

The impact of information security policies and innovations in digital technology on the transformation of healthcare in developing nations: A literature review

Rao Faizan Ali¹, Rao Nouman Ali², Sohaib Irfan³, *Bilal Hassan⁴

¹Universiti Teknologi PETRONAS, Malaysia

²College of physicians and surgeons, Pakistan

³Aga Khan University, Karachi, Pakistan

⁴London Metropolitan University, London, United Kingdom

*b.hassan@londonmet.ac.uk

Abstract. This paper delves into the pivotal challenges and transformative impacts of information security within the digital healthcare landscape of developing countries. Emphasizing the critical role of digital transformation in healthcare, this study highlights how it fundamentally enhances the efficacy and efficiency of healthcare systems. Central to our exploration are the multifaceted impacts of emerging technologies on patient data management in electronic health records (EHRs), encompassing aspects of risk management, utilization of advanced security tools, big data analytics, and the integration of cloud computing.

Our extensive literature review methodically examines the intricate interplay between these technological elements and their collective contribution to bolstering information security. We analyze various models and strategies currently being employed to safeguard sensitive healthcare data, addressing both technical and behavioral security challenges. The review synthesizes findings from a diverse array of sources, offering a nuanced understanding of how these security factors positively influence the digital healthcare transformation.

By exploring these dimensions, the paper aims to analyze the ongoing developments in digital healthcare security in developing countries as well as identifying key barriers and improvement opportunities.

Keywords: Emerging Technology, Healthcare, Digital transformation, Information security

Introduction:

This research article presents an efficient literature review about digitalized solutions for information security and the digital transformation of healthcare. Information technology (IT) has become essential for healthcare establishments as there is increased demand for management of data and the smooth operation of healthcare systems[1, 2]. The growing use of IT in health organizations has identified many errors related to low compliance with information security policies. Modern researchers have found data security breaches in healthcare organizations to be a critical area for investigation[3–5]. Information security is as much a technical issue as it is a behavioral one.

As time and technology progress, the evolution of information security has become a primary concern for organizations. Healthcare is undergoing a transformation thanks to digital twin technology, a virtual replica system that combines IoT and AI and allows for individualized therapy through thorough data analysis. This invention highlights its vital role in promoting patient-centered care frameworks and the digital transformation of healthcare by providing predictive insights on medication, dietary modifications, and surgical outcomes.

Towards the end of 1990s, Health Information Systems (HIS) were installed in many developing countries. Since then Health information systems has employed in government as well as private hospitals. HIS is a multi-operational system that maintains patient information, manages staff, and handles administrative tasks. Health information system can used as an application or be accessed via internet for data management. Easier accessibility makes this system vulnerable[6]. HIS data is sensitive and requires enhanced security measures. While the principles of patient privacy are widely accepted, they are not always enforced. Adequate security is essential for protecting patients' personal health information, regardless of the information's nature[7–9]. In health care sector, users take information security lightly. Employees have legal access to health information systems, and their negligence can put at risk the confidential data of patients[10].

Health organizations are considered among the most vulnerable in terms of information security. They tend to prioritize more on technicalities for security threats rather than on documentation and policies to mitigate system threats. Insider threats are more critical than external security problems, prompting health organizations to address insiders' behavioral issues. Negligence regarding the organization's information security policy has caused considerable damage. The heavy workload of health employees often leads to stress and conflicts, which are form bases for poor compliant behavior. Such stress and conflicts can be alleviated through organization surveillance and strong social cohesion. This paper synthesizes a simple review of literature on the necessity of information security and its role in the digital transformation of healthcare systems in developing countries.

Digital technology in health care:

Digital technology in healthcare represents a complex task[11]. It is an essential component of successful healthcare transformation [12]. The advancement of digital technology is often discussed as a complex institutional change. The creators of the technology link the stages of this transformation to the cooperation among three types of innovative advances[13]. In order to deliver digital health, involvement from multiple stakeholders is necessary, with the government often playing a crucial role. Understanding how government organization plan for digital transformation, especially in healthcare, is crucial for other involved[14].

Information security in digitalization is a significant and growing concern that affects all sectors in this digital age. Without information security, confidential information can be accessed by unrelated individuals or to the data being compromised. Considering this, the current study addresses information security in developing countries[15]. According to [16], technological innovation and transformation through the lens of four emerging technology fields—data analytics, the Internet of Things, blockchain, cloud computing, and artificial intelligence—underscore the need for better information security. Digital technologies have revolutionized our world since the advent of the Internet[17–19].

The healthcare industry assists with saving and extending patients' lives with a plan "to get individuals stable"[20]. Nations use personal health information (PHI), which is stored and transmitted through digital networks[21]. Updating and maintaining existing digital systems presents a significant challenge as a lot of software products are currently being used on computers and smartphones[22]. In the information systems (IS) security literature, there has been a growing interest in examining the issue of employee behavior that may have security implications in organizations. It can be addressed with operational controls within a covered entity[20, 23]. Lastly, a number of avenues for data security and privacy breach research have surfaced in the field of public reforms, particularly in areas like clinical research, the creation of public health information networks (Figure 1), disaster response, and the evaluation of healthcare services. These include the development of data interoperability, the regulatory implications of healthcare technology adoption, and secured data disclosure mechanisms [18].

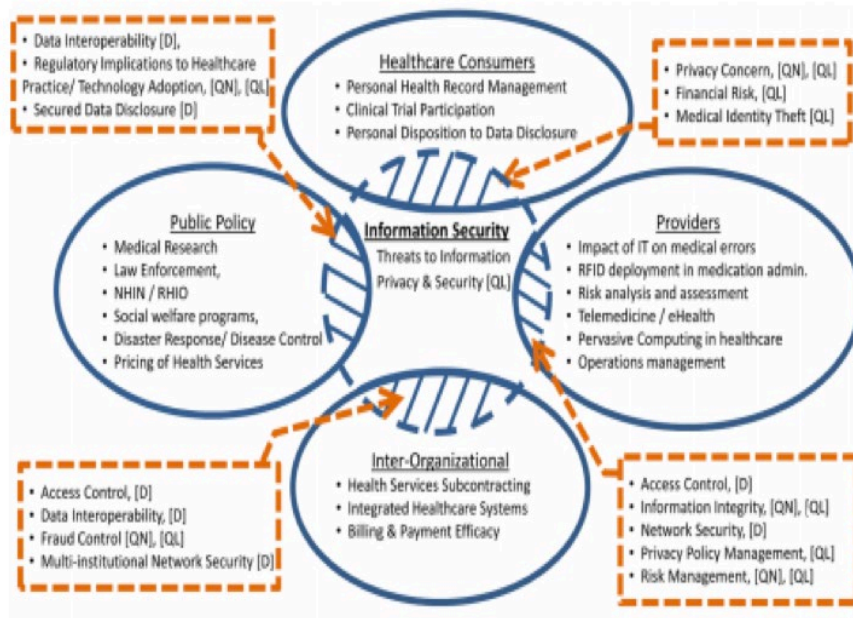


Fig. 1. Domains in the healthcare information security

Information security policy:

Security has been an important topic in popular media and journals recently. Alarmingly, the risk of attacks continues to grow. This includes adherence to an Information Security Policy Compliance (ISPC) framework[24]. While popular media often employs data breaches to external hackers, most misconducts result from employee negligence or unable to adhere to data security guidelines and procedures. To alter employee conduct, we draw from the institutional climate literature and introduce the term Information Security Climate Index, developed and checked through two studies[25]. The study begins by conducting a series of semi-structured interviews, which include end-user groups as well as IT staff and information security personnel. Regardless, data security remains a significant challenge in Health Information Systems (HIS) due to the sensitivity of the data and the critical nature of healthcare services, which increases the risk of unauthorized access and disclosure of confidential information[26–28].

Digital technology and information security policy:

This article presents a simple literature review on information security risk in the field of health. Cyber risk is the sum of the likelihood and impact of an undesirable event. It is reported as a function of probability that a source of threat will exploit a potential

weakness and the resulting effect of this harmful event on the institution[29]. Cyber threat, also known as information technology risk, represents a new challenge, affecting organizations' information and technological resources. The term 'cyber' refers to cyberspace, a domain composed of digital networks used for storing, customizing, and communicating information. This encompasses all sections supporting businesses and service[30]. Digital technology has brought significant changes and continues to transform our world, especially evident in the digital market transformation[31].

Cyber attacks and their aftershocks using innovation technologies

The effect of the internet on is undeniable. It has laid a framework for instant communication, exchange, and collaboration among individuals and organizations worldwide. However, as the internet has progressed, the number of cyberattacks have also increased[34]. Cybercrime poses a threat to society and can result in harm. This section engages in a detailed analysis of the cybercrimes targeting individuals[35]. As technology and mobile applications grow in volume and complexity, malicious cyber threats are evolving. Consequently, we face a greater security problem on the internet than ever before. To protect critical organizational data and information system assets, organizations have implemented sophisticated monitoring systems[36, 37].

Methods and research approach:

Methods:

This study employs a literature review to collect, gather, and analyze previous research on digital technology and information security in the digital era, focusing on perspectives from developing countries. This methodology is suitable for summarizing literature on the identified issue and the goals of the research. The study uses a quantitative method to investigate the factors of digital technology that influence Information Security (IS) perspectives in healthcare units in developing countries, thus, this approach is termed a theoretical study.

According to the plan outlined by references [36, 37], to better understand the main problems with domain, the research reviewed previous literature on healthcare in developing countries, including Pakistan. Compared to industrialized nations, which have more sophisticated safeguards and awareness in place, poor countries confront unique issues when it comes to information security in healthcare because of their limited infrastructure and resources. Due to this discrepancy, healthcare data in developing nations is more susceptible to cyberattacks, which lowers the standard of patient treatment. It focused on barriers associated with emerging technology in

healthcare sectors, using perspective models. Adopting a positivist perspective in this study, the exploratory stage becomes the primary task, where the researcher reviews and surveys existing literature to understand the extent of work done in the domain being examined.

Research approach:

The methodology adopted helps perform research effectively. When conducting a research, selecting a quantitative approach is crucial. However, the quantitative approach must be firmly grounded in the goals of the research. Using the quantitative method as the main design of research not only strengthens the researcher's approach but also minimizes potential weaknesses (Creswell, 2013). A quantitative approach is typically used for independently testing theories by analyzing the relationships among parameters of interest. This method is commonly used and adopted by many data researchers.

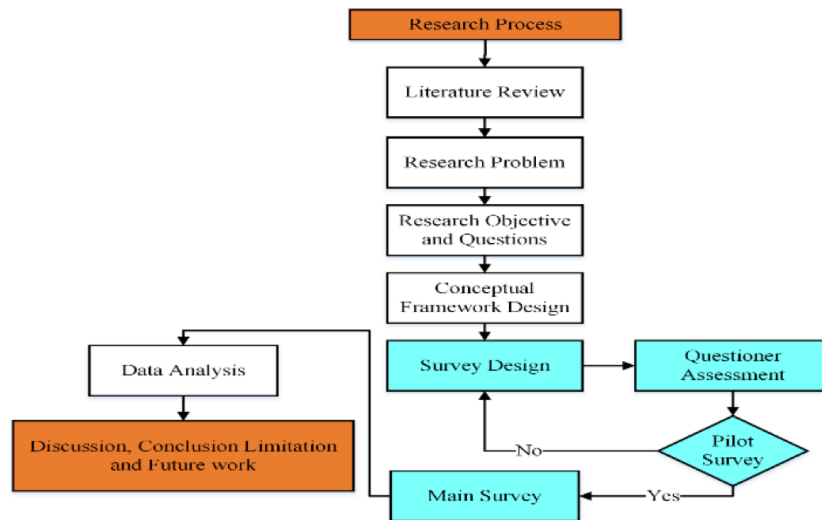


Fig. 2. Phases of the Quantitative Research Approach Adopted in the Current Study.

Creswell et al. [38] have stated that the research process consists of several essential phases. Figure 3 illustrates the adoption of a quantitative design, which can be achieved by following these phases: initiating the research process, conducting a literature review, identifying the research problem, formulating research objectives and questions, designing a conceptual framework, developing a survey, conducting data analysis, and developing a theoretical framework.

Conclusion:

In conclusion, this research highlights the main implications and relevant problem statements associated with the use of new technology and its impact on information security in transforming healthcare sector. It outlines specific goals to be achieved, the type of effort to be undertaken, and the overall impact. Additionally, it provides an overview of the current state of research and the methodology employed. Digital resources has the potential to close the gaps in time, distance, affordability, and expectations between patients and clinicians in healthcare. The future objective of the study is to explore the impact of developing technology and information security elements on healthcare transformation in Pakistan. To achieve this, 600 questionnaires will be given across ten hospitals within a particular region in Pakistan. Data will be collected from the selected sample using a survey method. This survey aims to explore a phenomenon of a specific activity[39]. The survey on this innovative technology collects data from several participants to assess various factors, testing the proposed hypotheses[40]. The questionnaire is an efficient data collection tool, allowing the researcher to understand the requirements and measure the variables of interest.

References

1. Ontological Model for Cohesive Smart Health Services Management. | Computers, Materials & Continua | EBSCOhost. <https://openurl.ebsco.com/EPDB%3Aagd%3A16%3A12291888/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Aagd%3A160062052&crl=c>. Accessed 21 Mar 2024
2. Naseer S, Ali RF, Dominic PDD, Saleem Y (2020) Learning Representations of Network Traffic Using Deep Neural Networks for Network Anomaly Detection: A Perspective towards Oil and Gas IT Infrastructures. *Symmetry* 2020, Vol 12, Page 1882 12:1882. <https://doi.org/10.3390/SYM12111882>
3. Shahriar H, Haddad HM, Farhadi M (2022) Assessing HIPAA Compliance of Open Source Electronic Health Record Applications. *Research Anthology on Securing Medical Systems and Records* 995–1011. <https://doi.org/10.4018/978-1-6684-6311-6.CH048>
4. Hasan Asfoor A, Kasim H, Binti A, et al (2022) Identifying Factors of Non-Compliance, Compliance with Information Security Policy, and Behavior Change to Compliance: Literature Review. *jonuns.com* AH Asfoor, H Kasim, ABA Latif, RA Razali, ZA Ibrahim, A Shanneb *Journal of Hunan University Natural Sciences*, 2022•*jonuns.com* 49:274–288. <https://doi.org/10.55463/issn.1674-2974.49.12.28>
5. Chen L, Xie Z, Zhen J, et al (2022) The impact of challenge information security stress on information security policy compliance: The mediating roles of emotions. *Taylor & Francis* L Chen, Z Xie, J Zhen, K Dong *Psychology Research and Behavior Management*, 2022•*Taylor & Francis* 15:1177–1191. <https://doi.org/10.2147/PRBM.S359277>

6. Humaidi N, Informatics VB-J of H& M, 2013 undefined Exploratory factor analysis of user's compliance behaviour towards health information system's security. academia.eduN Humaidi, V BalakrishnanJournal of Health & Medical Informatics, 2013•academia.edu
7. Islam S, Kwak D, Kabir M, et al The internet of things for health care: a comprehensive survey. ieeexplore.ieee.orgSMR Islam, D Kwak, MDH Kabir, M Hossain, KS KwakIEEE access, 2015•ieeexplore.ieee.org
8. Ali RF, Dominic PDD (2024) Investigation of information security policy violations among oil and gas employees: A security-related stress and avoidance coping perspective. *J Inf Sci* 50:254–272. <https://doi.org/10.1177/01655515221087680>
9. Hassandoust F, Subasinghage M, Johnston AC (2022) A neo-institutional perspective on the establishment of information security knowledge sharing practices. *Information and Management* 59:. <https://doi.org/10.1016/J.IM.2021.103574>
10. Humaidi N, Computer VB-MJ of, 2015 undefined The moderating effect of working experience on health information system security policies compliance behaviour. mjs.um.edu.myN Humaidi, V BalakrishnanMalaysian Journal of Computer Science, 2015•mjs.um.edu.my 28:2015
11. Parthasarathy R, Kern J, Knight JR, et al (2019) A Conceptual Model of the Role of Relative Advantage, Compatibility and Complexity in Electronic Medical Records Implementation Success. 26:
12. Galetsi P, Katsaliaki K, Kumar S (2023) Exploring benefits and ethical challenges in the rise of mHealth (mobile healthcare) technology for the common good: An analysis of mobile applications for health specialists. *Technovation* 121:. <https://doi.org/10.1016/J.TECHNOVATION.2022.102598>
13. Si S, Hall J, Suddaby R, et al (2023) Technology, entrepreneurship, innovation and social change in digital economics. *Technovation* 119:. <https://doi.org/10.1016/J.TECHNOVATION.2022.102484>
14. Benjamin K, Health HP-D, 2018 undefined (2018) Digital transformation in government: Lessons for digital health? journals.sagepub.comK Benjamin, HWW PottsDigital Health, 2018•journals.sagepub.com 4:205520761875916. <https://doi.org/10.1177/2055207618759168>
15. Osahon Igbino M, Elojie A, Joy Ikenwe I, et al (2016) Information security in the digital age: The case of developing countries. researchgate.netJJ Ikenwe, OM Igbino M, AA ElojieChinese Librarianship: An International Electronic Journal, 2016•researchgate.net 42
16. Li J, Herdem MS, Nathwani J, Wen JZ (2023) Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management. *Energy and AI* 11:. <https://doi.org/10.1016/J.EGYAI.2022.100208>
17. Weill P, Woerner S (2018) Is your company ready for a digital future?
18. Ahouanmenou S, Van Looy A, Poels G (2023) Information security and privacy in hospitals: a literature mapping and review of research gaps. *Inform Health Soc Care* 48:30–46. <https://doi.org/10.1080/17538157.2022.2049274>
19. Ande R, Adebisi B, Hammoudeh M, et al (2020) Internet of Things: Evolution and technologies from a security perspective. ElsevierR Ande, B Adebisi, M Hammoudeh, J SaleemSustainable Cities and Society, 2020•Elsevier 54:. <https://doi.org/10.1016/j.scs.2019.101728>
20. Hathaliya J, Communications ST-C, 2020 undefined An exhaustive survey on security and privacy issues in Healthcare 4.0. ElsevierJJ Hathaliya, S TanwarComputer Communications, 2020•Elsevier

21. Hassan N, Sciences ZI-P-S and B, 2012 undefined A conceptual model for investigating factors influencing information security culture in healthcare environment. ElsevierNH Hassan, Z IsmailProcedia-Social and Behavioral Sciences, 2012•Elsevier
22. Geismann J, Software EB-J of S and, 2020 undefined A systematic literature review of model-driven security engineering for cyber-physical systems. ElsevierJ Geismann, E BoddenJournal of Systems and Software, 2020•Elsevier
23. Security KG-C&, 2013 undefined Security-related behavior in using information systems in the workplace: A review and synthesis. ElsevierKH GuoComputers & Security, 2013•Elsevier
24. Nasirpouri Shadbad F, Biros D (2022) Technostress and its influence on employee information security policy compliance. Information Technology and People 35:119–141. <https://doi.org/10.1108/ITP-09-2020-0610/FULL/HTML>
25. Kessler SR, Pindek S, Kleinman G, et al (2020) Information security climate and the assessment of information security risk among healthcare employees. journals.sagepub.comSR Kessler, S Pindek, G Kleinman, SA Andel, PE SpectorHealth informatics journal, 2020•journals.sagepub.com 26:461–473. <https://doi.org/10.1177/1460458219832048>
26. Basfar R, ... KB-J of CS and M, 2020 undefined Information security assessment in King Abdullah Medical Complex: A case study. academia.eduRA Basfar, KY BajunaiedInternational Journal of Computer Science and Mobile Computing, 2020•academia.edu
27. Pirbhulal S, Samuel W, Wu W, et al (2019) A joint resource-aware and medical data security framework for wearable healthcare systems. ElsevierS Pirbhulal, OW Samuel, W Wu, AK Sangaiah, G LiFuture Generation Computer Systems, 2019•Elsevier. <https://doi.org/10.1016/j.future.2019.01.008>
28. Schmitz C, Security SP-C&, 2020 undefined LiSRA: Lightweight Security Risk Assessment for decision support in information security. ElsevierC Schmitz, S PapeComputers & Security, 2020•Elsevier
29. Sardi A, Rizzi A, Sorano E, et al Cyber risk in health facilities: A systematic literature review. mdpi.comA Sardi, A Rizzi, E Sorano, A GuerrieriSustainability, 2020•mdpi.com. <https://doi.org/10.3390/su12177002>
30. Kandasamy K, Srinivas S, Achuthan K, Rangan VP (2020) IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. SpringerK Kandasamy, S Srinivas, K Achuthan, VP RanganEURASIP Journal on Information Security, 2020•Springer 2020:. <https://doi.org/10.1186/s13635-020-00111-0>
31. Biener C, Eling M, Wirfs JH (2015) Insurability of cyber risk: An empirical analysis. Geneva Papers on Risk and Insurance: Issues and Practice 40:131–158. <https://doi.org/10.1057/GPP.2014.19>
32. Urintsov A, ... OS-2019 I, 2019 undefined Consulting of choice of information system in the conditions of digital transformation of business. ieeexplore.ieee.orgAI Urintsov, OV Staroverova, NA Mamedova, MA Afanasev, MS Klyachin2019 International Conference" Quality Management, Transport and, 2019•ieeexplore.ieee.org
33. Bada M, vulnerabilities JN-E cyber threats and cognitive, 2020 undefined The social and psychological impact of cyberattacks. Elsevier
34. arXiv:1811.06624 JN preprint, 2018 undefined (2019) Cybercrime and you: How criminals attack and the human factors that they seek to exploit. arxiv.orgJRC NursearXiv preprint arXiv:181106624, 2018•arxiv.org 662–690. <https://doi.org/10.1093/oxfordhb/9780198812746.013.35>

35. Quoc T, ... BH-: SA in TW of, 2023 undefined (2022) Study on the Intention and Behavior Complying with Accounting Information System Security Policy: The Case of Vietnam. atlantis-press.comTN Quoc, BN HuuInternational Conference on Emerging Challenges: Strategic, 2023•atlantis-press.com 77–92. https://doi.org/10.2991/978-94-6463-150-0_6
36. Li L, He W, Xu L, et al (2019) Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *Int J Inf Manage* 45:13–24. <https://doi.org/10.1016/J.IJINFOMGT.2018.10.017>
37. Journal PM-HER, 2023 undefined (2023) Sociology of education: Theories, communities, contexts. akjournals.comPJ MohammedHungarian Educational Research Journal, 2023•akjournals.com. <https://doi.org/10.1556/063.2023.00247>
38. Meissner HI, Creswell JW, Klassen AC, et al Best practices for mixed methods research in the health sciences. csun.eduJW Creswell, AC Klassen, VL Plano Clark, KC SmithBethesda (Maryland): National Institutes of Health, 2011•csun.edu
39. Lee V, Landers RN (2022) Sampling Strategies for Quantitative and Qualitative Business Research. *Oxford Research Encyclopedia of Business and Management*. <https://doi.org/10.1093/ACREFORE/9780190224851.013.216>
40. Sekaran U, Bougie R (2016) Research methods for business: A skill building approach