Chapter 11
Privacy and Security Concerns During the COVID-19 Pandemic: A Mixed-Method Study

Poonam Sahoo
https://orcid.org/0000-0001-7762-3570
National Institute of Technology, Karnataka, India

Pavan Kumar Saraf
National Institute of Technology, Karnataka, India

Rashmi Uchil
National Institute of Technology, Karnataka, India

ABSTRACT

The study's objective is to ascertain healthcare personnel's perspectives and experiences on information privacy and security during the COVID-19 pandemic. Despite the abundance of research on privacy and security issues, this study focuses on the elements that influence privacy concerns in volatile, unpredictable, complicated, and ambiguous situations, which in the current scenario might include the COVID-19 pandemic. Three levels of coding were applied to all interview transcripts using the qualitative technique. The pandemic of COVID-19 has raised various concerns about technology, data privacy, and protection. The study's objective is to find, extract, summarize, and evaluate trends in a list of privacy threats associated with the COVID-19 pandemic. Participants were healthcare practitioners who worked closely with COVID-19 cases during the COVID-19 pandemic.

INTRODUCTION

The Severe Acute Respiratory Syndrome Coronavirus-2 (SARS-Cov-2) outbreak began in humans in

DOI: 10.4018/978-1-6684-5250-9.ch011

Copyright © 2022, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

2019 (WHO,2020). As the COVID-19 influenza pandemic swept over the world, it accelerated the use of digital technologies, mostly for communication and commerce, and the growth of these technologies resulted in technological risks (Li, 2020). Almost every gadget is interdependent and networked, raising concerns about data privacy and protection. Since the outbreak, several incidents of healthcare fraud have been documented, and one of the major concerns across the board is data privacy (Mason & Williams, 2020; Viaene & Dedene, 2004). It is critical to have access to healthcare professionals' perceptions and experiences during pandemics in order to take control of the situation (Liu et al., 2020). Numerous academics and healthcare professionals have stressed the privacy and security concerns that have arisen as a result of the evolution of healthcare technology (Chung & Hershey, 2012; Ermakova et al., 2013; Parks et al., 2011). Healthcare organizations manage a large volume of electronic medical records created by their employees and have access to sensitive and important patient information, making it critical to throw light on healthcare staff (Kaplan, 2016; Rahim et al., 2017). The three most distinguish concept in healthcare setting to protect the healthcare information is privacy, confidentiality, and security (Thomas Rindfleisch, 1997).Privacy protection not merely depends on deidentification and anonymization, but on the transparency of how actually data is utilized (Kaplan, 2016). According to Rahim et al., (2017), Support from top management may lead to educating their employees about the importance of privacy and can be done by creating a personalized and classified privacy policy that outlines the methods for implementing adequate privacy controls to mitigate potential risks. Electronic health records (EHR) and health data networks provides a wealth of public data. Data can be used for variety of objectives, ranging from comparative research to design clinical trial and various monitoring purpose (Kaplan, 2016).

Although many researchers have investigated the deployment of blockchain technology and AI in dealing with the COVID-19 crisis (Nguyen et al., 2021). These studies largely concentrated on the deployment of blockchain for the storage of data, data management, and privacy, healthcare staff reported a significant degree of concern about privacy and security, and protecting healthcare professionals is a critical principle when dealing with pandemics such as COVID-19. Examining how healthcare staff handles privacy and security concerns during a pandemic is critical for improving healthcare organizations' capacity to continue dealing with emergencies (Dopelt et al., 2021; Mabrouk et al., 2016; Parks et al., 2011). Healthcare professionals will require training on how to use digital platforms. There are huge challenges to overcome to continue using this digital base healthcare platform and training is one of the keys to achieving the objective (Bouabida et al., 2022).In the healthcare setting, effective training and education about privacy can help healthcare professional users to have a better understanding of information privacy concerns (IPC) and to acquire better judgment, preventing privacy violations (Rahim et al., 2017). Businesses are putting a lot of effort into building privacy policies and measures to combat these threats of security concerns (Meingast et al., 2006; Parks et al., 2011; Thomas Rindfleisch, 1997). Prior to the deployment of digital technologies in the healthcare system, healthcare professionals should have sound knowledge of these technologies. Many professionals proclaimed positive experiences in online consultations, but online consultations performance in terms of relational aspects and in relation to privacy and security of software was found to be key impediments to deployment (De Witte et al., 2021; Lenert & McSwain, 2020). Doctors have always valued their privacy, before the advent of technology in the medical industry (Alhasan et al., 2020). According to Earp & Payton (2006), a Substantiated amount of awareness of privacy orientations among healthcare employees plays a significant role. Wilkowska & Ziefle (2011) investigates the perceived importance of security and privacy concerns in separate groups and evaluates the predictive value of these features on medical technologies and E-health technologies

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/privacy-and-security-concerns-during-the-covid-19-pandemic/312423

Related Content

Human Factors in Cybersecurity: Issues and Challenges in Big Data
Xichen Zhangand Ali A. Ghorbani (2021). *Research Anthology on Privatizing and Securing Data (pp. 1695-1725).*
www.irma-international.org/chapter/human-factors-in-cybersecurity/280252

A Simulation Model of Information Systems Security
Norman Pendegraftand Mark Rounds (2007). *International Journal of Information Security and Privacy (pp. 62-74).*
www.irma-international.org/article/simulation-model-information-systems-security/2471

Information Security Risk Analysis: A Pedagogic Model Based on a Teaching Hospital
Sanjay Goeland Damira Pon (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 2849-2864).*
www.irma-international.org/chapter/information-security-risk-analysis/23260

Automated Ruleset Generation for “HTTPS Everywhere”: Challenges, Implementation, and Insights
Fares Alharbi, Gautam Siddharth Kashyapand Budoor Ahmad Allehyani (2024). *International Journal of Information Security and Privacy (pp. 1-14).*
www.irma-international.org/article/automated-ruleset-generation-for-https-everywhere/347330

Addresses the Security Issues and Safety in Cyber-Physical Systems of Drones
Areeba Laraib, Areesha Sialand Raja Majid Ali Ujjan (2024). *Cybersecurity Issues and Challenges in the Drone Industry (pp. 381-404).*
www.irma-international.org/chapter/addresses-the-security-issues-and-safety-in-cyber-physical-systems-of-drones/340085