience sampling and purposive sampling. *Am J Theoretical Appl Statistics*. 2016;5(1):1-4.
 32. Uwizeyemungu S, Poba-Nzaou P, Cantinotti M. European hospitals' transition toward fully electronic-based systems: do information technology security and privacy practices follow? *JMIR Med Inform*. 2019;7(1):e11211.
 33. Klar R, Lanzerath DJR. The ethics of COVID-19 tracking apps—challenges and voluntariness. 2020;16(3-4):1-9.
 34. Bierer BE, Li R, Barnes M, Sim I. A global, neutral platform for sharing trial data. *N Engl J Med*. 2016;374(25):2411-2413.
 35. Gupta A, Katarya R. Social media based surveillance systems for healthcare using machine learning: a systematic review. *J Biomed Inf*. 2020;108:103500.
 36. Chen J, Wang Y. Social media use for health purposes: systematic review. *J Med Internet Res*. 2021;23(5):e17917.
 37. Amiri P, Moulaei K, Bahaadinbeigy K, Ghaemi MM, Sheikhtaheri A. The information-seeking behavior of medical sciences students toward COVID-19 in mass and social media: a cross-sectional study. *Health Sci Rep*. 2022;5(3):648.
 38. Verma A, Singh MK, Pareek A. Technology, information, misinformation, and disinformation about COVID-19: a content study of closed-cross platform messaging using Whatsapp. 2020;29(10):7797-7804.
 39. Ayani S, Moulaei K, Khaneshari SD, Jahanbakhsh M, Sadeghi FJAMI. A systematic review of big data potential to make synergies between sciences for achieving sustainable health: challenges and solutions 2019;41(2):53-64.
 40. Ayani S, Sadoughi F, Jabari R, Moulaei K, Ashrafi-Rizi H. Evaluation criteria for health websites: critical review. 2020;9(1):44.
 41. Schöley J, Aburto JM, Kashnitsky I, et al. Life expectancy changes since COVID-19. *Nature Human Behav*. 2022;6(12):1649-1659.
 42. Jin Y, Austin L, Vijaykumar S, Jun H, Nowak GJPRR. Communicating about infectious disease threats: insights from public health information officers 2019;45(1):167-177.
 43. McInnes C, Hornmoen HJO. 'Add Twitter and Stir': the use of Twitter by public authorities in Norway and UK during the 2014-15 Ebola outbreak 2018;12(2):23-46.
 44. Edosomwan S, Prakasan SK, Kouame D, Watson J, Seymour T. The history of social media and its impact on business. *J Appl Management Entrepreneurship*. 2011;16(3):79.
 45. Jung G, Lee H, Kim A, Lee U. Too much information: assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea. *Front Public Health*. 2020;8:305.
 46. Chen P, Mao L, Nassis GP, Harmer P, Ainsworth BE, Li F. Coronavirus disease (COVID-19): the need to maintain regular physical activity while taking precautions. *J Sport Health Sci*. 2020; 9(2):103-104.
 47. Mirzaei A, Kazembeigi F, Kakaei H, Jalilian M, Mazloomi S, Nourmoradi H. Application of health belief model to predict COVID-19-preventive behaviors among a sample of Iranian adult population. *J Educ Health Promot*. 2021;10(69):1-7.
 48. Grix J, Brannagan PM, Grimes H, Neville R. The impact of Covid-19 on sport. *Int J Sport Policy Politics*. 2021;13(1):1-12.
 49. Huang X, Wang S, Zhang M, et al. Social media mining under the COVID-19 context: progress, challenges, and opportunities. *International J App Earth Observation Geoinformation: ITC J*. 2022;113(2):1-13.
 50. Harrison D, Wilding J, Bowman A, et al. Using YouTube to disseminate effective vaccination pain treatment for babies. *PLoS One*. 2016;11(10):e0164123.
 51. Wong A, Capel I, Malbrain M. Social media in critical care: fad or a new standard in medical education? An analysis of international critical care conferences between 2014 and 2017. *J Intensive Care Soc*. 2019;20(4):341-346.
 52. Tandoc Jr EC, Jenkins J, Craft S. Fake news as a critical incident in journalism. *Journalism Practice*. 2019;13(6):673-689.
 53. Zhou L, Parmanto B, Joshi J. Development and evaluation of a new security and privacy track in a health informatics graduate program: multidisciplinary collaboration in education. *JMIR Med Educ*. 2018;4(2):e19.
 54. Armitage L, Lawson BK, Whelan ME, Newhouse N. Paying SPECIAL consideration to the digital sharing of information during the COVID-19 pandemic and beyond. *BJGP open*. 2020;4(2).
 55. Thompson N, Wang X, Daya P. Determinants of news sharing behavior on social media. *J Computer Information Sys*. 2019;5(2021): 1-10.
 56. Papa V, Maniou TA. Recurrent narratives around the COVID-19 crisis in social networks: a case study analysis on Facebook. *Tripodos*. 2021;2(47):11-28.
 57. Talwar S, Dhir A, Kaur P, Zafar N, Alrasheedy M. Why do people share fake news? Associations between the dark side of social media use and fake news sharing behavior. *J Retailing Consumer Services*. 2019;51:72-82.
 58. Verma A, Singh M, Pareek A. Information, misinformation, and disinformation about Covid-19: a content study of closed-cross platform messaging using whatsapp. *Inter J Adv Sci Technol*. 2020;29: 7797-7804.
 59. Coppersmith G, Leary R, Crutchley P, Fine A. Natural language processing of social media as screening for suicide risk. *Biomed Inform Insights*. 2018;10:1178222618792860.
 60. Guntuku SC, Yaden DB, Kern ML, Ungar LH, Eichstaedt JC. Detecting depression and mental illness on social media: an integrative review. *Current Opin Behav Sci*. 2017;18:43-49.
 61. Horvitz E, Mulligan D. Data, privacy, and the greater good. *Science*. 2015;349(6245):253-255.
 62. Rowlands I, Nicholas D, Williams P, et al. *In The Google Generation: the Information Behaviour of the Researcher of the Future*, Aslib Proceedings. Emerald Group Publishing Limited; 2008:290-310.
 63. Chatterjee S, Chaudhuri R, Vrontis DJ. Examining the global retail apocalypse during the COVID-19 pandemic using strategic omnichannel management: a consumers' data privacy and data security perspective 2021;29(7):617-632.
 64. Woogara J. Human rights and patients' privacy in UK hospitals. *Nurs Ethics*. 2001;8(3):234-246.
 65. Deb A, Donohue S, Glaisyer T. Is social media a threat to democracy? 2017.
 66. Acerbi AJPC. Cognitive attraction and online misinformation. 2019; 5(1):1-7.

How to cite this article: Moulaei K, Iranmanesh E, Amiri P, Ahmadian L. Attitudes of Covid-19 patients toward sharing their health data: a survey-based study to understand security and privacy concerns. *Health Sci Rep*. 2023;6:e1132. doi:10.1002/hsr2.1132