Case study

DIGITAL HEALTH

DIGITAL HEALTH
Volume 9: 1–8

DOI: 10.1177/20552076231203937
journals.sagepub.com/home/dhj

Sage

Integrating digital solutions into national health data systems through public–private collaboration: An early experience of the SPICE platform in Kenya

Gladwell Gathecha[1], Oren Ombiro[2], Kelly Shelden[2], Anne Stake[2], Mary Murugami[2], Ezra Mungai[1], George Odhiambo[2], Ephantus Maree[1], Rajkumar Muthusamy[3], M Marimuthu[3], Duke Daniel[3], Eric Angula[2], Swathi Seshadri[4], Eric Nderitu[1], Elizabeth Onyango[1] and Joseph Sitienei[1]

Abstract

Public–private collaborative efforts to address healthcare challenges in low- and middle-income countries have been the focus of digital initiatives to improve both access and quality of health services. We report the early feasibility, experience, and learnings of migrating healthcare data generated from a proprietary, privately owned cloud-based environment into an on-premises National Health Data Center (NHDC) in compliance with Kenya's data management legislation. In 2018, Medtronic LABS entered into a partnership with the Kenya Ministry of Health and other stakeholders to improve access to quality services and data availability for non-communicable diseases (diabetes and hypertension), anchored on the SPICE digital health platform. Data migration from SPICE to the NHDC necessitated the establishment of multi-stakeholder coordination structures, alignment on system configuration requirements, provisioning of on-premises servers, data replication and monitoring. The data replication process showed consistency in format and content with no evidence of data loss. The monitoring of the server uptime and availability, however, exposed overall downtime of 15% of the total time tracked between April and December 2022 caused by Internet Protocol address configuration issues, power outages, firewall rule changes, and unscheduled system maintenance. Monthly tracked downtime however reduced from a high of 28% in April 2022 to 5% in December 2022. Our early experience shows that data migration from proprietary host environments to public "one-stop-shop" national data warehouses are feasible provided investments are made in the requisite infrastructure, software and human resource capacity to ensure long-term sustainability, maintenance, and scale to match cloud-based data hosting. Further, digital health solutions developed in collaboration with non-state actors can be integrated into national data systems, saving Governments the cost and efforts of building similar tools while leveraging private sector capacity.

Keywords

Digital health, health data migration, cloud repatriation, public–private collaboration, national health data systems

Submission date: 27 February 2023; Acceptance date: 9 September 2023

Introduction

Inadequate data on non-communicable diseases (NCDs) is a major obstacle to planning and tracking progress towards universal health coverage (UHC) and other global health and national targets.[1] Primary data were available for only 42% of NCD indicators in the UHC index in 2021, and substantially lower in low- and middle-income countries

[1]Ministry of Health, Nairobi, Kenya
[2]Medtronic LABS, Nairobi, Kenya
[3]Ideas2IT, Chennai, Tamil Nadu, India
[4]Medtronic, Inc, Minneapolis, MN, USA

Corresponding author:
Oren Ombiro, Medtronic LABS, Delta Corner Annex Building, 4th Floor, Nairobi, Kenya.
Email: oren.ombiro@medtroniclabs.org

(LMICs).[2] Data systems across LMICs are largely paper based, contributing to a heavy documentation burden on health workers and imposing a risk on the quality of the data. Digitization efforts have been useful in creating robust, efficient data systems towards improving the quality of care and patient outcomes.[3–6] In 2018, the Kenya Ministry of Health (MoH) entered into a partnership with Medtronic LABS and other stakeholders to improve access to quality NCD (hypertension and diabetes) services and enhance data availability and management through an end-to-end primary health care model developed using a human-centered design approach. The model is anchored on a digital health platform, SPICE, which facilitates community-based screening by trained and equipped community health volunteers/promoters, enabling electronic referral and linkage to care. SPICE also enhances quality of care by leveraging digital decision-support tools, risk-stratification algorithms, personalized care plans, remote monitoring, and patient education through tele-counselling and targeted Short Messaging Service (SMS). The platform provides custom dashboards for real-time tracking of both individual and aggregate patient data and generates customized MoH reports, which are then pushed into the country's DHIS2 platform, the Kenya Health Information System.[7] A 2018 study of the model at its pilot stage revealed positive outcomes in blood pressure control among hypertensive patients.[8]

The SPICE platform is made up of multiple products that are enabled through a core platform, which leverages a microservice-based architecture. It consists of four main products, SPICE, SPICE Insights, SPICE Engage, and SPICE Connect. The core product, SPICE, is an Android application, which runs on tablets and phones. SPICE communicates with the core platform through private, secure Rest Application Programming Interfaces (APIs). SPICE Insights and SPICE Engage are web-based applications that communicate using the SPICE APIs, which are built using Java. No data is stored on the mobile device for security reasons; cached data from off-line community screening or follow up is pushed immediately to the database once internet connectivity is achieved.

The Kenya MoH has recently established a National Health Data Center (NHDC) to ensure all patient-level data is centrally hosted to avoid fragmented storage in different locations and formats, which otherwise renders collation and analysis difficult, especially when such data is domiciled outside the country or is inaccessible to the MoH. The NDHC also provides the foundation for patient-centered care by warehousing the shared patient file that will be available across health facilities. The establishment of the NHDC is also to prompt visibility, access, ownership, and accountability for the MoH across all national health programs, in alignment with the provisions of the Health Act 2017[9] and the Data Protection Act, 2019.[10] To comply with this legislation there was a need to migrate the data generated by SPICE, which was initially hosted in the Amazon Cloud Service (AWS) to the NHDC to fully integrate into the mainstream health system, ensure sustainability and scale up the model. While this initiative sought to migrate data from a cloud-based environment to locally hosted servers, the greater majority of initiatives reported in literature tend to explore the migration of health data from local, on-premises data centers into public cloud computing environment.[11,12] The decision to embark on reverse cloud migration was informed by the country's change in the data protection legislative environment, which recommends health data be hosted locally unless under special circumstances.[10,13] The process of moving data off cloud-based environments back to a local data center is also referred to as reverse cloud migration or cloud repatriation.[14]

This shift is, however, not just unique to Kenya; there has been a policy shift across many emerging markets that militates in favor of data migration. The trend is largely being driven by data protection requirements, change in data stewardship conditions, and decentralization as data storage shifts toward federated rather than centralized cloud-based storage. Over half of African countries enacted various forms of data protection legislation over the past two decades, with many such laws requiring data localization.[15,16] This shift is arguably meant to promote data sovereignty and greater control over access and utilization, as well as data security against misuse and exploitation.[17,18] However, arguments against data localization, especially where the localization is in the form of on-premise hosting environments are emerging in the literature, including the costs of upfront infrastructure set-up and appropriate human resources, inefficiencies in data processing and management, and difficulties in ready access to the data.[17–19]

As the first health program in Kenya to migrate data from a proprietary, privately owned cloud hosting environment to the NHDC, we describe the feasibility, migration process, and learnings from our experience as our findings may be useful for other countries and stakeholders as governments seek to strengthen coordination, visibility, ownership, and protection of health data. Furthermore, our experience demonstrates the important contribution that collaborations with the non-state sector can have in supporting governments to achieve these aspirations.

Methods

Study design and setting

This study adopted a descriptive case study methodology to delve into the rationale, context, process, and lessons learnt from the data migration process. The study took place from November 2021 to December 2022 in Kenya and consisted of review of published literature and project documentation,

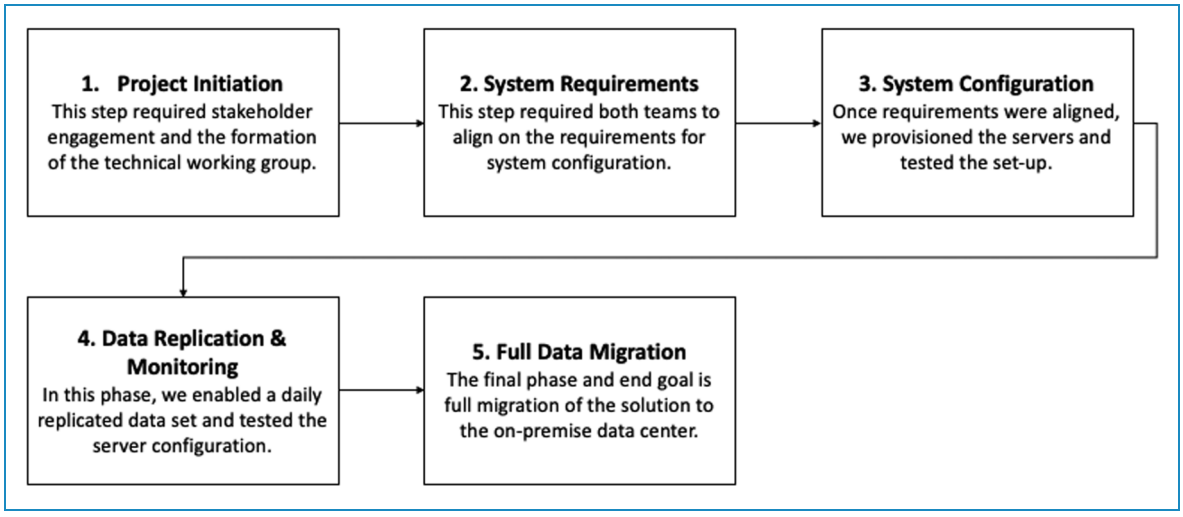

Figure 1. Data migration process. The above figure demonstrates the process that was followed to initiate and complete the data migration process.

data migration process mapping, server performance tracking, and stakeholder interviews.

Data migration process

A technical working group (TWG) was constituted in November 2021 consisting of representation from the MoH, Medtronic LABS, and Ideas2IT (software vendor partner) to operationalize the data migration. The TWG established bi-weekly meetings to facilitate close coordination, technical working sessions, and provide progress updates. Agreements were drafted to formalize the hosting relationship between the partners. This included a Service Level Agreement (SLA), which detailed the service, maintenance, and system uptime obligations that were agreed upon by all parties. A Data Access Agreement was also drafted to define the specific user roles and permissions for appropriate role-based access and security.

The main objectives of the TWG were to (a) align on system requirements, (b) provision and test the servers, and (c) enable full data replication and system monitoring. Figure 1 below highlights the key steps that were followed in the data migration process.

System requirements and architecture review. The TWG began with exchanging systems requirements and reviewing the platform architecture. They scoped the SPICE application data hosting requirements, such as server memory, core, disk memory, and operating system (OS) (see Table 1). The team then provisioned two servers to have a primary and backup server configuration. The TWG also established server maintenance, uptime, and support requirements to ensure optimal performance and responsiveness of the host system (NHDC). The need to have full time support and be able to run continuously without interruptions such as electricity or network failure was a key requirement of the servers.

Table 1. SPICE system server requirements.

Server requirement	Memory	Core	Disk memory	Preferrable OS
Database Server1 (primary)	8	4	100	Linux
Database Server1 (backup)	8	4	100	Linux

The team then analyzed potential options to facilitate SPICE data migration into the NHDC. The three options evaluated included: (a) local database with cloud app hosting, (b) local database with local app hosting, and (c) cloud database with cloud app hosting**.** The TWG opted for the first option to enable data to reside on-premises within the NHDC but maintain the application web services in the cloud-hosted environment. Following this decision, the TWG determined that the first phase would be to enact a fully replicated data set to the NHDC to enable system monitoring prior to full data migration.

Server set-up and system testing. A series of Internet Protocol (IP) addresses were whitelisted to enable remote access. Additionally, the Firewall settings were configured to support integrations with third-party systems to enable features such as SMS and e-mail. The NHDC also established a server maintenance and update plan, which provided policies for continuous backup operations, and

appropriate processes for data protection, disaster recovery, and failover procedures. The MoH NHDC Team provided all the server OS, Firewall and Network configuration related support.

Data replication and production-ready servers. Once the servers were provisioned and fully tested, they were production-ready to support data replication. The team began with data replication on 16 February 2022 to observe system performance and ensure application availability and server support met the defined requirements (i.e. Priority 1 tickets response within 1 hour: 99.5% server uptime). Replication involves writing or copying the same data to different locations. Instance Data Replication (IDR) copies data from one instance, called the producer instance (in this case Amazon Web Cloud Services where SPICE data was hosted), to one or more other instances called the consumer instances (the Kenya NHDC). IDR enables one to maintain consistent data across different organizations/host environments. The replication phase was also used to map out how long it would take to start coordinated data delivery, perform end-to-end tests, monitor system uptime and troubleshoot any connection errors to take corrective action. The server performance was tested by performing networking tests with different configurations (i.e. cloud/on-premises, on-premises/on-premises). The TWG continued to engage as a group to resolve issues and provide solutions to the challenges faced once the migration was live.

Ethical considerations. The SPICE Platform is certified by the Office of the Data Protection Commissioner as a Data Processor under certificate number 367-092D-2EC7 in line with Kenya's Data Protection Act, 2019.[10] The Data Migration process was commissioned and approved by the MoH on 11 November 2021. Given that this paper sought to only describe the process and learnings from the migration process rather than analyze individual-level data, ethical approval was not sought. Further, given that this study did not seek to interview patients or analyze individual-level data, patient consent for purposes of this study was not necessary. However, written informed consent is routinely collected from patients at the facility level before they are enrolled into the SPICE platform.

Findings and observations

The Kenyan data captured by SPICE has been successfully replicated to the NHDC and a daily data replication job ensures that the NHDC has all the latest application line lists. The NHDC system administrators have full read-write access to the database to directly query and access all the SPICE platform data. The SPICE platform has also been updated to include a data access portal, which facilitates real-time access to customized MoH reports, priority dashboards, and summarized data. The platform makes all data available to registered system users (health facility staff and health managers at all levels) in real-time and is also provided in a .csv format allowing further data analysis. Access rights are determined by the Data System Governance Framework published by the MoH in 2018.[20] Further, integration with DHIS2 has been achieved, into which all the relevant data elements are aggregated and pushed on a monthly basis.

The tracking of the data replication process so far shows consistency in format and content of data with no evidence of data loss. However, the cumulative proportion of downtime (defined as the server being unavailable) out of the total number of minutes tracked between 6 April and 31 December 2022 was 15% (see Table 2). Each system downtime was caused by a variety of factors such as IP address configuration issues, power outages, firewall rule changes, and unscheduled system maintenance. The server availability was monitored using Uptime Robot,[13] a service that enabled system monitoring through a constant ping that sent an internet control message protocol request to NHDC servers. Over time, the server uptime at the NHDC has been improving from 72% in April to 95% in December 2022.

Discussion

This case study outlines the practical steps that countries and non-state actors can use to successfully migrate data from private, proprietary systems to public-government-owned hosting environments. It demonstrates the need for close

Table 2. System uptime and downtime from 6 April to 31 December 2022.

Month	Uptime (minutes)	Downtime (minutes)	Uptime (%)	Downtime (%)
6 April from 04:39:31	25,670	10,050	71.86	28.14
May	37,414	7,226	83.81	16.19
June	33,549	9,651	77.66	22.34
July	37,413	7,227	83.81	16.19
August	39,539	5,101	88.57	11.43
September	32,293	10,907	74.75	25.25
October	43,651	989	97.78	2.22
November	38,076	5,124	88.14	11.86
December	42,307	2,333	94.77	5.23
Total	329,912	58,608	84.92	15.08

collaboration and multi-stakeholder engagement to leverage different capacities and expertise at varying touchpoints from development to data migration, system maintenance, and monitoring. In our experience, for this to be successful, there is the need to implement the migration using a phased approach and to support investments in strengthening the data center infrastructure. This ensures that system requirements are met and the migration to the locally hosted environment continues to perform and meet specifications for system availability, scalability, and reliability.

The downtimes observed showed that successful migration requires investment in the development of the core operating mechanisms of the local data center. Our learnings identified the following lessons learnt and focus areas for investment and capacity building (see Table 3) which are backed by other literature that propose various implementation models for data migration and data center strengthening.[21–24]

1. Leadership and governance structures

Strong leadership commitment from all parties plays a key role in providing direction and enables timely responses to issues as they arise. In this process, the governance structures between the parties resulted in the transparent sharing of ideas, strategies, implementation, and evaluation of the processes which drove mutual accountability in achieving the data migration milestones. An effective governance structure on a bedrock of trust among the stakeholders enhances a sustainable approach in driving the process through the various phases of implementation by ensuring a unified approach. Constant engagements through bi-weekly meetings provided the platform for timely response to any challenges encountered. The need for governance structures in the data and technology environment has been highlighted in other literature. For instance, Van Grembergen et al., in their technology governance publications posit that as technology evolves and becomes embedded in routine government operations and data management, and given the multiple stakeholders involved, establishment of robust governance structures, processes, and relational mechanisms is essential.[25,26]

2. Server availability, scalability, and performance

To ensure the data center is ready to support production-level systems, investments are needed to strengthen the data center infrastructure and system performance. The primary categories identified for infrastructure investment would be focused on power sources, networking, and monitoring to improve the system availability and enhance overall system performance. This is similar to the building blocks of data centers proposed by Patel and Shah, which include consistent power delivery; conditioning and backup; cooling systems; and network connectivity, fire protection, security and seismic safety.[23] Investing in redundant power sources will ensure the data center has a continuous power supply with sustained uptime.[27] Investing in improving the network speed and availability of internet will aid in system performance.[28,29] Lastly, investing in tools and technologies to monitor the servers (i.e. CPU monitoring, memory analysis, uptime/downtime alerting) will enable proactive responses to issues and provide alerts to partners.[30] Connectivity to data centers by electricity and internet services should always have redundant lines for continuous availability of services and any maintenance should be scheduled and agreed upon by all players.

3. Data center operating mechanisms and policies

The data center needs to invest in building and strengthening processes and operating mechanisms, similar to lessons documented from the Nordic societies data center industry development.[31] We recommend the data center to institute standard operating procedures and policies to clearly outline response times, server availability, and data access rights. Establishing strong documentation practices and processes will enable clear communication between parties (e.g. Firewall rules documented to allow for troubleshooting of system networking issues). Examples of policies and procedures to implement are disaster recovery plans,[32] server/system maintenance schedules, server configuration documents, and SLAs.

4. Data center security and privacy

To ensure that data stored at the data center is secure and meets all privacy regulations, the Center should implement security safeguards and engage security operations team members to monitor and safeguard the data. Examples of provisions include implementing access controls and ensuring safeguard mechanisms are implemented to ensure data privacy, for example, encrypting data at rest.[33,34] Cloud-based data centers provide a variety of security tools and controls (e.g. AWS Shield) out of the box[35]; on-premises data centers need to ensure the appropriate controls, monitors, and safeguards are implemented to build a secure, compliant data hosting environment.

To enable the realization of these priority investment areas, there is a need for additional domestic financing as well as development assistance to ensure readiness for full data repatriation. We also call for a hybrid model that allows data to be hosted locally while leveraging the advanced security, agility, and dynamic features of cloud-based services, where local laws allow.

Table 3. Key investment areas.

Thematic area	Key investment areas
Leadership and governance	1. Governance structures with representation from all parties and government at the forefront 2. Monitoring and accountability mechanisms to keep implementation on track
Server availability, scalability, and performance	1. Redundant power sources to ensure consistent availability of power supply 2. Optimize networking speed and availability of internet 3. Enhanced system performance (i.e. optimal server response time) 4. Ensure data center provides >99.5% system availability/uptime 5. Implement server CPU monitoring/memory analysis to enable scalability of servers. For instance, cloud-based host environments support auto-scalability; there is need to enable scalability of servers in the on-premises environment 6. Mechanisms to alert on downtime and enable identification of errors
Data center operating mechanisms and policies	1. Disaster recovery plans 2. Backup mechanisms to forestall the loss of data or disruption of essential services that rely on sustained uptime 3. Operating policies related to SLAs with partners 4. Documentation of system architecture (i.e. Firewall rules to allow for clear troubleshooting of system networking) 5. Server and system maintenance schedule to enable for planned system downtime
Data center security and privacy	1. Implement security safeguards and engage security operations team members to monitor and safeguard the data center 2. Implement access controls and safeguard mechanisms (i.e. encrypt data at rest) to ensure data privacy
Staff training and capacity building	1. Support capacity building and training programs that enhance developer skill sets in front-end/back-end development, full-stack, and database/system administration 2. Support staff to pursue certifications in server management and administration to strengthen knowledge of industry best practices

SLAs: service level agreements.

Limitations of the study

The study's focus is primarily on the initial phases of data migration, and the long-term impact of the migration process might not have been fully evaluated. Future studies should consider assessing the sustainability, scalability, and effectiveness of the data migration process over an extended period. The study's scope did not cover the cost implications of data migration. Future studies should consider analysis of financial resources required, including infrastructure investments, ongoing maintenance, and capacity building. Further, conducting a cost-benefit analysis of this kind of health data migration vis-à-vis cloud-based hosting may provide policy makers with much-needed evidence when considering such decisions.

Conclusion

Digital health solutions developed by non-state actors can be integrated into national data systems, saving governments the cost and efforts of building similar tools while leveraging private sector capacity. Data migration from proprietary systems to public "one-stop-shop" data warehouses is feasible if investments are made in the requisite infrastructure, software and human resource capacity to ensure long-term sustainability, maintenance and scale to match cloud-based data hosting.

Trade-offs to consider for data repatriation include the advantages of consolidating all the country's health data in one on-premise hosting environment to assure data security, privacy, sovereignty and ease of access vis-à-vis the capacity, additional infrastructure needs and consistent server availability to support prompt data transmission, especially where this is required for real-time clinical decision support. Careful planning, stakeholder engagement, and capacity building are essential to mitigate potential negative impacts and maximize the benefits of data repatriation from cloud to on-premise data hosting environments.

Acknowledgements: We would like to thank all the staff at the Kenya National Health Data Center, MOH Department of

Non-Communicable Diseases, Medtronic LABS technical team and Ideas2IT for their support during the entire process.

Contributorship: OO and GG researched the literature and conceived the study. OO, KS, and SS wrote the first draft of the manuscript. JS, AS, MM, and GO reviewed the manuscript and provided critical comments on its improvement. All authors reviewed and edited the manuscript and approved the final version of the manuscript.

Declaration of Conflicting Interests: OO, KS, AS, MM, GO, and EA are employees of Medtronic LABS; SS is an employee of Medtronic, Inc.

Ethical Approval: The SPICE Platform is certified by the Office of the Data Protection Commissioner as a Data Processor under certificate number 367-092D-2EC7 in line with Kenya's Data Protection Act, 2019.[10] The Data Migration process was commissioned and approved by the Ministry of Health on 11 November 2021. Given that this paper sought to only describe the process and learnings from the migration process rather than analyze individual-level data, ethical approval was not sought. Further, given that this study did not seek to interview patients or analyze individual-level data, patient consent for purposes of this study was not necessary. However, written informed consent is routinely collected from patients at facility level before they are enrolled into the SPICE platform.

Funding: This work was supported by Medtronic LABS.

Guarantor: Oren Ombiro.

ORCID iDs: Oren Ombiro https://orcid.org/0009-0003-4502-5877
Joseph Sitienei https://orcid.org/0000-0001-9140-4630

References

1. Gathecha G, Mwenda V, Mbau L, et al. Implementing a five year non-communicable disease strategic plan in Kenya: experience and lessons. *Public Health Research* 2022; 12: 14–23.
2. WHO. Tracking universal health coverage: global monitoring report, 2021, 2021.
3. Monaco A, Palmer K, Marengoni A, et al. Integrated care for the management of ageing-related non-communicable diseases: current gaps and future directions. *Aging Clin Exp Res* 2020; 32: 1353–1358.
4. Monaco A, Maggi S, De Cola P, et al. Information and communication technology for increasing healthy ageing in people with non-communicable diseases: identifying challenges and further areas for development. *Aging Clin Exp Res* 2019; 31: 1689–1693.
5. Monaco A, Palmer K, Holm Ravn Faber N, et al. Digital health tools for managing noncommunicable diseases during and after the COVID-19 pandemic: perspectives of patients and caregivers. *J Med Internet Res* 2021; 23: e25652.
6. Palmer K, Marengoni A, Forjaz MJ, et al. Multimorbidity care model: recommendations from the consensus meeting of the joint action on chronic diseases and promoting healthy ageing across the life cycle (JA-CHRODIS). *Health Policy (New York)* 2018; 122: 4–11.
7. Ministry of Health. Kenya health information system. KHIS, https://hiskenya.org/dhis-web-reporting/showDataSetReportForm.action (2022, accessed 25 November 2022).
8. Otieno HA, Miezah C, Yonga G, et al. Improved blood pressure control via a novel chronic disease management model of care in sub-Saharan Africa: real-world program implementation results. *J Clin Hypertens* 2021; 23: 785–792.
9. Government of Kenya. The Health Act, 2017.
10. Government of Kenya. The Data Protection Act, 2019.
11. Ansar M, Ashraf MW and Fatima M. Data migration in cloud: a systematic review. *Am Sci Res J Eng* 2018; 48: 73–89. http://asrjetsjournal.org/
12. Iqbal A and Colomo-Palacios R. Key opportunities and challenges of data migration in cloud: results from a multivocal literature review. In: *Procedia computer science*. 164. Sousse, Tunisia: Elsevier B.V., 2019, pp.48–55.
13. Government of Kenya. The Data Protection (General) Regulations, 2021.
14. Semilof M, Casey K, and Montgomery J. What is cloud migration? An introduction to moving to the cloud, https://www.techtarget.com/searchcloudcomputing/definition/cloud-migration (2021, accessed 21 August 2022).
15. Greenleaf G and Cottier B. Comparing African data privacy laws: international, African and regional commitments, https://au.int/memberstates (2020).
16. Greenleaf G and Cottier B. International and regional commitments in African data privacy laws: a comparative analysis. *Comput Law Secur Rev* 2022; 44: 105638.
17. Fredriksson T, Barayre C, Sinoncelli O, et al. Data protection regulations and international data flows: implications for trade and development, 2016.
18. Kijirah M and Thuo EW. Data protection and data localization in Kenya: potential economic impact and effect on Kenya's commitments in various regional treaty frameworks, 2021.
19. Drake WJ and Drake WJ. *Data localization and barriers to cross-border data flows: towards a multitrack approach*. Geneva: The World Economic Forum, January 2018, https://www.academia.edu/44491349/William_J_Drake_2018_Data_Localization_and_Barriers_to_Cross_Border_Data_Flows_Towards_a_Multitrack_Approach (2018, accessed 7 July 2023).
20. Ministry of Health Kenya. Data system governance and change management framework, 2018.
21. Vikas Pujara S and Pandit R. Automated approach for customized data migration. *Int J Eng Sci* 2015; 4(1): 258–260. http://www.ijesrt.com
22. Thalheim B and Wang Q. Data migration: a theoretical perspective. *Data Knowl Eng* 2013; 87: 260–278.
23. Patel CD and Shah AJ. Cost model for planning, development and operation of a data center, https://www.researchgate.net/publication/245808024 (2005).
24. Thalheim B and Wang Q. Towards a theory of refinement for data migration, 2011.

25. Van Grembergen W and De Haes S. *Implementing information technology governance*. IGI Global, 2008. DOI: 10.4018/978-1-59904-924-3.
26. Van Grembergen W, De Haes S and Guldentops E. Structures, processes and relational mechanisms for IT governance. In: *Strategies for information technology governance*. IGI Global, 2006. DOI: 10.4018/9781591401407.ch001.
27. Koot M and Wijnhoven F. Usage impact on data center electricity needs: a system dynamic forecasting model. *Appl Energy* 2021; 291: 116798.
28. Riddlesden D and Singleton AD. Broadband speed equity: a new digital divide? *Appl Geogr* 2014; 52: 25–33.
29. Menascé D. Performance and availability of internet data centers. *IEEE Internet Comput* 2004; 8: 94–96.
30. Johnson R and Elizabeth N. Network's server monitoring and analysis using Nagios, 2017. DOI: 10.1109/WiSPNET.2017.8300092.
31. Saunavaara J, Laine A and Salo M. The Nordic societies and the development of the data centre industry: digital transformation meets infrastructural and industrial inheritance. *Technol Soc* 2022; 69: 101931.
32. IT disaster recovery plan. Ready.gov, https://www.ready.gov/it-disaster-recovery-plan (accessed 8 July 2023).
33. Young CS. Data centers: a concentration of information security risk. *Inf Secur Sci* 2016; 1: 339–357. http://dx.doi.org/10.1016/B978-0-12-809643-7.00015-2
34. Knapp KJ, Denney GD and Barner ME. Key issues in data center security: an investigation of government audit reports. *Gov Inf Q* 2011; 28: 533–541.
35. How AWS shield works – AWS WAF, AWS Firewall Manager, and AWS Shield Advanced, https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html (accessed 8 July 2023).