The Effect of Security Information Sharing and Disruptive Technology on Patient Dissatisfaction in Saudi Health Care Services During Covid-19 Pandemic

Hasan Beyari[1*], Mohammed Hejazi[2], and Othman Alrusaini[3]
[1] Department of Administrative and Financial Sciences, Applied College, Umm Al-Qura University, Makkah, Saudi Arabia
[e-mail: hmbeyari@uqu.edu.sa]
[2] Department of Supply Chain Management, Collage of Business Administration, University of Business and Technology, Jeddah, Saudi Arabia
[e-mail: m.hejazi@ubt.edu.sa]
[3] Department of Engineering and Applied Sciences, Applied College, Umm Al-Qura University Makkah, Saudi Arabia
[e-mail: oarusaini@uqu.edu.sa]
*Corresponding author: Hasan Beyari

Received December 29, 2021; revised June 15, 2022; accepted July 8, 2022; published October 31, 2022

Abstract

This study is an investigation into the factors affecting patient dissatisfaction among Saudi hospitals. The selected factors considered for analysis are security of information sharing, operational practices, disruptive technologies, and the ease of use of EHR patient information management systems. From the literature review section, it was clear that hardly any other studies have embraced these concepts in one as was intended by this study. The theories that the study heavily draws from are the service dominant logic and the feature integration theory. The study surveyed 350 respondents from three large major hospitals in three different metropolitan cities in the Kingdom of Saudi Arabia. This sample came from members of the three hospitals that were willing to participate in the study. The number 350 represents those that successfully completed the online questionnaire or the limited physical questionnaires in time. The study employed the structural equation modelling technique to analyze the associations. Findings suggested that security of information sharing had a significant direct effect on patient satisfaction. Operational practice positively mediated the effect of security of information sharing on patient dissatisfaction. However, ease of use failed to significant impact this association. The study concluded that to improve patient satisfaction, Saudi hospitals must work on their systems to reinforce them against the active threats on the privacy of patients' data by leveraging disruptive technology. They should also improve their operational practices by embracing quality management techniques relevant to the healthcare sector.

Keywords: Security Information Sharing, Disruptive Technology, Operational Practice, Ease of Use, Patient Dissatisfaction, Health Care.

1. Introduction

The world is becoming more sensitive to privacy issues, especially now that information is a commercial product. The previous practices regarding information sharing have now come under heavy scrutiny by suspicious bystanders [1]. While hospitals may be naively sharing with other parties, the other parties could take advantage of this information by harvesting and selling it [2]. Another potential casualty is this information featuring in third-party studies for which the participating patients have not given their express consent to the researchers to use their data [3]. During the COVID-19 pandemic in Saudi Arabia, the world of healthcare shared data with third-parties including other hospitals and the government. This practice was considered normal and acceptable to the public. However, it is possible that some patients may have had reservations on the same.

Some researchers argue that because they do not reveal the identity of the participants, their consent may be irrelevant. However, research ethics dictate that studies using the primary data from participants should seek their express authority [4]. It is extremely difficult to follow the information sharing trail to where entities buy this data or use it in research. Nevertheless, it all begins at the point where patients share it with their healthcare service providers. The use of digital systems in capturing and transmitting this information has made it even more difficult to tell whether or not it is susceptible to malicious use in the software [5]. In the wake of this revelation, patients become more uncomfortable sharing some of their personal information fearing that it will end up in the hands of an unauthorized third party. This study investigates the associations among disruptive technology, security of information sharing, and patient dissatisfaction.

2. Literature Review

Information sharing in healthcare refers to the process through which facilities share data about their patients with other facilities. This information is mostly given in its crude form with its identification labels such as name and residence details. The need for sharing this information is not in doubt. However,[6] cast aspersions regarding whether the receiving parties actually use this information to enhance the quality of care of the patient in question. These doubts are what constitutes the need for securing patient information even during its transmission to other parties. Patients prefer to have their illness and treatment information kept confidential [7]. However, physicians have the legal authority to share it with other parties such as ambulance services and other hospitals when a patient is being transferred. The risk of misuse of this transmitted data is even more pronounced when it is digital [8]. The rise of artificial intelligence makes it possible to analyze big data, thereby exposing personal patient information to unauthorized analysts.

The effect of data security on patient satisfaction is a broadly examined scholarly area of research. According to [9] patient satisfaction is a product of many variables, among which privacy is one. The source claims that whenever a patient feels that their information is not safe, they are not likely to be more forthcoming with it. Healthcare organizations that give the explicit assurance that patient data is safe in their hands tend to attract more patients to their facilities, especially for chronic illnesses such as HIV and Cancer [10]. Some people would rather go through these illnesses without being subjected to public scorn. The only use of their

personal data that patients would understand is if it offers some potential improvement in their treatment.

Additionally, the security of information sharing often results in patients being free with their physicians and nurses. [11] finds that the fact that some patients may have had bad experiences in the past is already enough to have them not share sensitive information with their caregivers. Hence, the source underscores the need to ensure that patients trust the system for them to be open about their personal information. In [12], the researchers concluded that openness of patients is a prerequisite to proper diagnosis and treatment. However, data privacy is a concern for many who may wish to share their personal information with physicians[8]. When a patient reports back to a hospital, it is good practice to ask them about their information rather than chest-thumping that the facility has it already. It makes some patients feel uncomfortable.

Ensuring that information is shared securely is good practice because it conforms expectations of all stakeholders. Operationally, patient data is quite sensitive. Hence, healthcare organizations go to all lengths to ensure that it is protected. [6] argue that it is the operational responsibility of the IT or EHR department to guarantee the safety and privacy of all patient data. While sharing, it is considered best practice to conform to data privacy laws and technologies[8]. The success or failure of hacking and other malicious attempts at patient data inform the operational performance scores of the EHR department. These performance metrics are used to determine whether the system needs a security boost or that it is secure.

The security of information while sharing is what has prompted several healthcare organizations to consider operational changes. When management feels that its data transmission and sharing processes are not at par with current standards, it is an indication that its operations are at risk [13]. Hence, it would be time to consider more robust and secure data management technologies. Most of these organizations feel safe with blockchain, and it is because the technology has proven to be highly secure even to the most vicious attacks[14]. It has now become an operational practice for firms to engage in this technology. Hospitals follow closely the developments in this field because they appreciate the boost that it has given to their operations.

A system’s ease of use refers to the simplicity in design and functionality of healthcare electronic record systems (EHR). There are many ways with which a facility can enhance the ease of use of its digital systems. One such possibility is by tapping into Application Programming Interfaces (APIs), which provide requested data on a need basis [15]. Another possible mitigation is by using third-party software to accomplish tasks. These methods expose hospital data to third parties even when management is unaware of these happenings in the background. Trade-offs between ease of use and security are what prompt major hospitals to invest in their own technological systems [16]. Nevertheless, at some point, healthcare facilities have to rely on public data from repositories. It is at this point that the facilities expose themselves to phishing and hacking. Those that insist on not tapping into publicly available data have to do it the hard way, which is usually inconvenient.

Operational practice is the degree to which an organization achieves its operational goals by adhering to the Total Quality Management expectations. The TQM model requires that a firm must attempt continuous quality improvements organization-wide [17]. One of the ways in which healthcare facilities achieve this objective is by upgrading the security of their data

and that of their patients. One way of securing data is by enabling the two-factor authentication algorithm for all system users [18]. In this case, a username and a password are not enough to log in. Some use verification codes sent to a user's email address, while in other cases, the system sends this code to the user's phone. These security measures are effective in ensuring that only authorized personnel can log in. However, these mechanisms are somehow inconvenient, especially if the logging in is a requirement each time the system wakes up from idle time [19]. Hence, there is a trade-off between security of information sharing and operational practice.

The application of best operational practices such as Kaizen and six sigma mediate the relationship between security of information sharing and patient satisfaction. Six sigma has the potential to shorten wait times, reduce medication errors, increase turnaround time for lab results, and prevent falls [20]. According to [21], the 'Define, Measure, Analyze, Improve, and Control' (DMAIC) facilitates patient satisfaction through the use of technological systems. The source finds that fragmented processes and a dismal communication system can leverage DMAIC to improve patient satisfaction in a hospital setting. Similarly, [22] find a linkage between patient information security, six sigma, and patient satisfaction. The researchers report that a more comprehensive approach hospital culture on data security can have an impact on quality management, which then impacts patient satisfaction levels.

Using the Kaizen framework, hospitals are leverage improve upon the functionality of information systems, which ultimately impacts patient satisfaction. [23] claims that the evolution of the Kaizen concept in healthcare has positively impacted several aspects within it. One such way in which the concept has been helpful is by facilitating the use of information management systems in hospitals, especially the HER [20]. This notion is also reflected in [11], where the investigation finds that optimizing the workplace using Kaizen concepts helps to ensure that EHR systems positively impact patients by giving them better experiences while at the hospital. The relationships between security of information sharing may not be too apparent in these studies. However, their conclusions seem to allude to the existence of such a relationship.

Disruptive technology is technology that substantially impacts the current operational landscape. Its ability to change the landscape stems from the fact that such technology has superior attributes relative to those engrained in the incumbent systems [24]. Because of these features, its adoption is fast, and its acceptability is also wide. In the current dispensation, artificial intelligence technologies are on the rise, especially in the healthcare sector. As [25] find, nowadays, physicians no longer need to be all-knowing because they have AI at their disposal. For example, by feeding the system with a patient's symptoms, the AI algorithm can predict the diagnosis from the most likely to the least likely disease. Artificial intelligence is also engrained into other technologies such as cancer computerized tomography (CT) scan [26]. Disruptive technologies are inherently unpredictable. There is no telling which next technology will sweep the healthcare industry.

Disruptive technologies have been largely responsible for the overhaul of systems in the healthcare sector. Artificial intelligence is one such technology that has made it considerably easier to work with previously installed systems. According to [27], artificial intelligence is beneficial because it takes the pressure off a physician. Most of the pressures stem from the fact that wrong diagnoses lead to wrong treatment plans, which may be fatal at worst. However, relying on artificial intelligence has made it possible to confirm their personally made

diagnosis with what the AI predicts [28]. Coupled with big data, artificial intelligence is rising in its adoption in the healthcare sector because they simplify the previously tedious tasks that required high levels of intelligence.

The topic on disruptive technology and security of information is dominated by scholarly resources advocating for the adoption of blockchain technology. According to [29], this technology is secure because it uses a public ledger to confirm and verify transactions. Conventional systems work from a centralized point from where all authentication and verification occur. Blockchain's architecture is by default decentralized. Using self-executing programmable protocol, it is possible to develop a blockchain model that effectively protect patient data, allow patients to have full control over their data, and ensuring data provenance [30]. These data protection mechanisms are what make healthcare organizations move towards blockchain technologies.

Similarly, [31] draw significant relationships between blockchain technology as a form of disruptive technology on the security of patient information. The source particularly lauds the ability of the blockchain technology to share and storing of medical records discretely. This notion is also echoed in [32], where the researchers attest to the fact that blockchain technology is the future of the healthcare sector because of the sensitivity of data storage and sharing. Again, its decentralized principles seem to be the feature that resonates well with stakeholders in this sector [33]. The fact that the technology has been adopted widely in the healthcare sector indicates that it will be long before another technology trounces its footprint. However, the possibility of other technologies being built upon it is quite high because of its ease of integration with other technologies.

Patient dissatisfaction is the degree to which a patient forms a negative opinion of a health facility or its services because of their personal experiences with the said facility. Factors contributing this opinion are many, one of which is regarding how they observe or feel or think that the facility is using their private information [34]. According to them, it is a violation of the doctor-patient confidentiality if their private information finds its way to the public or even in the hands of a third-party physician. For this reason, facilities try to shield their patients from the background processing and transmittal of their information. Hospitals registering the best patient satisfaction metrics in terms of security of information are those that create a wall between patient data collection and how the data is utilized [35]. Other factors that influence patient satisfaction are the quality of healthcare, duration of stay at the hospital, interactions with hospital staffs, and their previous opinion about the facility or treatment plan.

3. Theoretical Background

3.1 Service Dominant Logic

This theory belongs to a category of dominant logic theories. Such theories explain the means through which firms realize their profits. In this case, the service-dominant logic explains the creation of value by an organization through intangible exchanges among actors [36]. The underlying assumption is that people use their competencies to benefit others and they still benefit from others' competencies. The theory is being applied across industries and geographical locations, which affirms its workability [37]. The S-D Logic views these exchanges as service for service exchanges [38]. In the business environment, the theory

asserts that while the quality of a product deserves attention, even more important is the experience to which the business subjects its customers [39]. By focusing more on the delivery of a service or good to the customer, a business is said to be adopting the service-dominant logic.

The theory is applicable in explaining the value-adding exchanges in the healthcare sector. The experiences that a patient goes through the hospital is of greater influence on their perception of quality than the actual medical procedures [40]. The theory seemingly explains the association between security of information sharing and patient dissatisfaction. Patients visit hospitals for treatment. However, they expect more from the hospital than just the treatment they seek. One of these expectations is privacy. If a healthcare facility cannot guarantee the security of a patient's information, they are unlikely to be satisfied with the treatment [3]. Additionally, having patients wait in line for hours before attending to them reduces the perceived quality of service and their satisfaction levels. In this case, the theory links operational practice to patient satisfaction. Hence, the exchanges occurring between patients and a hospital are more than just the treatment.

3.2 Integration Theory

The integration theory, otherwise known as the feature integration theory, is a theoretical model in psychology. It explains how people form opinion about phenomena by observing and internalizing the various features of the phenomena [41]. The underlying principle is that people do not perceive an object first; rather, they perceive its features such as movement, shape, and color. These features contribute highly to how they ultimately form an opinion on the object [42]. The theory contends that perception occurs after the completion of two stages. The first stage is the pre-attention stage, which is automatic, and it involves an individual focusing on one distinguishing factor [43]. The second stage involves an individual's active attention to form an opinion.

In healthcare, this model is applicable in that, patients do not form an opinion of a hospital as a unit. Instead, the features of the hospital such as the buildings, hospitality of staff members, proficiency of physicians, waiting time, and the location of the facility [44]. After internalizing these features, a patient may form a positive or negative opinion depending on which features are important to them. The model seems to explain the relevance of operational practices and how they mediate security of information sharing to result in patient satisfaction or dissatisfaction. In this case, if the patient finds short waiting lines, empathy from personnel, effective treatment, and a good physical environment, they tend to perceive the facility positively [45]. This perception ultimately leads to their satisfaction.

3.3 Conceptual Framework and Research Hypothesis

Based on the objectives, the conceptual framework of the study has multiple dependent variables and multiple independent variables. However, the ultimate dependent variable is patient satisfaction. **Fig. 1** diagrammatically illustrates the potential associations between the variables and groups of variables.

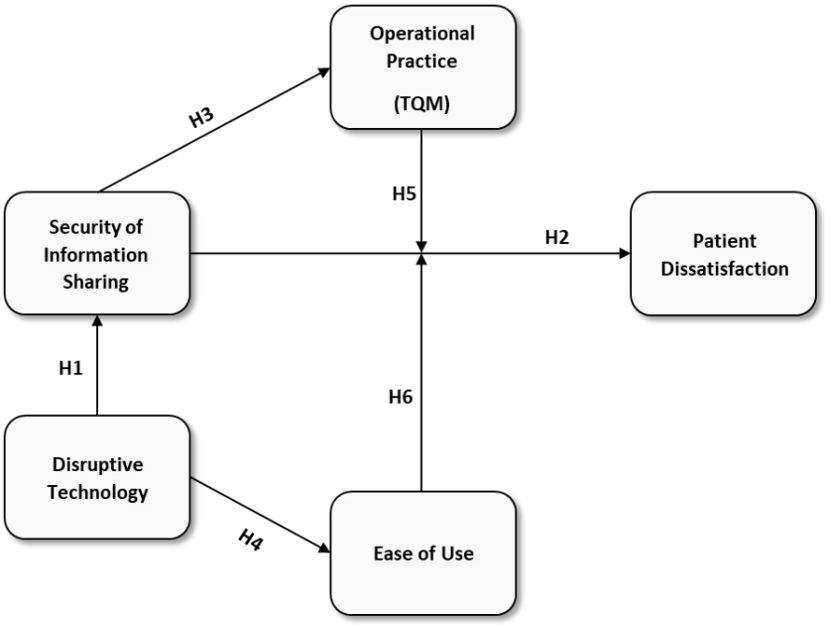

Fig. 1. Conceptual Framework for the Study

H1 - Disruptive technology has an impact on security of information sharing

In this hypothesis, the study preconceives that disruptive technology has a positive impact on the nature of information sharing among the three Saudi Hospitals. [25] find that disruptive technologies have positively contributed to the enhanced security around sharing of patient data. With the rise of emerging technologies, specifically blockchain, the expectation is that healthcare facilities use such technologies to improve the security of information exchanges. According to [25], blockchain is a disruptive technology that is particularly useful in enhancing the security of online activities. Hence, the effect of disruptive technology on information sharing should be significant and positive.

H2 - Security of information sharing has an impact on patient dissatisfaction

The hypothesis envisions that by not guaranteeing patients of data privacy when sharing information with other facilities and authorities, patient dissatisfaction occurs at the three Saudi Hospitals. While patients may understand that sharing this information with other facilities is important for their care, there is no guarantee that the information will be used specifically for this purpose [4]. Hence, the lack of trust on the process leads patients to consider that the worst will happen to their information after sharing it with a hospital.

H3 - Security of information sharing has an impact on operational practice

This hypothesis contends that the practice of sharing patient information between and among healthcare facilities is good for the operations of Saudi Hospitals. Having access to a patient's medical records implies that the current medical practitioner does not have to conduct some tests on the patient [13]. It also prompts the physician in question to only conduct tests that have not been done on the patient. It reduces the time it takes for patients to obtain

feedback on their health statuses, which is a good operational practice. Additionally, [44] finds that when the security of information sharing is sabotaged, there might be a need to overhaul the entire system and check for vulnerabilities. During this time, the system may be unavailable or supporting only a few limited functionalities. It can paralyze a hospital for days, weeks, or months until the experts have unearthed the source of the security breach. Therefore, security of information sharing has a positive effect on operational practice.

H4 - Disruptive Technology has an impact on Ease of use

This hypothesis contends that emerging technologies of a disruptive nature tend to improve the ease of use of hospital management systems at the selected Saudi Hospitals. According to [31], newer technologies in the industry have had a positive effect in how hospitals execute digital transactions. They do so by enhancing the user interfaces, using artificial intelligence to make more accurate predictions, and including more features that make digital operations more seamless. Hence, disruptive technology should have a significant and positive effect on the ease of use.

H5 - Operational practice moderates the relationship between security of information sharing and patient dissatisfaction

This hypothesis suggests that the effect of security of information sharing on patient dissatisfaction is mediated by operational practice at targeted Saudi Hospitals. It means that guaranteeing the security of information is not enough to mitigate patient dissatisfaction. According to [44], good operational practices such as the adoption of Kaizen and six sigma improves significantly improve the predictive ability of security of information sharing on patient dissatisfaction. This positive mediating effect comes as a result of the power of such techniques to influence the service offered to patients. The source also adds that the use of total quality management practices can be added upon any other hospital strategy to mitigate patient dissatisfaction.

H6 - Ease of use moderates the relationship between security of information sharing and patient dissatisfaction

This hypothesis contends that the ease of use of disruptive technology mediates the effect that security of information sharing has on patient dissatisfaction at Saudi Hospitals. It is not enough to have the technologies; the question is whether they can be used in the context in question. [31] contends that the ease of use of hospital systems ensures that patients are served fast and effectively. Hence, the source claims that having an easy-to-use hospital management system promotes satisfaction provided there is the guarantee that patient data captured in the process is safe from unauthorizes access. As [33] argue, blockchain technology is a difficult concept that applying it in a healthcare setting and expecting users to be comfortable with it may not be realistic. There is a need to abstract the technical features and allow users to interact with the regular features that they are used to. In this configuration, security of information sharing would be guaranteed and patient dissatisfaction mitigated.

4. Research Methodology

4.1 Construct Measurement and Questionnaire Design

To establish the factors contributing to customer dissatisfaction, this study considered four variables, namely security of information sharing, disruptive technology, ease of use, and operational practice. As a primary research investigation, the study relied on a questionnaire, which the researcher used to obtain responses from hospital staff members from various facilities. The measurement of these construct variables utilized the Likert scale of 1 through 5, where 1 indicated the lowest level of agreeableness and 5 indicated the highest agreeableness level by an individual. In ensuring content validity of the instrument, the researcher sourced the questions for each construct from peer reviewed articles that dealt with a specific construct. **Table 1** shows the questions, their parent constructs, and their sources.

Table 1. Constructs and survey items

Construct	Survey Question	Sources
Security of Information Sharing	Our staffs are well-trained on enforcing the security of EHR, patient information maintenance and sharing	[6]
	Our EHR systems are audited periodically to detect and unroot phishing and other unauthorized access to patient information	
	Sharing patient data for research usually does not attach the identities of patients to the shared data	
Operational Practice	Our facility engages in total quality management practices in all areas of operation during the pandemic	[46]
	Our facility extensively implements the Kaizen approach in carrying out its operations to enhance the safety and comfort of patients during the pandemic	
	Our facility extensively implements the six-sigma model to eradicate queues and enhance the efficiency of operations	
Disruptive Technology	Our facility's systems utilize the blockchain technology to enhance security and functionality	[47]
	A significant proportion of our systems' functionalities are powered by artificial intelligence	
	We adapt to the newest technological trends fast	
Ease of Use	Our systems' user interfaces are simple and intuitive to interact with	[48]
	The organization of menus and items on our systems foster expediency and efficiency	
	The interfaces running on our systems prevent errors and wrong input	
Patient Dissatisfaction	We receive a significant number of patients from referrals	[45]
	Many of our patients explicitly acknowledge their satisfaction with our services	
	We have many cases of repeat patients coming to our facility	

In affirming the content validity of the instrument, the researcher engaged research experts who examined the questionnaire to determine whether the questions were relevant to the attainment of the purposes of the investigation. The outcome of their examination was positive because they found all the questions relevant. Hence, the content validity of the questionnaire was 100%. There was a need to establish the instrument's reliability. Firstly, the researcher conducted a mini-study, which involved 20 participants five times. After the analysis of the results, the study found that the consistency among responses given by the same respondents was 98%, which confirmed the reliability of the tool. Additionally, the researcher considered running reliability tests of the data on SPSS. Using the software, the study found that the Cronbach's Alpha depicting reliability was 95%, which was acceptable since it was greater than the threshold of 70%.

4.2 Sampling and Data Collection

The study engaged with 3 hospital staffs in Saudi Arabia. All these hospitals which the researcher leveraged to disburse links to the online questionnaire. In this case, the researcher first approached the management of the hospitals and indicated their interest to carry out the survey. After the acceptance, the researcher was introduced to various heads of groups around the hospital with whom they shared the questionnaire links. The group leaders then shared the links via secure email system. The number of attempts made to respond to the questionnaire was 434. However, complete and valid responses were 303. Computing the response rate is hard because the number of staffs exposed to the links is unknown.

Apart from the online disbursed questionnaire, the researcher also used a paper-based questionnaire, which was shared with departmental heads at the hospitals. The number of questionnaires shared in this way was 51. Those that managed to fill them in and hand them back were 47. Hence, the response rate was 92.2%. The data obtained was cleaned for outliers and validated programmatically using the SPSS software. In building the structural equation models, the researcher opted for AMOS as the preferred tool to draw the model and produce outputs. Some of the tabular data needed some editing for presentation purposes. Therefore, the researcher used MS Excel to edit their appearance.

5. Data Analysis

5.1 SEM Approach to the Operationalization of the Study Constructs

In this section, the study establishes the assessment of the measurement model and computes some reliability and validity metrics.

5.2 Assessment of the Measurement Model

To carry out the structural model analysis, the study used the AMOS software. The analysis first established the reliability coefficients of the variables under investigation as reported in the subsequent sections. The primary variables that were considered for analysis were patient dissatisfaction, security of information sharing, disruptive technology, ease of use, and operational practice.

5.3 Indicator Reliability

Indicator reliability refers to the ability of the construct variables to consistently explain the variance in the target variable. The path-weighting scheme is more reliable relative to the factorial scheme. This analysis used the factor loadings and their respective error values to compute the indicator reliability of all the construct variables in the study. Findings suggested that all the indicators passed this reliability test because they all scored at least 0.700, which is the conventional threshold acceptable to affirm the consistency of indicator variables as shown in **Table 2**.

Table 2. Constructs Evaluation

Construct	Items	Factor Loading	Composite Reliability	Indicators	Cronbach's Alpha	AVE
Security of Information Sharing	SIS 1	0.9	0.86	3	0.843	0.67
	SIS 2	0.771				
	SIS 3	0.773				
Disruptive Technology	DSR 1	0.521	0.71	3	0.713	0.47
	DSR 2	0.535				
	DSR 3	0.929				
Ease of Use	EOU 1	0.787	0.81	3	0.792	0.58
	EOU 2	0.818				
	EOU 3	0.683				
Operational Practice	OPR 1	0.691	0.71	3	0.713	0.45
	OPR 2	0.631				
	OPR 3	0.694				
Patient Dissatisfaction	PDS 1	0.751	0.84	3	0.824	0.65
	PDS 2	0.920				
	PDS 3	0.726				

5.4 Internal Consistency

The internal consistency of an instrument is determined by examining the degree to which the specific question variables explain their latent constructs. The universally acceptable level is 0.70 as the minimum value. The analysis indicated that all the variables scored an internal consistency value of 0.777, which is greater than 0.70. Hence, the instrument can be considered to be internally consistent as shown in **Table 2**.

5.5 Convergent Validity

Convergent validity occurs when an item and its intended measurement constructs correlate significantly. Essentially, an item's measurement should have a strong association because the child variables explain the parent variable. Without this correlation, it would imply that the some of the selected construct or indicator variable does not accurately measure the parent variable. To compute convergent reliability, this study considered the Average Variance Extracted values, which are reported in the AVE column of **Table 2** Findings indicate that two construct variables scored greater than 0.5. The minimum acceptable value is 0.5. Therefore, most indicator variables seemed to fail on the convergent reliability test.

5.6 Discriminant Validity

Discriminant validity is acceptable where the indicators of a variable explain that variable more than they do explain other variables in the model. In other words, a construct variable should not be explained better by question variables belonging to other construct variables. To make this determination, the Fornell-Lacker Criterion was used, where the discriminant validity value must be greater than the correlation coefficients. From **Table 3**, it is clear that all the construct variables passed the discriminant validity test.

Table 3. Discriminant Validity test

	Security of Information Sharing	**Disruptive Technology**	**Operational Practice**	**Ease of Use**
Security of Information Sharing	**0.817**			
Disruptive Technology	0.735	**0.688**		
Operational Practice	0.681	0.681	**0.765**	
Ease of Use	0.596	0.669	0.596	**0.673**

5.7 Assessment of the Structural Model

Fig. 2 shows the structural model developed in AMOS to depict the associations between and among study variables.

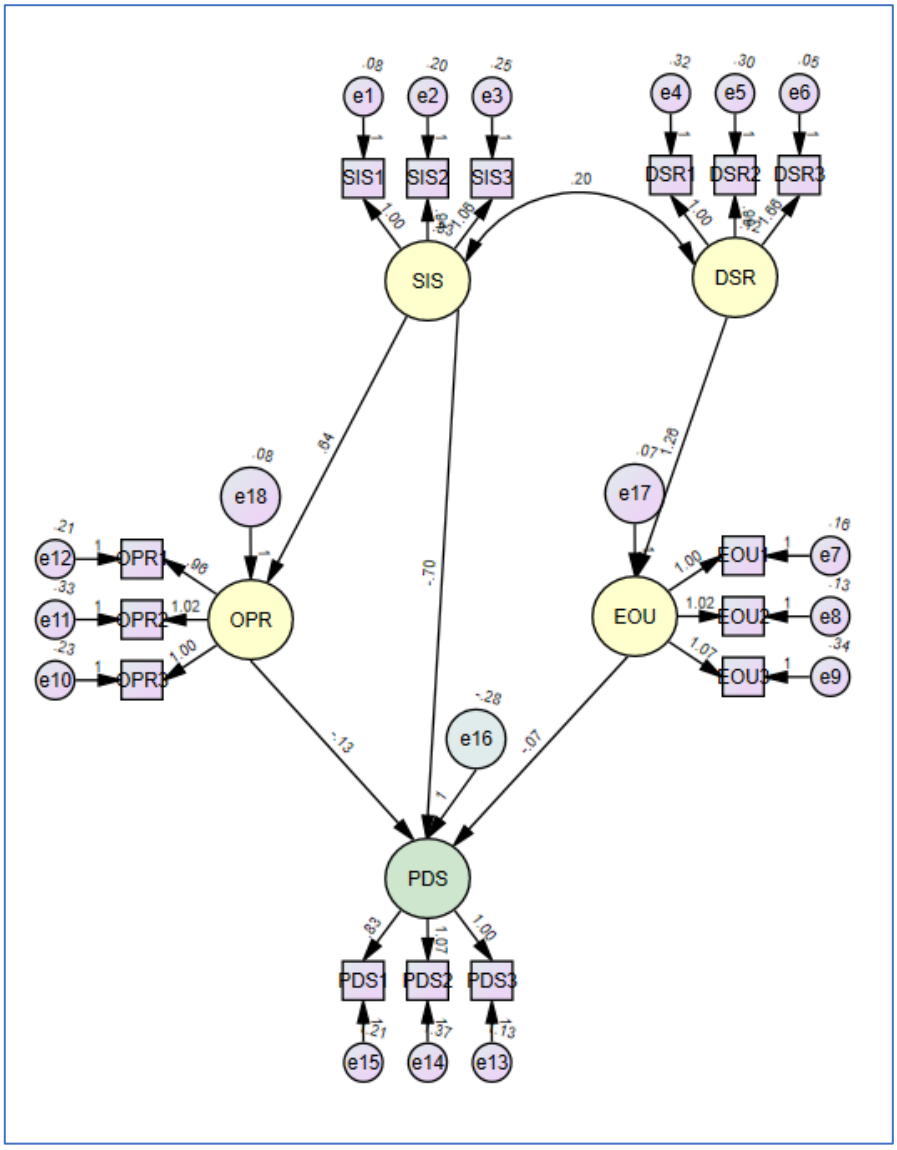

Fig. 2. Structural model

5.8 Model Fit

From the examination of the model and as shown in **Table 4**, it is clear that it is significant. The chi-square test run indicates that it scored 466.936 (p=0.000, df=84) on the default model, which implies that the chances of obtaining a discrepancy from the model projections are very low. For this reason, the analysis suggests that the model is significant as a whole. However, there is a need to inspect the significance of the individual elements of the model regarding their effect on patient dissatisfaction.

Table 4. Model fit indices

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	36	466.936	84	.000	5.559
Saturated model	120	.000	0		
Independence model	15	2949.989	105	.000	28.095

The effect of information sharing on patient dissatisfaction was the highest, as it scored a beta coefficient of -0.70 and R Squared of 0.49. This value suggests that the security of information sharing explains 49% of the variation in patient dissatisfaction. The effect of security of information sharing on operational performance was denoted by a beta coefficient of 0.64, and an R Squared Coefficient of 0.41. Again, this value suggests that security of information sharing explains 41% of the variation in operational practices. The effect of security of information sharing on patient dissatisfaction mediated by operational practice scored a beta coefficient of -0.13. This effect was minimal but still significant. Ease of use had a negative mediation effect on the effect of disruptive technologies on patient dissatisfaction, as it scored a beta coefficient of -0.07. It is a mild effect and cannot be considered to be reliable as such. The effect of disruptive technology on the ease of use of healthcare systems was denoted by a beta coefficient of 1.26 as shown below in **Table 5**.

Table 5. Path Analysis

Hypothesis	Path	Beta	p-value	Result
H1	DSR → SIS	0.20	0.00	Supported
H2	SIS → PDS	-0.70	0.00	Supported
H3	SIS → OPR	0.64	0.00	Supported
H4	DSR → EOU	1.26	0.00	Supported
H5	SIS → OPR → PDS	-0.13	0.00	Supported
H6	DSR → EOU → PDS	-0.07	0.00	Supported

6. Discussions, Implications and Limitations

6.1 Discussions and Implications

The study has revealed that disruptive technology has a significant effect on security of information sharing. This effect implies that disruptive technologies are an integral part of hospitals' efforts to secure patient information while sharing it. The study was compelled to refuse to reject the relevant null hypothesis because sufficient evidence had come to light to support it. For a one of the hospitals, these findings imply that the adoption of disruptive technologies can positively influence the ability of the hospital to secure patient information. These findings are consistent with the study conducted by [25]. The said investigation argues that technologies such as blockchain have significantly improved the manner in which information storage, dissemination, and transmission occurs in the healthcare field. Information disseminated in this fashion evades unauthorized interceptions and usually protects the identity of the owner. Similarly, [6] posit that emerging technologies in data management are focusing on the protection of patients' privacy. Research studies that require patient information do not necessarily have to obtain their identity. Hence, disruptive

technologies such as the one mentioned above has been instrumental in ensuring that such studies only get what they need.

Findings have suggested that the security of information sharing significantly impacts patient dissatisfaction levels. The negative effect implies that if a hospital enhances its compliance with securing patient data, their patients' dissatisfaction levels are likely to decline. These findings seem to affirm the hypothesis held throughout the study that the sharing of patient information affects patient dissatisfaction. This position is consistent with that held in the study conducted by [4]. The study consistently claims that when patients feel that their personal data is not safe in the hands of a healthcare provider, their dissatisfaction levels dwindle. This low satisfaction manifests even in the even that the patients have been accorded quality treatment at a facility. According to [15], low satisfaction by patients is a key indicator that a hospital is not performing to its level best. By simply enhancing the security around the management of patient data, this study has shown that healthcare facilities can improve their patients' perception of quality. It is an indication that securing patient data and explicitly showing these efforts to patients can go a long way in enhancing their satisfaction levels.

The investigation has revealed that security of information sharing has a significant effect on operational practice. For this reason, the study had to refuse to reject the null hypothesis made beforehand suggesting that operational practice was a product of security of information sharing. The systems that hospitals use are subject to both internal and external experts. If a hospital exhibits any signs of insecurity, audits and repairs may ensue for several days, weeks, or months to unearth the security threat. During this time, operations may not as smooth because of the absence or limited use of the system to transaction. Hence, the association between security of information sharing and operational practice. Also, securely transmitting patient information between and among healthcare organizations is critical to the operations of such entities. These findings seem to concur with those established in the study by [38] where the researchers indicated that if a facility has access to a patient's medical records, it does not necessarily have to carry some tests already done on the patient in the recent past. Such information is great operational significance because it saves time and helps to zero in on the problem.

Findings indicated that disruptive technologies have a significant impact on the ease of use of hospital electronic health records systems. For this reason, the researcher refused to reject the null hypothesis held throughout this investigation. The ease of use, which is measured by efficiency, navigability, intuitiveness, and vulnerability to errors, is a key metric when determining whether a system is fit for use in a hospital. Saudi hospitals can leverage this information to enhance the ease of use of its systems. As noted in [48], the execution of digital transactions has been enhanced by emerging technologies over time. A good example given in this context is artificial intelligence, which has ensured that medical diagnoses are efficient by using intelligent collaborative software. Hospitals in some regions seem to be benefitting from this technology, as it has streamlined their operations and alleviated many of physicians' deficiencies.

The study finds that operational practice effectively subtly mediates the effect of security of information sharing on patient dissatisfaction. Even here, the researcher refused to reject the relevant null hypothesis because there was sufficient evidence to suggest some mediation. It meant that while the security of information sharing variable was effective in influencing patient dissatisfaction, operational practice could also affect this relationship. If Saudi

Hospitals improve their operational practices, they can leverage security of information sharing to impact patient dissatisfaction. According to [28], quality management practices such as Kaizen and Six sigma have been known to impact patient satisfaction levels even in hospitals where the security of information sharing is guaranteed. By applying these quality management techniques, Saudi hospitals would be building an even more robust strategy against patient dissatisfaction. This study has made the novel revelation that the security of information sharing coupled with proper operational practices can have a significant positive effect on patient dissatisfaction levels. If hospitals can leverage on these findings, they stand a chance of alleviate patient dissatisfaction by a great margin.

The study failed to establish a significant mediating effect of the ease of use in the relationship between security of information sharing and patient dissatisfaction. Therefore, the researcher rejected the null hypothesis held throughout the investigation. The evidence was insufficient to back up the claim that ease of system use significantly mediates between the two main variables. While it is a good practice for Saudi hospitals to consider enhancing the use of information systems, its effect on patient dissatisfaction is minimal. The findings are inconsistent with those established in the study by [45]. The said study finds that the ease of use of hospital systems contributes positively to limiting patient dissatisfaction by leveraging the security of information sharing. By examining the concepts closely, it seems the findings in this study are justified. There should not be a significant relationship between the ease of use of EHR systems and how patients gauge their dissatisfaction. The two are fairly distant concepts with minimal points of intersections.

6.2 Limitations

The study in focus succeeded in finding answers to the purpose and objectives of the investigation. However, it encountered some limitations that could have had a negative effect on the validity of the reported findings. Below is an outline of the said limitations.

1. The researcher did not have control over who answered the online questionnaire. The disbursement of the questionnaire was via a link that was sent to the healthcare professionals of the three hospitals via official email. However, these links could have been further shared with other parties that had little knowledge on the subject at hand. To counter against such as possibility, the researcher specifically instructed that the survey was to be taken only by healthcare professionals.
2. Some respondents may have attempted to answer multiple times, which would have violated the expectations of the study. To curb against this possibility, the online survey required one to register with an email before attempting to fill in their answers. If an email has already been used to answer, such a respondent would be unable to proceed beyond the first page.
3. The respondents may have been biased while answering the questions. Some respondents may have felt the need to defend their hospitals so that the facility does not appear reckless for not having adopted latest technologies. In this case, they may have answered in favor of their organization even if the information provided is untrue or inaccurate in some aspects. The researcher preempted this possibility by explaining to the respondents about the importance of answering in truth. This information was included at the beginning of the questionnaires, right after one has signed the informed consent form.
4. While many Saudis and those working in Saudi hospitals are usually well-versed with the English language, there are some who are not as comfortable. Such people would give

wrong answers because they may have misunderstood the questions. Also, because of language difficulties, they could have reached out to friends to fill the questionnaire for them. Such a scenario would be disastrous because the data collected would be inaccurate. Therefore, in anticipation of this eventuality, the researcher prepared the questionnaire in English and Arabic. Respondents were at liberty to select which language they feel more comfortable in.

7. Conclusion and Future Research

This study has investigated the effect of security of information sharing on patient dissatisfaction. It included other factors such as disruptive technologies, operational practice, and ease of use to reach its conclusion. It reached out to three hospitals in various regions of the kingdom must work on their systems to reinforce them against the active threats on the privacy of patients' data by leveraging disruptive technology. While at it, they should also consider ensuring that their operational practices embrace quality management techniques. Many other areas of research need to be addressed. It concluded that indeed, security of information sharing influences patient dissatisfaction. However, the investigation was not conclusive. Many other areas were either underdeveloped or not touched by the study in focus. One of the suggested areas for furfure research is deliberating on the mediating effect of patient consultation on the relationship between security of information sharing and patient dissatisfaction. Also, since the research has been overly about patient dissatisfaction, it would be interesting to consider one that captures patient satisfaction. Finally, another potential area of study is determining the opinions of healthcare personnel regarding emerging technologies that seek to protect patient privacy.

References

[1] P. Esmaeilzadeh and M. Sambasivan, "Patients' support for health information exchange: a literature review and classification of key factors," *BMC medical informatics and decision making*, vol. 17, no. 1, pp. 1-21, 2017. Article (CrossRef Link)

[2] M. M. Mello, K. L. Ding, and L. Savage, "Legal barriers to the growth of health information exchange—boulders or pebbles?," *The Milbank Quarterly*, vol. 96, no. 1, pp. 110-143, 2018. Article (CrossRef Link)

[3] N. Shen et al., "Understanding the patient privacy perspective on health information exchange: a systematic review," *International journal of medical informatics*, vol. 125, pp. 1-12, 2019. Article (CrossRef Link)

[4] C. S. Cocanour, "Informed consent—It's more than a signature on a piece of paper," *The American Journal of Surgery*, vol. 214, no. 6, pp. 993-997, 2017. Article (CrossRef Link)

[5] J. Pool, S. Akhlaghpour, and F. Fatehi, "Health Data Privacy in the COVID-19 Pandemic Context: Discourses on HIPAA," in *Navigating Healthcare Through Challenging Times*, New York: IOS Press, 2021, pp. 70-77. Article (CrossRef Link)

[6] W. Bani Issa et al., "Privacy, confidentiality, security and patient safety concerns about electronic health records," *International nursing review*, vol. 67, no. 2, pp. 218-230, 2020. Article (CrossRef Link)

[7] C. Shachar, J. Engel, and G. Elwyn, "Implications for telehealth in a postpandemic future: regulatory and privacy issues," *Jama*, vol. 323, no. 23, pp. 2375-2376, 2020. Article (CrossRef Link)

[8] I. Ekong, E. Chukwu, and M. Chukwu, "COVID-19 mobile positioning data contact tracing and patient privacy regulations: exploratory search of global response strategies and the use of digital tools in Nigeria," *JMIR mHealth and uHealth*, vol. 8, no. 4, p. e19139, 2020.

Article (CrossRef Link)
[9] L. J. Rogo-Gupta, C. Haunschild, J. Altamirano, Y. A. Maldonado, and M. Fassiotto, "Physician gender is associated with Press Ganey patient satisfaction scores in outpatient gynecology," *Women's Health Issues*, vol. 28, no. 3, pp. 281-285, 2018. Article (CrossRef Link)
[10] R. Lin, Z. Ye, H. Wang, and B. Wu, "Chronic diseases and health monitoring big data: A survey," *IEEE reviews in biomedical engineering*, vol. 11, no. 1, pp. 275-288, 2018. Article (CrossRef Link)
[11] V. Kisekka and J. S. Giboney, "The effectiveness of health care information technologies: evaluation of trust, security beliefs, and privacy as determinants of health care outcomes," *Journal of medical Internet research*, vol. 20, no. 4, p. e9014, 2018. Article (CrossRef Link)
[12] A. Jalil, R. Zakar, M. Z. Zakar, and F. Fischer, "Patient satisfaction with doctor-patient interactions: a mixed methods study among diabetes mellitus patients in Pakistan," *BMC health services research*, vol. 17, no. 1, pp. 1-13, 2017. Article (CrossRef Link)
[13] L. Savage, M. Gaynor, and J. Adler-Milstein, "Digital health data and information sharing: A new frontier for health care competition?," *Antitrust Law Journal*, vol. 82, no. 2, pp. 610-612, 2019.
[14] P. K. Wan, L. Huang, and H. Holtskog, "Blockchain-enabled information sharing within a supply chain: A systematic literature review," *IEEE Access*, vol. 8, no. 1, pp. 49645-49656, 2020. Article (CrossRef Link)
[15] S. K. Woody, D. Burdick, H. Lapp, and E. S. Huang, "Application programming interfaces for knowledge transfer and generation in the life sciences and healthcare," *NPJ digital medicine*, vol. 3, no. 1, pp. 1-5, 2020. Article (CrossRef Link)
[16] S. K. Mukhiya, F. Rabbi, V. K. I. Pun, A. Rutle, and Y. Lamo, "A GraphQL approach to healthcare information exchange with HL7 FHIR," *Procedia Computer Science*, vol. 160, no. 1, pp. 338-345, 2019. Article (CrossRef Link)
[17] A. A. Zaid, S. M. Arqawi, R. M. A. Mwais, M. J. Al Shobaki, and S. S. Abu-Naser, "The Impact of Total Quality Management and Perceived Service Quality on Patient Satisfaction and Behavior Intention in Palestinian Healthcare Organizations," *Technology Reports of Kansai University*, vol. 62, no. 3, pp. 221-232, 2020.
[18] F. Wu et al., "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 82, no. 1, pp. 727-737, 2018. Article (CrossRef Link)
[19] C. Thapa and S. Camtepe, "Precision health data: Requirements, challenges and existing techniques for data security and privacy," *Computers in biology and medicine*, vol. 129, no. 1, p. 104130, 2021. Article (CrossRef Link)
[20] Q. N. AL-Mahwey and H. R. Sayah, "The Impact of Information and Communication Technology on the Technical Quality of Health Services "A Study at Al-Shatrah General Hospital–Dhi-Qar, Iraq"," *Global Journal of Management And Business Research*, vol. 20, no. 5, pp. 1-33, 2020.
[21] M. Arafeh et al., "Using six sigma DMAIC methodology and discrete event simulation to reduce patient discharge time in king hussein cancer center," *Journal of healthcare engineering*, vol. 2018, 2018. Article (CrossRef Link)
[22] J. Y. Lee, K. L. McFadden, M. K. Lee, and C. R. Gowen III, "US hospital culture profiles for better performance in patient safety, patient satisfaction, Six Sigma, and lean implementation," *International Journal of Production Economics*, vol. 234, p. 108047, 2021. Article (CrossRef Link)
[23] S. A. V. Lordelo, S. M. S. Nogueira, J. R. d. Farias Filho, H. G. Costa, C. L. Barbosa, and R. D. Calado, "Kaizen and Healthcare: A Bibliometric Analysis," in *Proc. of IFIP International Conference on Advances in Production Management Systems*, pp. 314-322, 2021. Article (CrossRef Link)
[24] B. Meskó, Z. Drobni, É. Bényei, B. Gergely, and Z. Győrffy, "Digital health is a cultural transformation of traditional healthcare," *Mhealth*, vol. 3, no. 9, p. 3, 2017. Article (CrossRef Link)
[25] S. Chakraborty, S. Aich, and H.-C. Kim, "A secure healthcare system design framework using blockchain technology," in *Proc. of 2019 21st International Conference on Advanced Communication Technology (ICACT)*, pp. 260-264, 2019. Article (CrossRef Link)
[26] W. L. Bi et al., "Artificial intelligence in cancer imaging: clinical challenges and applications," *CA: a cancer journal for clinicians*, vol. 69, no. 2, pp. 127-157, 2019. Article (CrossRef Link)

[27] M. Jamshidi et al., "Artificial intelligence and COVID-19: deep learning approaches for diagnosis and treatment," *IEEE Access*, vol. 8, pp. 109581-109595, 2020. Article (CrossRef Link)
[28] M. Coccia, "Deep learning technology for improving cancer care in society: New directions in cancer imaging driven by artificial intelligence," *Technology in Society*, vol. 60, no. 1, p. 101198, 2020. Article (CrossRef Link)
[29] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability," *Computational and structural biotechnology journal*, vol. 16, pp. 224-230, 2018. Article (CrossRef Link)
[30] Y. Zhuang, L. R. Sheets, Y. W. Chen, Z. Y. Shae, J. J. Tsai, and C. R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE journal of biomedical and health informatics*, vol. 24, no. 8, pp. 2169-2176, 2020. Article (CrossRef Link)
[31] H. M. Hussien, S. M. Yasin, S. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction," *Journal of medical systems*, vol. 43, no. 10, pp. 1-35, 2019. Article (CrossRef Link)
[32] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782-147795, 2019. Article (CrossRef Link)
[33] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, 2018. Article (CrossRef Link)
[34] E. Layfield, V. Triantafillou, A. Prasad, J. Deng, R. M. Shanti, Newman, J. G, and K. Rajasekaran, "Telemedicine for head and neck ambulatory visits during COVID-19: evaluating usability and patient satisfaction," *Head & Neck*, vol. 42, no. 7, pp. 1681-1689, 2020. Article (CrossRef Link)
[35] S. Mukherjee and N. Lakshmikantha, "Does usage of Online Technology among hospitals improve communication with the stake holders? Examining the patient satisfaction based on the usage of online appointment applications in India," *Journal of Critical Reviews*, vol. 7, no. 13, pp. 1436-1441, 2020.Article (CrossRef Link)
[36] S. L. Vargo and R. F. Lusch, "Evolving to a new dominant logic for marketing," *Journal of marketing*, vol. 68, no. 1, pp. 1-17, 2004. Article (CrossRef Link)
[37] R. F. Lusch, "Reframing supply chain management: a service-dominant logic perspective," *Journal of supply chain management*, vol. 47, no. 1, pp. 14-18, 2011. Article (CrossRef Link)
[38] M. Blaschke, U. Riss, K. Haki, and S. Aier, "Design principles for digital value co-creation networks: a service-dominant logic perspective," *Electronic Markets*, vol. 29, no. 3, pp. 443-472, 2019. Article (CrossRef Link)
[39] R. Wilden, M. A. Akaka, I. O. Karpen, and J. Hohberger, "The evolution and prospects of service-dominant logic: an investigation of past, present, and future research," *Journal of service research*, vol. 20, no. 4, pp. 345-361, 2017. Article (CrossRef Link)
[40] S. K. Callaway and D. D. Dobrzykowski, "Service-oriented entrepreneurship: service-dominant logic in green design and healthcare," *Service Science*, vol. 1, no. 4, pp. 225-240, 2009. Article (CrossRef Link)
[41] Á. Kristjánsson and H. Egeth, "How feature integration theory integrated cognitive psychology, neurophysiology, and psychophysics," *Attention, Perception, & Psychophysics*, vol. 82, no. 1, pp. 7-23, 2020. Article (CrossRef Link)
[42] J. M. Wolfe, "Forty years after feature integration theory: An introduction to the special issue in honor of the contributions of Anne Treisman," *Attention, Perception, & Psychophysics*, vol. 82, no. 1, pp. 1-6, 2020. Article (CrossRef Link)
[43] J. Pomerantz and M. Portillo, "Emergent features, gestalts, and feature integration theory," *From perception to consciousness: Searching with Anne Treisman*, vol. 1, no. 1, pp. 187-192, 2012. Article (CrossRef Link)
[44] A. Karaca and Z. Durna, "Patient satisfaction with the quality of nursing care," *Nursing open*, vol. 6, no. 2, pp. 535-545, 2019. Article (CrossRef Link)
[45] A. H. Ramli, "Patient satisfaction, hospital image and patient loyalty in West Sulawesi Province," *Business and Entrepreneurial Review*, vol. 17, no. 1, pp. 1-14, 2019. Article (CrossRef Link)

[46] M. M. B. Tufail, M. Shakeel, F. Sheikh, and N. Anjum, "Implementation of lean Six-Sigma project in enhancing health care service quality during COVID-19 pandemic," *AIMS Public Health*, vol. 8, no. 4, pp. 704-719, 2021. Article (CrossRef Link)
[47] F. Bublitz et al., "Disruptive technologies for environment and health research: an overview of artificial intelligence, blockchain, and internet of things," *International journal of environmental research and public health*, vol. 16, no. 20, p. 3847, 2019. Article (CrossRef Link)
[48] A. L. Russ and J. J. Saleem, "Ten factors to consider when developing usability scenarios and tasks for health information technology," *Journal of biomedical informatics*, vol. 78, no. 1, pp. 123-133, 2018. Article (CrossRef Link)

Hasan Beyari received BSc, MSc and Ph.D. degrees in marketing, consumer marketing and business information systems from University of Business and Technology (2007), Saudi Arabia, University of Liverpool (2009), UK and RMIT University (2018), Australia respectively. He currently works at Applied college, Umm Al-Qura University. He is an assistant professor of marketing and business information systems. He worked as Vice Dean and chairman of the department of administrative and financial sciences. He is an active researcher in the field of social commerce and marketing. His research interests are all related topics to social commerce, social media, marketing research, service marketing, and electronic commerce.

Mohammed Hejazi is an Assistant Professor of Supply Chain Management at the University of Business and Technology, Jeddah, Saudi Arabia. He is a former Chairman of Supply Chain Management Department and a former Vice Dean of Student Affairs at University of Business and Technology. He earned a PhD degree in Manufacturing and Technology Management from University of Toledo, USA. He holds a MSc degree in Environmental, Safety and Health Management from the University of Findley, USA and a BSc degree in Medical Science from King Abdul Aziz University, Saudi Arabia. His research interest is in the areas of Digital Supply Chain, Green Supply Chain, Health Care Operations, Service Innovations, Supply Chain Disruption, Supply Chain Resilience, Supply Chain Vulnerability and Sustainable procurement. His articles have been published in *Business Process Management Journal, Journal of Critical Reviews* and *Journal of Positive School Psychology*

Othman Alrusaini is an assistant professor of Computer Engineering at the Umm Al-Qura University, Makkah, Saudi Arabia. He received the Ph.D. degrees in Electrical & Computer Engineering from King Abdul Aziz University, in 2017. From 2019 to 2021, he worked as a chairman, Engineering and Applied Sciences Department at Umm Al-Qura University. His current research interests include Computer Networking, Fiber Optic Communication, Computer Security, Neural Networks, Machine Learning and Deep Learning.