COVID-19's Healthcare Economic Struggles: A Looming Crisis in Hospitals with Growing Online Crime Threats

Fredrick Ochieng' Omogah*

Uzima University, Kenya

Abstract

Background: The coronavirus disease (COVID-19) pandemic has led to unprecedented challenges in healthcare systems worldwide, leading to significant economic strain and a surge in technological reliance. This heightened dependence on technology, including Internet of Things (IoT) medical devices, has introduced new risks, particularly regarding cyber threats that can disrupt healthcare services and present clinical challenges. Hospital management became more critical and sensitive in the face of the highly infectious nature of COVID-19. This study explored the intersection of healthcare, technology, and cybersecurity during the pandemic.

Methods: Using a cross-sectional study design, surveys were distributed to 20 healthcare workers, and international news media reports were analyzed to gather insights into the challenges faced by hospitals during the COVID-19 pandemic.

Results: The results highlight the economic challenges faced by the healthcare sector during the pandemic and subsequent surge in technological adoption. Significant cyber risks are associated with the use of technology, particularly IoT devices. Hospitals have emerged as prime targets for cybercriminal activities during the pandemic, posing a threat to health care interventions.

Conclusion: The COVID-19 pandemic has accelerated technological integration into healthcare, presenting both opportunities and challenges. Recommendations for improved hospital management and future pandemic preparedness include implementing robust cybersecurity measures, diversifying technological solutions, and fostering awareness among health care professionals.

Keywords: COVID-19 pandemic, Healthcare Management Challenges, Electronic Healthcare Systems, Cyber Security, IoT Medical devices

Introduction

The global impact of the COVID-19 pandemic has been devastating, with the virus rapidly spreading across various geographical locations between late 2019 and early 2020 and originating in Wuhan, China (Liu et al., 2021). On March 11, 2020, the World Health Organization (WHO) officially declared COVID-19 caused by SARS-CoV-2 as a global pandemic (Dhama et al., 2020). In response to the containment measures recommended by the WHO, there has been a significant increase in technology reliance on business continuity worldwide (Donthu & Gustafsson, 2020). However, this reliance introduced a new risk, as cyber attackers could exploit the

 *Corresponding Author: fomogah@gmail.com

situation, especially with the widespread use of connected Electronic Healthcare Systems for patient management and disease control in hospitals (Williams & Woodward, 2015).

Research indicates that the health sector experienced several data breaches in the first half of 2016, making it a leading target for such incidents (Seh et al., 2020). The value of health data has grown, making it an attractive target for various motives, including financial gain, malicious activities, notoriety, and curiosity, among others. This interference disrupts critical healthcare service delivery activities. Given the manifold ripple effects of COVID-19 on health care, online attackers might exploit disparities in health facilities, leading to significant disruptions (Earle, 2020). Currently, challenges persist in managing health facilities, posing potential yet unknown clinical dangers owing to evolving cyber and electronic threats (Haghani et al., 2020).

COVID-19 Impact on Global Economy and Related Online Threats

The far-reaching impact of the COVID-19 pandemic has resounded globally, sending shockwaves into every corner of the world. As of mid-2020, the global economy has been in a state of vulnerability. Control Risks' team of cybersecurity experts issued timely warnings about the emergence of cyber threats linked to COVID-19 as early as January 2020. During this period, alarming cyber-attack incidents were reported, targeting individuals attempting to escape the outbreak epicenter in Wuhan, China. These attacks sparked apprehension regarding the continued spread of COVID-19 and its influence on a global scale.

The targets of these attacks were not limited to one region; they affected organizations and individuals in various countries, including Japan, the United States, Italy, and numerous European, American, and Southeast Asian nations. Cybercriminals capitalized on the COVID-19 crisis, leveraging their increased reliance on Information and Communication Technology (ICT) equipment to ensure business continuity. This reliance stemmed from the measures the World Health Organization (WHO) implemented to contain the pandemic's escalation. Of particular concern was the potential vulnerability of Hospital's Electronic Healthcare Systems (EHCS) to such attacks, adding a layer of complexity to an already dire situation (Control Risks, 2020). Lately, online threats have been intensified by the growth of mobile or portable devices and the presence of interconnected IoT medical devices in cyberspace (Buhari & Isa, 2023).

Challenges in sub-Saharan African Countries

Devastating reports on COVID-19 and the shift in business operations due to disruptions has been an uphill task for sub-Saharan African countries. This has resulted in numerous humanitarian and healthcare-related effects. This was not the case in struggling African economies. The

bottom line shows that the ripple effects were adverse because even the attention in healthcare shifted to COVID-19 cases with a focus on technology, leaving other medical conditions unattended. The spontaneous outbreak and geographical spread had multiple implications: raging fear, panic, and confusion; and emotional feelings such as anger, loss of control, and defenselessness, which led to high mortality rates (Omogah, 2020).

Challenges Facing Healthcare Services in Kenya

The Kenyan Constitution of 2010 introduced the concept of devolved governance in the country, establishing forty-seven (47) county governments that are separate from the national government. Various critical government functions, including healthcare services, have been devoted to these counties. In Kenya, the responsibilities of county governments in healthcare services include the governance of hospitals, allied facilities, and services, as well as the promotion of primary healthcare, licensing, and employment of healthcare workers, among other duties. Devolving healthcare services without clear policies and adequate funding is a significant oversight. The provision of high-quality healthcare services to citizens is of paramount importance in any nation. Even before the emergence of the devastating COVID-19 pandemic, devolved healthcare services in Kenya struggled and fell short of the standards expected by citizens at the county level.

Consequently, the challenges in delivering healthcare services during the COVID-19 pandemic exacerbated. Securing the resources necessary to manage the COVID-19 pandemic posed a considerable challenge to county governments. The devolved governance system in Kenya has significantly impacted healthcare services (Kenyan Constitution, 2010).

Impact of COVID-19 on Kenyan Health Sector

In 2020, the Journal of Global Health noted a lack of commitment and policy interventions by governments, including Kenya, in managing COVID-19 treatment costs. Additionally, clear strategies are absent to support vulnerable citizens, particularly low-income earners, in covering these expenses (Chersich et al., 2020). This highlights the need for governments to allocate resources and create comprehensive policies to address these challenges, ensuring equitable access to COVID-19 treatment and financial support for those in need.

Lack of Personal Protective Equipment (PPEs). In Kenya and other developing nations, the accessibility of healthcare facilities and crucial Personal Protective Equipment (PPEs) are frequently considered a luxury in the fight to ensure safety and an efficient response to the deadly COVID-19 (Kazungu et al., 2021). Consequently, healthcare providers face substantial risk of infection (Silva et al., 2020). This highlights the challenges healthcare workers face in resource-constrained settings, where the scarcity of essential protective gear can put their well-being at risk. A lack

of PPEs is a health risk for healthcare workers. This would put them in a panic mode of contracting the disease. Online criminals could use the situation to invade the systems for financial gain.

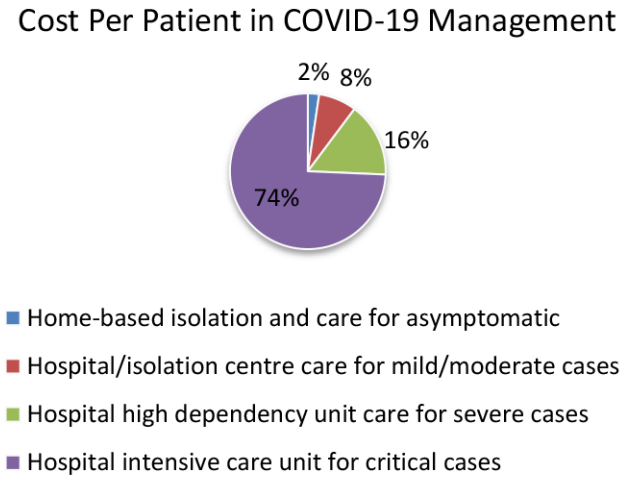
Healthcare Financing Challenge. In Kenya, the National Health Insurance Fund (NHIF) has not yet expanded its coverage to include COVID-19 cases in healthcare facilities. Consequently, individuals affected by the virus often find themselves responsible for financing their own treatment or depending on the support of well-wishers and family members. Private healthcare facilities have introduced their own unregulated fee schedules, leading to excessively high costs for COVID-19 patients. In turn, this has contributed to a notable increase in the region's mortality rate (Ouma et al., 2020). This situation underscores the urgent need for comprehensive healthcare coverage and affordable treatment options to address the challenges presented by the pandemic.

General Costs of Running Hospitals during the COVID-19 Pandemic

According to Barasa et al. (2021), the unit cost of COVID-19 case management in Kenya per day per patient for asymptomatic and mild-to-moderate cases receiving home-based care is Ksh. 1,993.01, which is equivalent to US$18.89, and Ksh. 1,995.17, equivalent to US$18.991. For more severe and critical cases, the management of patients with underlying conditions involves admission to referral hospitals and isolation centers where critical oxygen and ICU care are provided at the cost of Ksh. 13,137.07, equivalent to US$124.53, and Ksh. 63,243.11, which is equivalent to US$599.51 per patient per day.

Figure 1

Cost Per Patient in COVID-19 Management



Note: Author's Interpretation from BMJ Global Health data, 2021

Based on these cost estimates, running hospitals during the COVID-19 pandemic became daunting, with expenses exceeding double what they were before the pandemic (Horowitz, 2022). It is worth noting that these financial burdens create incentives for potential online criminal activity, as attackers might see hospitals as lucrative targets given the significant financial transactions involved in managing COVID-19 patients (Bansal et al., 2020). Figure 1 illustrates the economic challenges of managing COVID-19 patients in both referral hospitals and at home.

Online Threats to Healthcare Information

In a hospital environment, online attacks can originate from insider and outsider threats, constituting unauthorized access or interference with patient or healthcare personnel data as well as compromising the operation of computer systems or healthcare programs. Such interference may involve the permanent or temporary deletion of data or computer programs. Specific threats and attacks encompass the Distributed Denial of Service (DDOS) attack on Electronic Healthcare Systems (EHCS), which could result in the critical issue of patient information becoming entirely unavailable when urgently required for healthcare service delivery. A Distributed Denial of Service (DDOS) incident occurs when a healthcare facility's electronic healthcare network infrastructure is inundated with spoofed packets from unknown sources, carrying malicious spyware that gets installed on computer systems (Omogah, 2020).

Additional threats include modification attacks, which can alter data or programs, and malicious codes such as viruses attached to emails or websites. The Interception attack involves infiltrating electronic healthcare system (EHCS) networks to intercept and capture access control details of healthcare personnel, including passwords and other sensitive information required for launching attacks on hospital databases. Fabrication attacks are related to Denial of Service (DOS) attacks and encompass falsifying addresses to send emails from fabricated users. A Botnet Attack pertains to compromised computers connected to the Internet, remotely monitored and controlled by a "bot master" to carry out distributed threats and attacks. There are also common threats and attacks, such as Social Engineering and Ransomware attacks.

Freshly Emerging Technology in the Healthcare Domain

Contemporary healthcare systems worldwide have witnessed the emergence of new Information and Communication Technology (ICT) trends, particularly in the context of healthcare intervention measures. Recent efforts to combat COVID-19 have amplified the significance of this trend (Sparrow et al., 2020). However, various studies continue to underscore the healthcare sector's relative lag in implementing robust data security measures and enhancing workforce capacity compared to other industries.

Argaw et al. (2019) indicate that the healthcare sector has swiftly become a prime target for cyber-attacks. As critical and highly sensitive facilities, hospitals are acutely vulnerable to disruptions and security breaches due to the potential risks they entail. Currently, healthcare facilities are extensively equipped with interconnected IoT medical devices to exchange vital patient information (Argaw et al., 2019). While facilitating patient care, these devices also present a potential vulnerability, rendering them susceptible to exploitation by online criminals seeking to harm patients during a pandemic. The absence of comprehensive knowledge and secure management practices concerning IoT medical devices remains a glaring vulnerability that malicious actors can exploit for personal gain (Kalamkar & Prasad, 2023).

Change in Patient Management as a Challenge

Managing patients during the COVID-19 pandemic has presented many daunting challenges and complexities (Cohen et al., 2020). These challenges are inherently linked to the unique characteristics of the virus, including its mode of transmission, infectiousness, and severity (Shanthanna et al., 2020). Notably, a critical scenario has unfolded, mandating the isolation of COVID-19 patients from those without the virus to curtail its spread. This has greatly strained healthcare facilities and their available resources (Stawicki et al., 2020).

The most severe outcomes were observed when the resources of referral hospitals became stretched to their limits, leading to the continued presence of the virus within the hospital environment alongside other patients. What further exacerbated the situation was fear among frontline healthcare workers potentially carrying the virus home, contributing to an environment of discrimination. This overwhelming scenario within the healthcare system has regrettably led to a diminished level of attention and care provided to patients with other serious illnesses, such as Diabetes, Cancer, and HIV, as the focus shifted towards the management of COVID-19, among others.

COVID-19 Billionaires Versus Donor Fatigue

One of the major corruption scandals that has plagued many African countries during the COVID-19 pandemic revolves around the misappropriation of donor funds, which were intended to mitigate the impact of the COVID-19 crisis. This mismanagement involved prominent politicians and key officials from the healthcare ministry (Badu et al., 2020). Notably, in Kenya, an estimated 8 billion Ksh was misappropriated by the Kenya Medical Supplies Authority (KEMSA), and to date, the so-called "COVID-19 billionaires" are yet to be held accountable for their actions (Ochieng' & Odhiambo, 2022).

This unfortunate situation has given rise to donor fatigue, as well-wishers and development partners have been disheartened by the misuse of hard-earned funds, resulting in a lack of recognition of

their contributions. When these donors are approached for future assistance without prior accountability, they may become disheartened, feeling that their efforts are not truly making a difference. Ultimately, vulnerable members of society suffer the consequences of decreased donor support (Duwa, 2021).

Methodology

A cross-sectional research design was employed, involving the administration of a survey from 20 randomly selected healthcare workers: four (4) medical officers, eight (8) nurses, four (4) clinicians, two (2) health record officers, and two (2) health facility administrators. Other data were gathered from multiple sources, including online bulletin news from four (4) major international news media houses, two (2) local print media, and other relevant reports addressing the challenges of hospital management during the COVID-19 pandemic. This data collection spanned early to mid-year 2020, coinciding with the spontaneous outbreak and spread of the COVID-19 pandemic, which was associated with emerging cyber threats targeting hospitals (Huang et al., 2020).

The study focused on several key dimensions, including healthcare workforce capacities, strain on infrastructure capacities, cost of healthcare financing for COVID-19 patients, technology adoption in the healthcare sector, and emerging cyber threats (Haldane et al., 2021). These threats could significantly affect the clinical management of patients, posing a looming danger to all categories of hospital patients during the pandemic.

Results

Data Presentation and Analysis

Table 1 and Figure 2 represent a survey assessment of gathered information from healthcare workers, online bulletin news, local print media, and other related reports about challenges in managing hospitals during the COVID-19 pandemic in western Kenya between January and June 2020 (Afriyie et al., 2020).

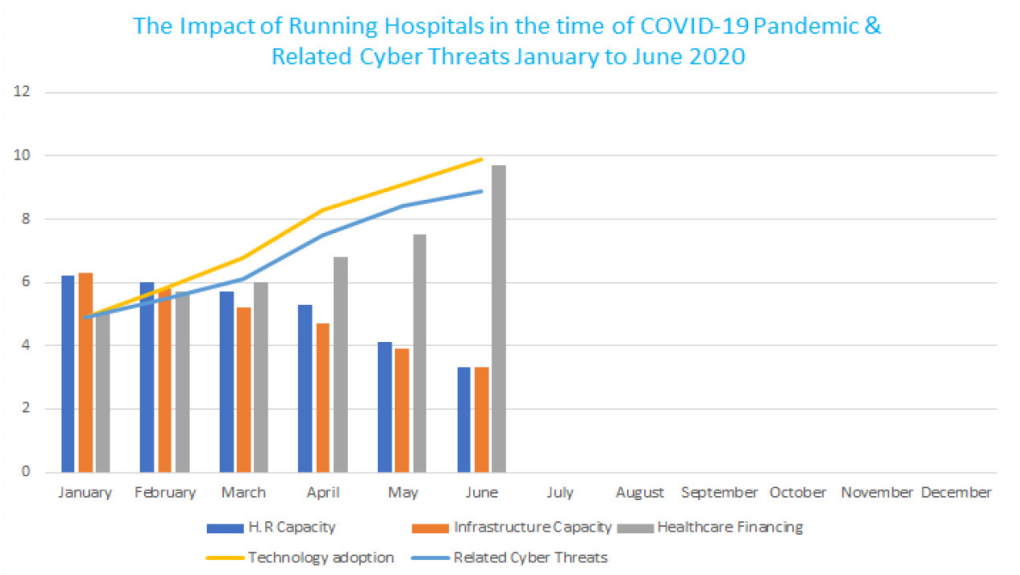
Table 1

Discoverable Data on a Score Scale between 0-10 on Healthcare Workers' Capacities, Healthcare Infrastructure Capacities, Cost of Financing COVID-19 Patients, Technology Adoption and the Emerging COVID-19-Related Cyber Threats from January – June 2020

Year 2020	H.Resource Capacity	Infrastructure Capacity	Healthcare Financing	Technology adoption	Related Cyber Threats
January	6.2	6.3	5.1	4.9	4.9
February	6	5.8	5.7	5.8	5.5
March	5.7	5.2	6	6.8	6.1
April	5.3	4.7	6.8	8.3	7.5
May	4.1	3.9	7.5	9.1	8.4
June	3.3	3.3	9.7	9.9	8.9

Figure 2

Impact of Running Hospitals during the COVID-19 Pandemic from January June 2020



The analyzed data reveals that healthcare workers' capacity decreased steadily from January to June 2020, while healthcare infrastructure capacity has been overstretched because more patients were flocking into hospitals with COVID-19-related cases, which required space, special beds, oxygen and ICU care for proper admissions (Mulholland et al., 2020)

Healthcare financing became a challenge because of the high costs of COVID-19 patient management due to insufficient oxygen and personal protective equipment (PPEs) in many facilities (Oladino et al., 2020). The technology adoption in many healthcare facilities went up from January to June 2020, following WHO containment measures, which led to over-reliance on Technology use for business continuity in the healthcare sector (Salvador et al., 2020)

Ideally, COVID-19 could only be managed using technology, such as ventilators in ICU care and many other connected Internet of Things (IoT) equipment (Chamola et al., 2020). Finally, the analyzed data cite the outbreak of the COVID-19 pandemic, instigating potential electronically perpetuated online criminal conduct. These are threats targeting hospitals that would have far-reaching consequences for patients during the COVID-19 pandemic (Joshpe, 2020).

Discussion

Addressing the increasing use of portable and mobile devices in healthcare facilities is crucial because their proliferation raises concerns about vulnerabilities and security incidents that can compromise patient information within Electronic Healthcare Systems. Furthermore, the growth of mobile devices has amplified online threats, necessitating the development and implementation of a robust mobile device policy. Healthcare stakeholders should prioritize governance and strategic planning for mobile device policies in healthcare facilities. Regular reviews and updates are essential to ensure that these policies align with the requirements of patient data security and procedures for handling patient data.

Engaging healthcare providers in understanding the system is essential to mitigate these challenges. Organizing scheduled training and awareness activities for healthcare workers can help address electronic healthcare issues, particularly access control measures that might otherwise impose constraints owing to the high workload in healthcare facilities. Prioritizing focus by providing the necessary resources to establish healthcare cyber laws is crucial in the effective fight against cyber threats, making potential perpetrators more cautious.

One of the primary motivations for online criminal activity is financial gain, and the healthcare sector, especially during events such as the COVID-19 pandemic, has been a prime target. Hospitals, related health facilities, and banks are often targeted by online payment gateways that connect them. These gateways authenticate and verify payment details and process orders according to hospital bill payer instructions from merchant websites. Security becomes a major concern during such pandemics, with attackers potentially deploying malicious code to trace hospital bill transaction activities and alter details through attacks like "Man in the Browser" (MitB) exploits. An advanced technique called "Double Verification" should be employed to detect such attacks when paying hospital bills during pandemics.

Healthcare services play a critical role on a global scale, and achieving economic stability in any nation necessitates treating them as essential and affording them the respect they deserve. This can only be accomplished through a comprehensive policy framework and sufficient funding resources to ensure efficient management of healthcare services.

Conclusion

In conclusion, hospitals play an indispensable role in healthcare fraternities. The COVID-19 pandemic has brought about a multitude of vulnerabilities within healthcare systems, which have had far-reaching consequences. They have placed immense pressure on already overwhelmed healthcare staff, stretched healthcare infrastructure to its limits, incurred very high costs in patient management, and exposed healthcare facilities to a range of cyber and electronic threats, primarily

owing to the adoption and overreliance on technologies (Rice & Williams, 2022).

This overreliance on technology is necessary for business continuity plans for healthcare interventions and service delivery (Connell, 2006). However, it also catalyzed exploitation by COVID-19-related cybercriminals, posing significant threats and potential for full-blown tragedies within our hospitals.

Additionally, the COVID-19 pandemic has revealed a troubling aspect of corruption in some African countries, misappropriating donor funds to combat the pandemic. The involvement of prominent politicians and healthcare ministry officials in these scandals has eroded trust. This has resulted in what is known as "donor fatigue," where well-wishers and development partners are disheartened by misusing their hard-earned funds, leading to a lack of recognition of their contributions. This fatigue could lead to reduced future donor support, ultimately affecting vulnerable members of society who rely on this assistance (Duwa, 2021).

In light of these challenges, healthcare institutions must balance embracing technology for efficiency with being vigilant in securing patient data and resources. This balance is crucial to ensure the resilience of healthcare systems and the well-being of patients, especially during crises such as the COVID-19 pandemic.

Recommendations

To enhance healthcare cybersecurity and safeguard patient information, a comprehensive strategy is recommended. Firstly, establishing and enforcing Mobile Device Policy Standards within the Health Insurance Policy and Accountability Act (HIPAA) will protect patient rights and minimize vulnerabilities. Secondly, prioritizing resources for developing healthcare cyber laws is crucial to combat online threats targeting hospitals. Thirdly, implementing Double Verification for Online Payments in medical billing transactions adds an extra layer of authentication, promoting secure financial transactions between healthcare institutions and banks.

Creating a legal framework for legislation, law enforcement, and jurisdiction is imperative for punishing cybercrime perpetrators. Awareness and training programs on the importance of patient information and electronic healthcare systems should be conducted to address the challenges posed by healthcare workers. Globally, there is a need for an age-cutting policy to bolster Cybersecurity in healthcare, particularly during pandemics like COVID-19. Lastly, while devolving healthcare services to counties is essential, it should be accompanied by adequate funding from national governments to ensure effective implementation. Alternatively, centralizing healthcare functions under the national government can promote standardized policies and efficient healthcare management nationwide.

References

Afriyie, D. K., Asare, G. A., Amponsah, S. K., & Godman, B. (2020). COVID-19 pandemic in resource-poor countries: challenges, experiences and opportunities in Ghana. *The Journal of Infection in Developing Countries*, 14(08), 838-843.

Argaw, S. T., Bempong, N. E., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyber-attacks against hospitals and available best practice recommendations: a scoping review. *BMC Medical Informatics and Decision Making,* 19(1), 1-11.

Badu, K., Thorn, J. P., Goonoo, N., Dukhi, N., Fagbamigbe, A. F., Kulohoma, B. W., & Gitaka, J. (2020). Africa's response to the COVID-19 pandemic: A review of the nature of the virus, impacts, and implications for preparedness [version 1; peer review: 2 approved with reservations].

Badu K, Thorn JPR, Goonoo N et al. Africa's response to the COVID-19 pandemic: A review of the nature of the virus, impacts and implications for preparedness [version 1; peer review: 2 approved with reservations]. *AAS Open Res 2020*, 3:19 (https://doi.org/10.12688/aasopenres.13060.1)

Bansal, P., Bingemann, T. A., Greenhawt, M., Mosnaim, G., Nanda, A., Oppenheimer, J., & Shaker, M. (2020). Clinician wellness during the COVID-19 pandemic: extraordinary times and unusual challenges for the allergist/immunologist. *The Journal of Allergy and Clinical Immunology: in Practice*, 8(6), 1781-1790.

Barasa, E., Kairu, A., Maritim, M., Were, V., Akech, S., & Mwangangi, M. (2021). Examining unit costs for COVID-19 case management in Kenya. *BMJ Global Health*, 6(4), e004159.

Buhari, A., & Isa, Z. (2023). Social media and cyber security: protecting against online threats and attacks. https://www.researchgate.net/publication/373328868_social_media_and_cyber_security_protecting_against_online_threats_and_attacks

Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. *IEEE Access*, 8, 90225-90265.

Chersich, M. F., Gray, G., Fairlie, L., Eichbaum, Q., Mayhew, S., Allwood, B., ... & Rees, H. (2020). COVID-19 in Africa: care and protection for frontline healthcare workers. *Globalization and Health*, 16, 1-6.

Cohen, S. P., Baber, Z. B., Buvanendran, A., McLean, B. C., Chen, Y., Hooten, W. M., ... & Phillips, C. R. (2020). Pain management best practices from multispecialty organizations during the COVID-19 pandemic and public health crises. *Pain Medicine*, 21(7), 1331-1346.

Connell, J. (2006). Medical tourism: Sea, sun, sand and… surgery.

Tourism Management, 27(6), 1093-1100.

Control Risks. (2020, March 23). COVID-19 Impact on global economy and related online threats. Retrieved from https://www.controlrisks.com/our-thinking/insights/covid-19-and-remote-working

Dhama, K., Khan, S., Tiwari, R., Sircar, S., Bhat, S., Malik, Y. S., & Rodriguez-Morales, A. J. (2020). Coronavirus disease 2019–COVID-19. *Clinical Microbiology Reviews*, 33(4), e00028-20.

Donthu, N., & Gustafsson, A. (2020). Effects of COVID-19 on business and research. *Journal of Business Research*, 117, 284-289.

Duwa, M. R. (2021). COVID-19 Crisis Management: A Content Analysis of the Kenyan Governmental Communication Strategies. (Dissertation, North Carolina State University).

Earle, P. C. (Ed.). (2020). Coronavirus and disease modeling. American Institute for Economic Research.

Haghani, M., Bliemer, M. C., Goerlandt, F., & Li, J. (2020). The scientific literature on Coronaviruses, COVID-19, and its associated safety-related research dimensions: A scientometric analysis and scoping review. *Safety Science,* 129, 104806.

Haldane, V., De Foo, C., Abdalla, S. M., Jung, A. S., Tan, M., Wu, S., & Legido-Quigley, H. (2021). Health systems resilience in managing the COVID-19 pandemic: lessons from 28 countries. *Nature Medicine*, 27(6), 964-980.

Horowitz, D. (2022). American dreams, American nightmares: Culture and crisis in residential real estate from the great recession to the COVID-19 pandemic. UNC Press Books.

Huang, Y., & Zhao, N. (2020). Generalized anxiety disorder, depressive symptoms, and sleep quality during the COVID-19 outbreak in China: a web-based cross-sectional survey. *Psychiatry Research*, 288, 112954.

Ibeh, I. N., Enitan, S. S., Akele, R. Y., Isitua, C. C., & Omorodion, F. (2020). Global impacts and Nigeria responsiveness to the COVID-19 pandemic. *International Journal of Healthcare and Medical Sciences*, 6(4), 27-45.

Joshpe, B. (2020). Considering Domestic and International Frameworks for Analyzing China's Potential Legal Liability in the Aftermath of COVID-19. Available at SSRN 3598614.

Kalamkar, M. D., & Prasad, R. (2023). Impact of the COVID-19 pandemic on cyber security issues in the healthcare domain: A Scoping Review. *Cyber Security Threats and Challenges Facing Human Life*, 24-41.

Kazungu, J., Munge, K., Werner, K., Risko, N., Vecino-Ortiz, A. I., & Were, V. (2021). Examining the cost-effectiveness of personal protective equipment for formal healthcare workers in Kenya during the COVID-19 pandemic. BMC

health services research, 21(1), 992. https://doi.org/10.1186/s12913-021-07015-w

Kenyan Constitution. (2010). Devolved Governance and Healthcare Services in Kenya. http://www.parliament.go.ke/sites/default/files/2023-03/The_Constitution_of_Kenya_2010.pdf

Liu, A., Kim, Y. R., & O'Connell, J. F. (2021). COVID-19 and the aviation industry: The interrelationship between the spread of the COVID-19 pandemic and the frequency of flights on the EU market. *Annals of Tourism Research*, 91, 103298.

Mulholland, R. H., Wood, R., Stagg, H. R., Fischbacher, C., Villacampa, J., Simpson, C. R., ... & Sheikh, A. (2020). Impact of COVID-19 on accident and emergency attendances and emergency and planned hospital admissions in Scotland: an interrupted time-series analysis. *Journal of the Royal Society of Medicine,* 113(11), 444-453.

Ochieng'-Springer, S., & Odhiambo, H. (2022). Governance during COVID-19: Kenya's graft practices. *The Round Table*, 111(4), 489-505.

Omogah, F. (2020). The Embryonic Covid-19 themed cyber threats: A looming tragedy to already vulnerable global electronic healthcare systems (GEHCS)! EHealth 2020, e-Health and Alternative Healthcare Innovations. Webinar, October 12-13, 2020.

Omogah, F. (2020). Online Threats in Hospital Environments: Unauthorized Access, Data Interference, and the Distributed Denial of Service (DDOS) Attack on Electronic Healthcare Systems.

Ouma, P. N., Masai, A. N., & Nyadera, I. N. (2020). Health coverage and what Kenya can learn from the COVID-19 pandemic. Journal of global health, 10(2), 020362. https://doi.org/10.7189/jogh.10.020362

Rice, S., & Williams, M. (2022). Vulnerabilities in healthcare systems: consequences of the covid-19 pandemic and the role of hospitals.

Salvador-Carulla, L., Rosenberg, S., Mendoza, J., Tabatabaei-Jafari, H., & Network, P. M. H. I. (2020). Rapid response to crisis: Health system lessons from the active period of COVID-19. *Health Policy and Technology*, 9(4), 578-586.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare (Basel, Switzerland)*, 8(2), 133. https://doi.org/10.3390/healthcare8020133

Shanthanna, H., Strand, N. H., Provenzano, D. A., Lobo, C. A., Eldabe, S., Bhatia, A., & Narouze, S. (2020). Caring for patients with pain during the COVID-19 pandemic: consensus recommendations from an international expert panel. *Anaesthesia*, 75(7), 935-944.

Silva, A. L. P., Prata, J. C., Walker, T. R., Campos, D., Duarte, A. C., Soares, A. M., ... & Rocha-Santos, T. (2020). Rethinking and optimizing plastic waste management under

COVID-19 pandemic: Policy solutions based on redesign and reduction of single-use plastics and personal protective equipment. *Science of the Total Environment*, 742, 140565.

Sparrow, R., Dartanto, T., & Hartwig, R. (2020). Indonesia under the new normal: Challenges and the way ahead. *Bulletin of Indonesian Economic Studies*, 56(3), 269-299.

Stawicki, S. P., Jeanmonod, R., Miller, A. C., Paladino, L., Gaieski, D. F., Yaffee, A. Q., De Wulf, A., Grover, J., Papadimos, T. J., Bloem, C., Galwankar, S. C., Chauhan, V., Firstenberg, M. S., Di Somma, S., Jeanmonod, D., Garg, S. M., Tucci, V., Anderson, H. L., Fatimah, L., Worlton, T. J., … Garg, M. (2020). The 2019-2020 Novel Coronavirus (Severe Acute Respiratory Syndrome Coronavirus 2) Pandemic: A Joint American College of Academic International Medicine-World Academic Council of Emergency Medicine Multidisciplinary COVID-19 Working Group Consensus Paper. *Journal of Global Infectious Diseases*, 12(2), 47–93. https://doi.org/10.4103/jgid.jgid_86_20

Walker, D. M., Yeager, V. A., Lawrence, J., & Mcalearney, A. S. (2021). Identifying opportunities to strengthen the public health informatics infrastructure: exploring Hospitals' Challenges with Data Exchange. *The Milbank Quarterly*, 99(2), 393-425.

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices (Auckland, N.Z.),* 8, 305–316. https://doi.org/10.2147/MDER.S50048

World Health Organization. (2003). Adherence to long-term therapies: evidence for action. World Health Organization.