INFORMATION SECURITY STRATEGIES AND PATIENT DATA PRIVACY AMONG HEALTH FACILITIES IN NAIROBI

BY:

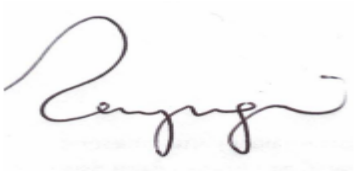
ELIZABETH DELLA AKINYI AYUGI

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT FOR THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF BUSINESS ADMINISTRATION, FACULTY OF BUSINESS AND MANAGEMENT SCIENCES, UNIVERSITY OF NAIROBI

NOVEMBER 2021

DECLARATION

I declare that this project is my original work, and that it has never been submitted for a degree at any other university.

Signed…  ……. Date……26/11/2021...…….....

Elizabeth Della Akinyi Ayugi.

D61/P/8448/2004

This project has been submitted with my approval as University Supervisor.

Signed…….  ……..... Date……26/11/2021……....

Mr Joel Lelei,

Lecturer.

Department of Management Science and Project Planning.

Faculty of Business and Management Sciences.

University of Nairobi.

TABLES OF CONTENTS

ACKNOWLEDGEMENT

First and foremost, I wish to express my gratitude to God the Almighty. May His will be done on earth as it is in heaven.

A special thanks to my supervisor, Mr. Joel Lelei, for his expertise, consistent supervision and availability throughout my research project.

I appreciate the Department of Management Science and Project Planning at the University of Nairobi for their administrative support.

Many thanks to the management of the participating health facilities for allowing me to collect data from respondents in their respective organisations.

I take this opportunity to express my gratitude to colleagues who supported me throughout the course of this research project. I am thankful for their aspiring guidance, invaluable constructive criticism and friendly advice during the project work.

.

DEDICATION

This project is dedicated to my parents, may they rest in peace, in the name of Jesus.

I also dedicate this project to my daughter, love always.

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

ACL : Audit Command Language

BCM : Business Continuity Management

CERTs : Computer Emergency Response Teams

CEO : Chief Executive Officer

CIA : Confidentiality, Integrity and Availability

CIs : Critical Infrastructures

CIIs : Critical Information Infrastructures

CIRTs : Computer Incident Response Teams

COBIT : Control Objectives for Information and Related Technologies

COVID-19: Coronavirus Disease 2019

CSIRTs : Computer Security Incident Response Teams

DPA : Data Protection Act

DR : Disaster Recovery

ECRI : Emergency Care Research Institute

ERC : Ethics and Research Committee

EU : European Union

EUR : European Union Currency

FBO : Faith Based Organisation

FIPS : Federal Information Processing Standard Intellectual Property

GDPR : General Data Protection Regulation

GRC : Governance, Risk and Compliance

GDP : Gross Domestic Product

HIPAA	**:**	Health Insurance Portability and Accountability Act of 1996
HIM	**:**	Health Information Management
HIV	**:**	Human Immunodeficiency Virus
HMIS	**:**	Health management information system
HPTs	**:**	Health Products and Technologies
ICT	**:**	Information and Communications Technology
IDS	**:**	Intrusion Detection Systems
IEC	**:**	International Electrotechnical Commission
IP	**:**	Intellectual Property
IPS	**:**	Intrusion Prevention System
IS	**:**	Information System
ISACA	**:**	Information Systems Audit and Control Association
ISSN	**:**	International Standard Serial Number
ISO	**:**	International Organisation for Standardisation
IT	**:**	Information Technology
ITU	**:**	International Telecommunication Union
ITGITM	**:**	IT Governance Institute
KEMRI	**:**	Kenya Medical Research Institute
KEPH	**:**	Kenya Essential Package for Health
KES	**:**	Kenyan shilling
KHF	**:**	Kenya Healthcare Federation
KHSSP	**:**	Kenya Healthcare Sector Strategic and Investment Plan
KNH	**:**	Kenyatta National Hospital

MIS	**:**	Management Information System
M-PESA	**:**	Mobile money transfer service in Kenya
NATO	**:**	North Atlantic Treaty Organization
NIST	**:**	National Institute of Standards and Technology
NGO	**:**	Non-Governmental Organisation
OECD	**:**	Organisation for Economic Co-operation and Development
OPCs	**:**	Outpatient Clinics
PIA	**:**	Privacy Impact Assessment
PII	**:**	Personally, Identifiable Information
PwC	**:**	PricewaterhouseCoopers
R&D	**:**	Research and Development
RoGGK	**:**	Reporting on Good Governance Kenya
SCADA	**:**	Supervisory Control and Data Acquisition
UHC	**:**	Universal Health Coverage
UON	**:**	University of Nairobi
US	**:**	United States
USD	**:**	United States Dollar
VCT	**:**	Voluntary Counselling and Testing

ABSTRACT

Health facilities have become more reliant on information systems and are subsequently, more susceptible to security and data breach challenges. This study investigated information security strategies and patient data privacy among health facilities in Nairobi County. Security applies to how patient information is secured. Privacy refers to the privileges that patients have in relation to access and use of their personally identifiable information. The objectives of the study were to: (i) establish information security strategies implemented by health facilities in Nairobi, (ii) establish performance of data privacy by health facilities in Nairobi and (iii) establish information security and patient data privacy implementation challenges faced by health facilities in Nairobi. This research employed a descriptive survey design and the study population comprised of all 49 registered facilities as per the Kenya master health facility list of November 2020. A questionnaire with open and closed ended questions was used to collect data. The respondents were persons in charge of health information systems and data or records management in the health facilities. Data analysis was done using descriptive statistics. Data tables, frequencies and percentages were used to draw numerical summaries. Data presentation was done by way of tables and figures. As pertains to application of information security strategies, the study found that implementation of compliance mechanisms was the most popular strategy applied by the health facilities, followed by governance and risk management. The second finding of the study, on application of data privacy principles by health facilities in Nairobi, indicated that performance of data accountability and data protection components was the best, followed by legal and regulatory requirements. A notable finding of data privacy performance was that the facilities did not register any significant data breach occurrences. The study however, appreciated the fact that such sensitive information might have been classified confidential and limited to the health facilities. Lastly, the study identified challenges that affected the health facilities in adoption of data protection and privacy. Common challenges that affected all the facilities were identified as; dynamic regulatory environment, fast pace of digital innovation and transformation, increased interconnection and data sharing with third parties and increase in cyber threats, attacks and crime. The study concluded that although the health facilities implemented robust information security strategies they did not achieve some of their data privacy performance requirements like: percentage of staff receiving privacy training, privacy impact assessment completion rate, satisfactory privacy internal audit score and percentage of organisational budget dedicated to privacy programmes. The study recommended that the facilities scrutinise and address the challenges identified in adoption of their information security and privacy strategies. Health facilities must address information security and data privacy risks to prevent patient harm and preserve the human life. Health facilities can assure attainment of their business goals and objectives by aligning their information security, privacy and business strategies.

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Recently, the technological know-how scene in Kenya has undergone significant transformation and organisations are operating in a competitive, turbulent, innovative and digital environment. Information being the currency of the next millennium, and data the modern oil, means that organisations require suitable information systems and associated technology to fully exploit data, a critical sustainability and success factor (Rafeq, 2019). “Information risk in healthcare can lead to patient harm and is therefore an issue of growing importance. The introduction of digital health records, increased enforcement and sharing of information all point to the need for enhanced information security” (Appari & Johnson, 2010).

HIPAA (2019) confirmed that healthcare breaches were caused by loss, theft, disclosure and hacking. The most prevalent motive for breaches was financial benefit with espionage cases also occurring. Majority of healthcare breaches are linked to internal actors with legitimate access to systems. “Availability issues also arise in the form of ransomware and denial of service attacks” (Verizon, 2019). Four economic sectors, Health Care (15.4%), Information (15.1%), Public Administration (12.2%), and Financial Services and Insurance (10.5%) accounted for 53.2% of the breach activity reported in Q1. Breach events related to illegitimate access to systems were prevalent in 2020, indicating that cyber criminals have become more intentional, competent and targeted with their attacks. However, most data exposed is attributed to disclosure on the internet. On average, hacking exposed approximately 850,000 records per breach. Web disclosure exposed an average of approximately 106,000,000 records per breach (Risk Based Security, 2020).

1.1.1. Information Security Strategy

An information system (IS) is a blend of managerial, strategic and operational activities involved in processing data via information technologies hardware, software, communication networks and databases. Information systems, including online information systems, are increasingly performing essential roles in business (O’Brien & Marakas, 2011). The safeguard of resources against the waste, unavailability, leakage, operational discontinuity or disability relates to information protection. It is

also focused on assuring compliance to alleviate liability that organisations might encounter because of inappropriate processing. Information must be duly secured considering emerging risks, associated costs, obligations and regulations. Information must therefore be handled in the same manner as other business critical resources (Brotby & ITGITM, 2008).

Fundamentally, the scope of security includes technical, managerial and operational measures. Information security policies, exposure assessment and security plans are governance measures for control that determine network infrastructure security. Guidelines on how a network can be accessed securely and consequences of security violations are included in security policies. Operational measures include confidential data defence, incident response, physical security, personal security, security advocacy, business sustainability, hardware and software maintenance. Intrusion detection systems (IDSs), anti-virus, firewalls, intrusion prevention systems (IPSs) and strategies for access controls are technical measures (Sirma et al.,2014).

Benefits of implementing a full proof information security strategy are alignment of business and information security strategies, risk optimisation, value delivery, resource governance, performance evaluation, tracking and disclosing to assure attainment of enterprise objectives (Brotby & ITGITM, 2006).

As information technology progresses, organisations become more reliant on it and are subsequently, more susceptible to security challenges associated with maintaining information systems confidentiality, integrity and availability. Information systems and technologies are under continuous threats, endangered by deficient security measures and a viciously mutating cybercrime landscape, leading to serious repercussions. There is also a disparity between lower cybercrime budget allocations in comparison to information technology budgets by organisations. The estimated cybercrime costs in Kenya in 2016 were USD 175 million, up from USD 150 million reported back in 2015 (Serianu & Paladion, 2016). In the event that privacy data is disclosed in an unintended or unauthorized way, regulatory requirements include mandatory actions to advise those affected by the loss or breach. In a global investor survey in which over 550 business professionals provided feedback, 73% of the participants confirmed cyber hazard as an area of concern (Horne, 2017). According to Hachiya (2005) non-technical

challenges such as administrative and management issues have adversely impacted patients' information security and posed a thorny issue.

1.1.2. Data Privacy

The definition of privacy has been impacted by the fast growth of digital era, social network and cyberspace transactions. Data privacy is associated with appropriate processing, consumption and disposition of personal information while taking into consideration permission to use, notification to the owner, and compliance with regulatory obligations. It is all about the entitlement of people as concerns their personal information. (Intel Corporation, 2011). "Privacy concepts are rooted in legal guidance, such as the United States Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the European Union's General Data Protection Regulation Act of 2018 (GDPR) (EU)" (Murphy, 2015).

Privacy within a business encompasses compliance with legal and regulatory requirements regarding duration of data retention, international regulations and intellectual property (IP). Information security strategies should proactively ensure compliance, by implementing privacy by design and default, while enabling enterprises effectively use big data in support of sustainability and competitiveness. Privacy by design stipulates that every product, process, and project be engineered with privacy in mind, while privacy by default advocates for standardization of such privacy-defence measures within the organisation. Responsibilities for data protection and privacy enforcement must be streamlined and addressed by a cohesive collection of control priorities and activities that satisfy regulatory requirements. Such a method involves cooperation between stakeholders in gathering, processing, utilizing and managing intellectual property, trade secrets, and personally identifying information (PII) and other types of confidential information (ISACA, 2020).

A case study on Facebook social media and privacy by Haumann (2015) illustrates that on social networking, privacy is becoming increasingly vulnerable to exploitation, surveillance and commodification. An online survey of employees in 312 HIV outpatient clinics (OPCs) across Vietnam by Hai et al. (2017) on practices in privacy and security submitted that there was room for improvement in safeguarding patient confidentiality. The California Privacy Rights Act added enhanced penalties for violations involving children's data, e-mail and password combinations. The

implications of failure to adhere to the Kenya Data Protection Act 2019 could result in fines of up to KES 5 million or 1% of previous year's turnover in the case of an organisation, whichever is lower (Dentons et al., 2019).

Benefits of implementing data privacy include regulatory compliance; organisation and technology alignment; better consumer confidence; personalised customer offerings; improved data security management; it also helps cut costs by prompting withdrawal of legacy applications that are no longer vital to businesses; and lastly increases decisions making ability for organisations and returns (Sneha, 2017)

1.2 Health Facilities in Kenya

A health facility is any place where health care is provided, ranging from small clinics, doctors' offices, emergency care facilities to large hospitals with elaborate emergency rooms and trauma centers. Health facilities offer nursing care, medical and surgical treatment for sick or injured people with specialized equipment, nursing and medical staff. One common measure of a country's or region's stability and quality of life is the number and quality of health facilities present (Wikipedia, 2020). Inadequate expenditures on health undermines the quality of care offered in public hospitals, as evidenced by scarcity in human resources, medical supplies and poorly maintained infrastructure. Addressing gaps in elements of the health care delivery system will increase accessibility and affordability of services, especially for the poor. Around 6% of the Gross Domestic Product (GDP) in government spending is on healthcare, and 25% of Kenyans are included by way of a public, non-public or community-based health schemes (Njuguna & Wanjala, 2019).

One of the 14 devolved roles governed by the 47 county governments is the health sector in Kenya. There are six separate tiers of health services, and although the first five are managed at the county level, the national government oversees the sixth level (Kamau & Kisika, 2019). Health facility types in Kenya can be categorised into three: Public government financed facilities; private practitioner regulated facilities run for income; and Mission facilities or Faith Based Organisations (FBOs) associated with, sponsored by, or founded on a religion or religious group. Health facilities information sources include; administrative and management activities; vital events data -on births, disease and deaths; notifiable conditions or critical health events occurring in the

community including health and demographic surveys; and Biomedical, Scientific and systems researches (Task Force Health Care, 2016).

In 2011, the Government of Kenya launched a national e-health strategy to achieve Vision 2030, promoting uniform, quality and reasonably priced healthcare for Kenyan citizens. Safeguarding information privacy and security are mandatory principles regulating system development and procedures to support the e-health strategy. Information technology and health are becoming more interconnected in Kenya, a front runner in innovative information technology solutions. “Kenya is the only country with a comprehensive e-health strategy with a multi-billion USD turnover mobile money (M-PESA) payment system linked to the payment of healthcare services” (KHSSP, 2016). Information for Citizens, Telemedicine, E-Learning and M-Health as well as the Health Information Systems are the five pillars of the e-Health Strategy (Ministry of Medical Services, & Ministry of Public Health and Sanitation, 2011).

Kenya's government has stated that it will achieve Universal Health Coverage (UHC) by 2022. The government's big four strategy, which includes healthcare for all, reflects a strong political commitment to UHC whose purpose is to ensure affordable quality healthcare for all citizens. Countries must expand priority health services, cover more individuals and reduce out-of-pocket costs to achieve UHC (KEMRI, 2019). ICT plays an important role in achieving UHC by speeding up, improving, and supporting primary health care education. ICT is a powerful tool for increasing labour capacity, assisting in the recruitment and retention of experts while also reducing expenses. It increases the standard patient healthcare by promoting experiential practice, which has a significant impact on health outcomes (Kenya Healthcare Federation, 2021).

1.3 Research Problem

Cyber criminals thrive on distractions and opportunities such as the COVID-19 pandemic during which time many organisations have been forced to implement speedy large-scale remote work policies that increases the probability of compromising information systems. Healthcare data violations are likely to increase with digital transformation due to facilities information security practices, which while vigorous, are often less elaborate in comparison to other industries, like the financial sector (Risk Based Security, 2020). Fraudsters use medical records to access free medical services, secure prescription medications or bill insurance. Repositories holding medical records

are precious to cybercriminals as they include social security details, demographics, insurance details and addresses which can sell at 20 times the cost of a stolen credit card number on the black market (Moffit & Steffen, 2017).

Health Products and Technologies (HPT) are strategically crucial investments as pertains to optimal and universal access to healthcare in Kenya . Health Products and Technologies should be effective, available, safe, affordable, of good quality and appropriately used. The Kenya Health Management Information System (HMIS) covers five key areas in data life cycle management, these are namely: information validation, generation, utilization, analysis and dissemination. These areas are all interlinked and together, form the spectrum of the Health Management Information System in Kenya (KHSSP, 2017).

Several related studies on information security and privacy have been undertaken in Kenya. The outcome of a study by Sirma et al. (2014) stated that information breach occurrences can be alleviated by reinforcing and applying robust network and server security policies. A study by Kweri (2013) submitted that data integrity and network security is influenced by data volume, user knowledge and technology. The research recommended training, ability up-grading and awareness mechanisms for personnel to allow them adapt to rising technological challenges. A study by Waithaka (2016) recommended that cyber security issues need to be championed positively to influence adherence to the cyber security strategy and ethics. A study by Nyawanga (2016) has shown that the rate of cyber-crime had accelerated over the previous 12 months, with 80 per cent of attacks originating in China and Kenya being carried out by bank staff, either knowingly or unknowingly. Aside from recommending cyber training, the research additionally observed that weak systems, policies and security structures were another cause of cyber-attacks.

A Chogoria Hospital staff study by Nyaga (2016) on information security and service delivery in health sector, which adopted a descriptive survey design, established a strong relationship between information security adoption and service delivery in the health sector. Patients information is very sensitive and disclosure to unintended audience could lead to stigma, discrimination, errors and even death. The study recommends adoption of information security strategies, guidelines and policies to improve service delivery by ensuring that patients are well-cared for and managed.

Following the historical research discussed above, it is evident that there is no specialised study on information security strategies and patient data privacy in health facilities in Nairobi, leading to the knowledge gap that this study is trying to fill. The research will answer these questions: what information security strategies have health facilities in Nairobi implemented? What is the data privacy performance of health facilities in Nairobi? What challenges are health facilities in Nairobi facing with regard to implementation of information security strategies and patient data privacy?

1.4 Objectives

1.4.1 Overall Objectives

To investigate information security strategies and patient data privacy among health facilities in Nairobi.

1.4.2 Specific Objectives

i. To establish information security strategies implemented by health facilities in Nairobi.

ii. To establish data privacy performance by health facilities in Nairobi.

iii. To establish information security and data privacy implementation challenges faced by health facilities in Nairobi.

1.5 Value of the Study

Valuable study findings will better enable health facilities business and technology alignment; regulatory compliance; patient confidence; personalised patient care and improved data security management. It will also help the facilities optimise business costs, maximising returns and decision-making capacities and capabilities.

Data privacy enhances confidentiality, availability and integrity. These are key considerations in successful health research resulting into breakthrough discoveries, exceptional improvement and creation of new therapies. Medical research can have a profound impact on human health and longevity, resulting in increased capability of the population thereby, contributing significantly to the national economy.

The study will enlighten patients on data privacy. Disclosure must be made to and consent sort from patients before personal information is shared. Health facilities

largely function by having contractual undertakings with third parties who may pose a privacy risk. Patients have a right to sue health facilities for data breaches resulting from poor security practices. The study will provide guidance by means of recommending security controls which will help ensure that both partner and patient agreements and contracts contain the necessary control clauses.

Last but not least, practically this study will inform key success drivers of information security and data privacy to policy makers, including the Government and Regulators. It will also inform the Academic Society, on the basis of empirical evidence and theories of research supporting arguments related to information security strategies and patient data privacy.

This study will also point out specific areas where future research can be done.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

A number of investigations conducted by various researchers concerning theories used in information security studies for framework development are herewith interrogated. Theory is mainly involved with providing an explanation focusing on establishing cause-and-effect relationships (Henning et al., 2004). Kerlinger (1979) suggests that theory explains the relationship between key variables in a present or future state.

2.2 Theoretical Literature Review

Information security and organizational agility theories include the following: Resource based view; social cognitive theory; socio-technical system theory; dynamic capabilities and integrated system theory (Muhamad et al., 2018). Grounded; social cognitive; socio-technical systems; activity; general deterrence; and distributed cognition are theories used in information security studies (Ada et al., 2008).

2.2.1 Socio-technical System Theory

According to socio-technical systems theory, work is made up of people interacting with one another and a technical system that produces products or services. Following this paradigm, the socio-technical interaction has a reciprocal and dynamic impact on the technology's operation and appropriateness, as well as the behaviour of those who use it. Given the interconnection of human and technology systems, socio-technical systems theory proposed that combined optimisation might increase productivity and satisfaction. In other words, optimal job performance would only be possible if the social and technological systems were built to complement one another (Trist, 1981).

2.2.2 Social Cognitive Theory

According to social cognition theory, when people believe they have the ability to execute a beneficial act, they will make a significant effort to do so (Muhamad et al., 2018). A study by Rhee et al. (2009) illustrates that information security is dependent on user (the weakest link) activities, and that sanctions for violations would have insignificant impact. User security awareness, lobbing and advocacy are therefore key information security strategies in achieving successful implementation of and patient data privacy. “All staff handling patient’s information should have proper training on information security” (Nyaga, 2016) . Health care workers should be aware of ethical issues and security practices in the health care environment when it comes to medical

identity theft. Many health-care workers are ignorant of the security risks that exist throughout the integrated network delivery system, which includes many third-parties (Hachiya, 2005).

2.2.3 Integrated System Theory

Hong et al., (2003) incorporated management system, risk management , security policy, contingency, control and audit theories in their review of information system security management . This study demonstrates how integrated system theory can be used to interpret information security management, describing techniques for predicting management performance. A good information security strategy consists of a suitable combination of different components. A study by Nyaga (2016) established that information security and its elements are important in management. A study by Ismail et al.,(2014) submitted that information security is a key component because it emphasizes best defence in relation to the organisational environment. The model has five components: risk management, security policy, auditing of records, internal control and contingency management.

2.2.4 Resource Based View

A study by Wernerfelt (1995) suggests that the foundation for success lies in utilization of resources at a firm's disposal in an agile manner. In respect to information security, it is considered that an organisation can sustain their competitive advantage by implementing privacy and security (Nelson & Romer, 2009). Resource based view indicates that, when monitored, organisational resources- assets, processes, attributes, capabilities, knowledge, information etc- enable design and implementation of strategies that improve efficiency and effectiveness. Dynamic capabilities are an extension of resource-based view but concentrates on an organisations capability to use sufficient information allowing it to become more agile and resilient (Barney, 1991).

2.3 Information Security Strategy

A general plan to achieve one or more long-term or overall objectives under conditions of uncertainty is the original definition of a strategy, a Greek military term. It's a well-coordinated set of efforts aimed at increasing shareholder value and long-term success (Wikipedia, 2020). An information security program is a collection of procedural, technical, operational controls and management structures put in place in accordance with the needs of the company and its risk profile. (Da Veiga & Eloff, 2007). An

information security design should incorporate guidelines on policies and procedures, security governance, risk management, compliance, organisational culture, user awareness and training; and should be based on the effective implementation of security technology (Killmeyer, 2006).

There are many types of security controls, such as access models, encryption, business continuity, data disposal, and incident response, to name a few. Each control has a focus on preventing, detecting, or correcting data incidents, or any combination of those. Mastering management and implementation of information security controls is key, yet the skills required can be complicated and demanding (Murphy, 2015). " Governance, Risk, and Compliance (GRC) is a coordinated effort to ensure cooperation among diverse stakeholders in risk management and regulation within an organization" (PricewaterhouseCoopers,2019). "The Governance, Risk, and Compliance (GRC) management process for Information Security is a necessity for any software systems where important information is collected, processed, and used" (Asnar & Massacci, 2015).

2.3.1 Governance

Governance entails enterprise controls such as implementation of policy, authority, organisational structure, ownership and oversight. This element consists of executive support and dedication from leadership (Krag, 2006). Data governance can be described as a data and information management organisational approach that is formalized as a collection of policies and procedures that cover the entire data life cycle, from acquisition to use to disposal. It pertains risk optimization, measurement and management to ensure that business objectives are met (Da Veiga & Eloff, 2007). The data governance policies describe specific requirements necessary to inform and guide uniform implementation of protective solutions including information quality, inventory and classification, disclosure and sharing.

An assessment of time management of 500 executives who manage cybersecurity indicated that most executives were spending a substantial amount of their time in three specific areas: cyber governance, cyber monitoring, operations and resilience. Effective governance allows the principle of shared accountability to be integrated into a system for information security to create organisational or business resilience. Cyber is everyone's responsibility (Deloitte,2019).

2.3.2 Risk Management

Risk management entails determining, prioritising, and treatment application to reduce, track, and control the likelihood and impact of unforeseen occurrence so as to maximise the achievement of opportunities (ITU,2018). According to ISACA (2020), Risk management entails acknowledging risk; evaluating the effect and possibility of that risk; and formulating risk treatment to manage it within the acceptable risk appetite.

The notion of hospital risk management began in the 1970s in the United States, following a court judgment that established the hospital's corporate obligation for quality of care and held medical staff liable for quality of treatment. In the United States, a comprehensive risk management program is required in all health-care facilities and is a requirement for hospital accreditation (Singh & Ghatala, 2016). Today an organisation wide collaborative risk management approach is the key to sustainability (PwC,2017). A significant aspect of Risk management is the identification, analysis and control of an organisation’s critical information infrastructure and critical resources whose harm or incapacity would have a devastating impact on an agency, nation or community's economic protection. An effective information security strategy promotes protection of Critical Infrastructures (CIs), and Critical Information Infrastructures (CIIs) (Horne, 2017).

The implementation of an organisational contingency plan is part of risk management and includes precautionary measures action taken in the face of potential disasters. Such operations can require both physical preparations and emergency action training. (Chesley & Amitrano, 2016). For a robust response to any threat, resilience enables the integration of business continuity, disaster recovery, and emergency preparedness programs. It is critical to appoint incident response teams and emergency response teams with authority (Horne, 2017). A research covering 523 crisis management, business continuity and senior risk executives in 20 counties, confirmed that being ready, and especially with board support significantly reduces disaster impact on business. 84 % of the respondents submitted that they have a crisis management plans in place, separate from disaster, business continuity and incident management plans (Woo & Cudworth, 2018).

The human or user aspect of risk management has an immense effect on the achievement and failure of business, facilities, systems and information security and

preservation efforts. User aspects include ethical conduct; trust; user awareness; education and training; and privacy (Orshesky, 2003). Policy and Technology issues can overshadow user cybersecurity discussions. A good information security strategy should include capability, capacity building and awareness raising. This may include support of innovation, training schemes, research and development (R&D) clusters. "Human mistakes are by far the greatest security weakness in 2009 (86%), followed by technology (63%)" (Melek, 2009). Ethical behaviour is one of the principles for developing a security culture where both management and the board establish and communicate corporate codes of conduct (Force, N. C. S. S. T. ,2004). Security incidents attributed to insiders, such as third parties and workers, have remained roughly the same or increased. Those linked to hackers, rivals and other outsiders have decreased (PwC,2017).

2.3.3 Compliance

An organisational information security strategy should formulate compliance mechanisms to detect, prevent, and mitigate threats in tandem with their legal requirements, security policies and standards, and technical compliance requirements (ITU,2018). A global risk management survey based on responses from 94 Financial intuitions found that Regulatory enforcement was the third most common of the top three threats (Woo & Cudworth, 2018). International information security standards for governance guidance include; "the International Organisation for Standardisation (ISO) / International Electrotechnical Commission (IEC) 27000 family of security standards, Federal Information Processing Standard (FIPS) Publication 200 and US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53" (ITGITM, 2008). "Security standards are defined as procedures, directives, guidelines, principles or baselines that state what needs to be done and concentrate on areas of current relevance and concern; they are a translation of the problems already stated in security policy" (ISACA, 2020). In their study Kiura and Mango (2017) suggested a model based on ISO 27001:2013. In his study, Kitheka (2013) suggested a framework derived from NIST special publications and ISO 27001 standard. A research by AlKalbani et al. (2017) clearly demonstrates that legislation and regulation advantages have a considerable impact on commitment.

An independent audit is needed to ensure that appropriate steps have been designed and are being implemented to minimise organisation's assets exposure to various risks

including consequences associated with data privacy breaches. An IT review is a probe into and assessment of an organization's information technology systems, policies, and activities. It is possible to analyse the process of acquiring and assessing information in order to determine whether a computer system protects assets, preserves data integrity and allows for effective use of resources. Auditors judgement relies on the persuasiveness of the proof supporting the results and the reasoning used to formulate the conclusions (GrantThornton, & Territoriale, n.d).

There are a range of guidelines for security audits that define protocols that should be followed to ensure proper safeguarding of information resources. The procedures carried out include testing of current security protocols, guidelines, security configurations and technical controls. It is critical to safeguard the physical components of the network (wires, servers, communication devices) from abuse and theft. However, logical access and administrative controls must be strongly stressed by the company. The auditor is also charged with safeguarding the audit data and tools, following through corrective actions and continuous improvement (Ana-Maria et al, 2010). "As companies digitally transform, more digitally-fit internal audit roles help their stakeholders make better decisions and take more calculated risks as a result of their efforts" (PwC,2019). A case study revealed that various security goals were discussed during the audit process to enhance access control and vulnerability of systems, and it can therefore be inferred that IT security audit is a crucial task that any IT organisation must provide for and conduct from time to time (Barzilay, 2019).

2.4 Data Privacy

Privacy is the right of a person to have confidence that his data will used in accordance to the reason for which it was collected. "An individual also has the right to fairly monitor and be aware of the collection, use and disclosure of personal and sensitive information associated with him or her" (Moffit & Steffen, 2017). Personally, identifying information must be processed transparently, appropriately and only for legitimate purposes; should take minimisation into consideration; should be accurate; should be stored for a limited duration only and protected to ensure integrity and confidentiality and related entities should be held fully accountable (Privacy International, 2018).

Potential data privacy threats include employees who abuse legitimate access by stealing and selling sensitive medical and financial information to criminals for purposes of patient identity theft, intimidation or even blackmail; state-of-the-art phishing and malware programmes that install malicious scripts; failure to access third party or vendor information risk and inadequate disposal of hardware, including, lost or stolen medical devices that do not meet security standards. Health facilities can prevent cyber threats by creating awareness; entrenching procedures and policies and making sure that they are adhered to; implementing timely software updates on machines; enforcing secure password policies ; establishing protocols around use of mobile devices and disposal of hardware. Threats are constantly evolving and will become more prevalent and malicious. Data storage and backup is therefore critical and essential. A good backup strategy is the best defense against data loss as facilities will be able to recover lost data and files when required (Consolidated Technologies, Inc., 2019).

2.4.1 Accountability

Professionals in health information management (HIM) must reinforce their roles in promoting access to and usage of digital health information while, taking patient privacy and security into consideration. It's important to stress and expand their emerging position as data stewards. To tackle data privacy and security challenges, health information management workers might use the following strategies: ensure that the practice of health information management adheres to all applicable laws and regulations; create awareness; actively participate in health information system design, development, or implementation (Zeng, Reynolds & Sharp, 2009).

Data processors or controllers, are responsible for complying with legal and regulatory requirements. Accountability breaches can be investigated resulting into sanctions and penalties (DLA Piper, 2017). For success, organisations should ensure adequate data privacy governance such as; current and relevant policies, processes, procedures and structures; senior management buy-in and commitment and; continuous education and training of staff (ITGITM, 2008). A study of 300 executives submitted that trust is a barrier to monetizing data. 33 % said that they were unable to address the new regulations impacting data privacy and protection and 32% were unable to sufficiently protect and secure data (PwC, 2020).

2.4.2 Data Protection

According to ECRI Institute (2015), one of the top ten patient safety risks facing healthcare organizations is lack of data integrity, (incomplete, erroneous, or out-of-date information) resulting mostly from human error but also from technological or software flaws that prevent data from being transmitted from one computer system to another. Medical errors caused by incorrect data entry or manipulation can be reduced by implementation of user-friendly interfaces; due diligence or extreme care; identification of patients at various points throughout the care process; thoroughly testing health information systems, including any upgrades and changes made; and providing comprehensive training to health information system users.

Management can uphold integrity, confidentiality and availability of data by providing appropriate administrative, technological and physical safeguards. Personal data in transit, at rest, and storage should be protected against risks like unauthorised access, disclosure, use, destruction, damage or loss. Controls include: logical measures, like identity management, access controls and data loss prevention; physical measures like locked doors and identification cards; informational measures like threat-monitoring and incident response planning; and technical measures, like pseudonymisation, encryption, anonymisation (Jeimy, 2014). Other information security measures include third party risk management; testing for control adequacy, formulation and execution of policies, training, and code of conduct adherence (Andreas & Marit, 2011). Data protection laws provide for correction of personal data by individuals and organisations. Accuracy of data enhances the decision-making process in organisations (United Nations General Assembly, 1990). 94% of 300 executives surveyed considered client preference data critical or important, but only 15% actually have comprehensive data in this area (PwC, 2020).

Data minimisation is a major aspect in data privacy, both from an information security and an individual's rights point of view demanding that those handling data take relevance, limitation and adequacy of data into consideration (Privacy International, 2018) Organisations can confirm if they are holding the right amount of personal data by being clear about why they need it and periodically reviewing processing policies to check for relevancy and adequacy. In their research, technical concepts for privacy are through data minimization, undetectability, pseudonymity, unobservability,

confidentiality and unlinkability that can be refined into device privacy specifications (Andreas & Marit, 2011).

2.4.3 Legal Requirements

Data must be handled lawfully . Laws are essential in preventing selling and transfer of personal data. Transparency and fairness are vital in guaranteeing that data is used as expected. Consent is a legal basis for processing data and individuals must be appraised (Fortes, 2016). 2,000 consumers were surveyed online submitted that; only 10% feel that they have full control over their personal information; 25% trust that companies manage their data responsibly and; 87% will take business elsewhere if they suspect data abuse (PwC, 2017). Data for one purpose should not be disclosed, made available or used for something else without justification or notice. Acceptable exceptions are the approval of the owner of the data or the legal authority (Fortes, 2016). 2,000 consumers surveyed online submitted that, if they had the option, more than half of consumers (53%) would recall data and that 71% would cease transacting with an entity for unauthorized disclosure of data (PwC, 2017). An assessment of privacy application by more than 100 leading customer brands confirmed that 94% of customers believe trust is more significant than convenience and that explaining how information is used and shared enhances trust (Australian & Index, 2016). All data privacy implications should be taken into consideration in regards to storage limitations. Data controllers should formulate programs detailing retention and deletion policies. In addition, subject's information should be deleted on their request as provided for in legislation (United Nations General Assembly, 1990). The ability and time required to achieve the specified purpose should be used as a guide in determining the period for which personal data are kept (Abouelmehdi et al, 2018).

2.5 Information Security Strategy and Data Privacy

Privacy and protection are related, according to Symanovich (2019). Privacy refers to the privileges that patients have to access and use their personal details. On the other hand, protection applies to how the sensitive information of a patient is secured. In as much as information security entails protection of information transmission, collection and processing, information privacy is related to the safeguard of data identity of the subject. Information security secures information assets, while privacy focuses on safeguarding data subjects' rights. Information systems that meet baseline

requirements may not fulfil privacy compliance requirements. Therefore, organisations must design alternate solution to protect personally identifiable information.

Information protection standards such as integrity confidentiality and availability are not equal to privacy solutions like anonymity and pseudonymity. Implementation of information security policies ensures correct access; the protection of privacy requires data subject disassociation and anonymity. Information protection is focused on authorization and access control, privacy requires informed consent. It is therefore realistic for an organization to enjoy security ,by protecting its assets, without taking into consideration the impact of this activity on the individuals' privacy. Security is about data protection, while privacy is about user identity protection. (Jeimy, 2014).

Privacy and security differences are complex and overlap . An example of protection is the form of data transmission used , such as any worker using secure official systems to communicate with patients instead of sending information through personal email accounts. Privacy laws, on the other hand, would restrict access to patient health information to particular members of hospital staff, such as physicians, nurses, and physician assistants. It is conceivable to have security without privacy, but privacy without security is impossible. Privacy can also stipulate when users can access sensitive information (HIV, gov, 2018).

2.6 Empirical Literature Review

It is quite clear from several scholars like Rafeq (2019), KHSSP (2017), Serianu and Paladion (2016) that todays organisations are operating in a digital environment and that information is a critical success factor. Organisations are therefore at risk as they continuously face complex information security threats as they adopt emerging technologies which are prone to cyber security attacks.

Health Products and Technologies (HPT) are strategically crucial investments as pertains to optimal and universal access to healthcare and by a number of studies carried out by Horne (2017), Moffit and Steffen (2017), HIPAA (2019), Verizon (2019), Deloitte (2019) and Risk Based Security (2020) are in agreement that health care information is precious due to its rich composition and also due to that fact that information security controls implemented by health care facilities are still not as robust

as those implemented by other industries like the Financial sector. Significant information security breaches have been observed and recorded by these studies.

O'Brien and Marakas (2011), Brotby and ITGITM (2006 and 2008) and Sirma et al. (2014) accept that technological, administrative and operational solutions should be incorporated in information security strategy with the objective of safeguarding organisations information resources to enable benefits such as alignment of business and information security strategies and risk optimisation.

Data privacy is about the entitlement of people as concerns their personal information and privacy concepts are rooted in legal guidance as submitted by Murphy (2015), Intel Corporation (2011) and ISACA (2020). Scholars such as Haumann (2015), Hai et al (2017) and Sneha (2017) have observed that generally there is still room for improvement by organisations in regards to embracing privacy and subsequently, promoting benefits such as regulatory compliance, better consumer confidence and improved data security management. According to Symanovich (2019), Jeimy (2014) and HIV, gov (2018), in as much as privacy and security are linked, protection without privacy is possible, but privacy without security is impossible.

Scholars like Nyaga (2016), Sirma et al. (2014), Kweri (2013), Waithaka (2016) and Nyawanga (2016) agree that information security supports attainment of organisational goals. Weak systems, security structures and policies were some causes of cyberattacks. The scholars recommend adoption of information security strategies, guidelines and policies to enhance service delivery and alleviate information breach occurrences. Information security strategies such as effective training, skill up-grading and awareness mechanisms are key for employees to enable them respond appropriately to and continuously adapt to emerging technological challenges affecting organisations information systems infrastructure.

Several studies carried out by researchers like Bostrom and Heinen (1977), Rhee et al. (2009), Hong et al. (2003), Ismail et al. (2014), Wernerfelt (1995), Nelson and Romer (2009), Barney (1991) and Ada et al. (2008) concerning theories applicable to formulation of information security policy submitted resource-based view theory, social cognitive theory, Socio-technical System theory, dynamic capabilities, Integrated system theory among others.

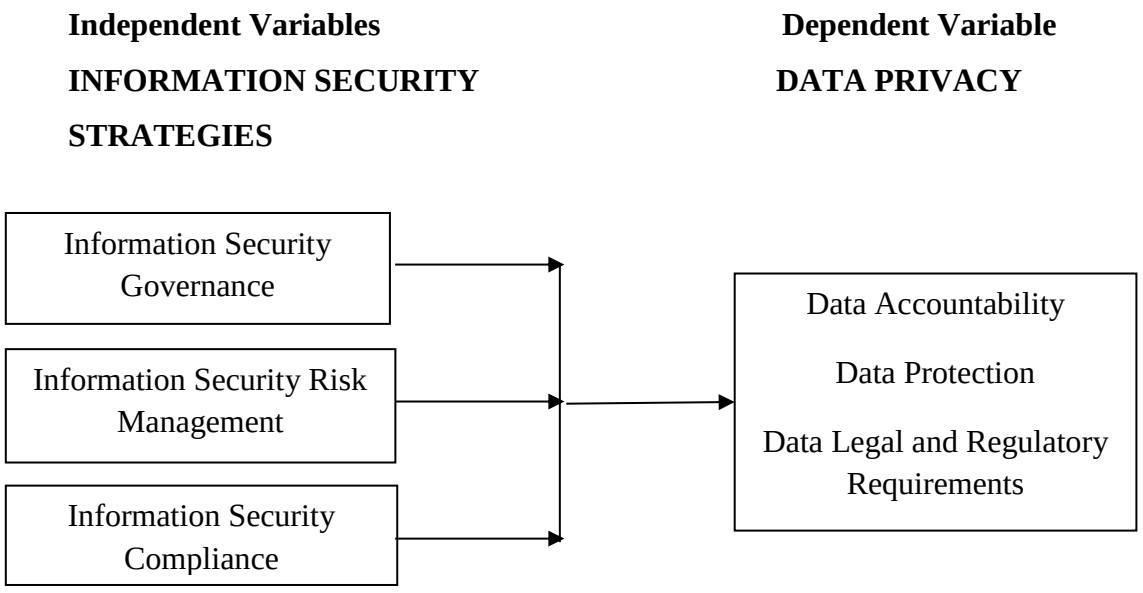
Da Veiga and Eloff (2007), Killmeyer (2006), Murphy (2015), PricewaterhouseCoopers (2019) and Asnar and Massacci (2015) agree that an information security design should incorporate guidelines on policies and procedures, security governance, risk management, compliance, organisational culture, user awareness and training; and should be based on the effective implementation of security technology. It is very clear from the literature review that research has been done in a variety of sectors on information security techniques, but there is little emphasis on the privacy of patient data in healthcare that this study aims to cover extensively.

2.7 Conceptual Framework

According to Mugenda and Mugenda (2010) , A conceptual context is the perspective of the researcher on the research issue guiding the study by showing the relationship between the different components under investigation. The conceptual model in figure 2.1 below expresses the relationship between the independent information security strategies variables and dependent data privacy variable.

2.7.1 Independent and Dependent Variables

Figure 2.1 Conceptual Model



Source: Researcher (2021)

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter details the research methodology used. It comprises of research design, target population, sampling design and sample size, data collection procedures, instruments, as well as the data analysis methodology.

3.2 Research Design

This research employed a descriptive survey design since it attempts to describe structures, conditions, practices, relationships or differences that exist naturally. It looks at opinions held, ongoing processes or apparent patterns (Blumberg, Cooper & Schindler, 2005). Patterns on health facilities information security strategies and data patient data privacy performance were evident once the data was analysed.

3.3 Population of the Study

A study population is described as a universal collection of actual or hypothetical, set of individuals, events or objects which share certain characteristics that an investigator wishes to study (Borg and Crall, 2006).

The study focused on health facilities in the Nairobi County area .The study took a census covering the 49 registered health facilities as per the Ministry of Health, Kenya Master Health Facility List , as at the year 2020.

The health facilities Kenya Essential Package for Health (KEPH) service levels are organized from Level 1 which is at the community level, Level 2 ; dispensaries and clinics, Level 3; health centres and maternity homes and sub district hospitals, Level 4; primary facilities which include District hospitals, Level 5; secondary facilities/ Provincial hospitals to Level 6 which are the Tertiary/ National hospitals. The facilities are in *appendix 2: List of Health Facilities in Nairobi.*

The study instrument was administered to health information management (HIM) officers, in charge of patient data security and privacy, or their equivalent in the health facilities who may include officers in charge of health data or records management and health information systems managers.

Table 3.1 Target Population

KEPH Level	Frequency	Percentage
Level 6	2	4
Level 5	1	2
Level 4	11	22
Level 3	10	20
Level 2	25	51
Level 1	0	0
Total	49	100%

Source: Ministry of Health, Kenya Master Health Facility List (2020) Kenya Master Health Facility List: Find all the health facilities in Kenya

3.4 Inclusion and Exclusion Criteria

3.4.1 Inclusion Criteria

All health facilities in Nairobi as per the Ministry of Health, Kenya Master Health Facility List, as at the year 2020, and using a Health Management Information System. The facilities span five different KEPH levels (Level 1-6; none in level 1) and four owner types namely; public, private and mission or faith-based organisations (FBOs).

3.4.2 Exclusion Criteria

All health facilities in Nairobi, as per the Ministry of Health, Kenya Master Health Facility List , as at the year 2020, not using a Health Management Information System and are therefore, unable to provide relevant and reliable information. Secondly all facilities unable to provide informed consent.

3.5 Data Collection Procedures

To collect data, a questionnaire with open and closed ended questions was used. Closed ended questions restricted respondents to those variables that were of concern to the researcher, while unstructured questions were used to give respondents space to express their views in a more realistic way. The questionnaire is divided into four sections details of which are described in table 3.2 below.

The researcher physically administered the questionnaires. The instrument was sufficiently designed and tested by the researcher to capture relevant data for analysis and measurement. The respondents were persons in charge of data or records management , health information systems managers or data security managers in the health facilities.

3.6 Data Analysis

Defined as the process of placing the collected information in order and structuring its key components in order to communicate the results efficiently and effectively (Borg & Crall, 2006). All questionnaires were checked critically and labelled sequentially after the field work. Data preparation and classification was done using ACL and Microsoft Excel software to identify meaningful categories for analysis and possible associations between the variables. A summary of the description of data methods are captured in table 3.2 below. The data was also tabulated. Tables, frequencies, and percentages were used to draw numerical summaries. Data presentation was done by way of tables, graphs and maps.

Table 3.2: Summary of Data Collection and Data Analysis

DESCRIPTION	AREA	ACTION
To gather and compile general health facility and worker information from participating health facilities.	Section A	Descriptive Statistics
To establish information security strategies implemented by health facilities in Nairobi	Section B	Descriptive Statistics
To establish performance of data privacy by health facilities in Nairobi.	Section C	Descriptive Statistics
To establish patient data protection and privacy implementation challenges faced by health facilities in Nairobi.	Section D	Descriptive Statistics

Source: Researcher (2021)

3.7 Ethical Considerations

Six ethical areas were considered in the research. This included voluntary participation, informed consent, confidentiality, anonymity, the potential for harm and communicating the results to the participant as required.

Permission was obtained from the relevant authority in the School of Business, Management Sciences.

Ethical approval was sought from the University of Nairobi Research, Ethics and Standards Committee to carry out this study.

Information forwarded in the questionnaire was private, confidential and strictly for research purposes.

3.7.1 Screening and Consenting

A written consent form was obtained from respondents in charge of data or records management, health information systems managers, data security managers or their equivalent in the health facilities the consent document was used as a guide for the verbal explanation of the study and was the basis for a meaningful exchange between the researcher and the respondent.

3.7.2 Data Management

The researcher did not collect any personally identifiable information. The health facilities records were kept secure by use of password protected files when the data was in electronic storage and encryption when sending information over the internet. Research documents were locked in secure drawers. Health facility information was not recorded in a way that links the subject responses with identifiable information. The researcher reported only aggregate findings, and not individual health facility data to the public and physical records were destroyed securely by shredding.

CHAPTER FOUR: DATA ANALYSIS, PRESENTATION AND INTERPRETATION OF FINDINGS

4.1 Introduction

This study conducted an evaluation of information security strategies implemented by health facilities in Nairobi and proposed appropriate methods to ameliorate patient data privacy. The study had three objectives namely; to establish information security strategies implemented by health facilities in Nairobi; to establish performance of data privacy and to establish information security and data privacy implementation challenges faced by health facilities in Nairobi. The study further made appropriate recommendations towards improvement of patient data protection and privacy. This chapter therefore presents an analysis and presentation of findings as per the above stated objectives. Analysed data was recorded in frequency and percentage tables. Data presentation was done in graphs and charts. The findings were thereafter interpreted qualitatively based on data analysis, interviews held, observations made on-site and information collected from open ended questions.

4.2 General Health Facility Information

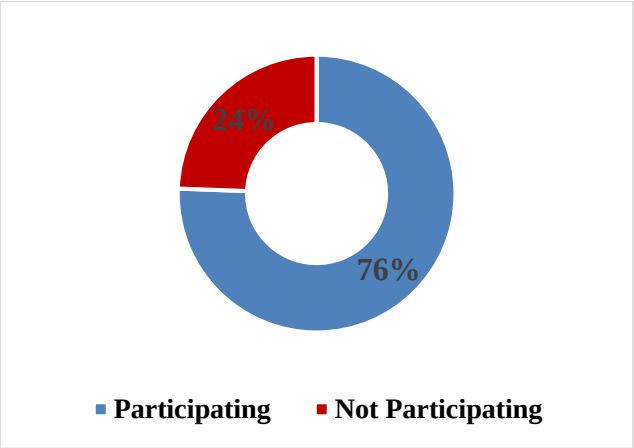
4.2.1 Health Facilities Response Rate

Table 4.1 Health Facilities Response Rate

Category	Frequency	Percentage
Participating	37	76
None participating	12	24
Total	**49**	**100**

Source: Author (2021)

Figure 4.1 Health Facilities Response Rate



Source: Author (2021)

The researcher issued 49 questionnaires to 49 health facilities. However, after consultations with their management, some of the respondents declined to participate in the research. The results in table above indicates a fit for analysis response rate of 76% as per the Mugenda and Mugenda (2010) study indicating that any response rate of 70% and above is considered excellent for analysis and making conclusions.

The researcher observed that health facilities that were known for provision of progressive, quality care services in the region were extremely welcoming to the study. They had an open-door policy whereby managers in charge attended to the researcher almost immediately with utmost decorum. These facilities also had clear internal structures and processes on how research requests were handled. Further, they were interested in learning how their facilities would benefit from the study, not limited to getting a copy of the completed study. This observation confirms that alignment of information security and business strategy assure attainment of enterprise objectives (Brotby & ITGITM, 2006).

4.2.2 Number of Patients Attended to Per Month

The study sort to establish the approximate number of patients attended to per month by the health facilities with the intention of investigating the relationship between facilities using health management information systems and number of patients attended to. The findings were documented in the table below:

Table 4.2 Number of Patients Attended to Per Month

Health Facility Code	KEPH Level	Category	Patients Per Month	Using HMIS
HFC-003	Level 5	Hospital	>50,000	Yes
HFC-010	Level 4	Hospital	20,000	Yes
HFC-026	Level 2	Medical Clinic	150-200	Yes
HFC-027	Level 2	Medical Clinic	130-200	No
HFC-045	Level 2	Dispensary	3900-6000	Yes

Source: Author (2021)

Unfortunately, as indicated in the table above only 5 (14%) of the respondents agreed to provide this information. 86 % of the respondents withheld this information due to a number of reasons including; patient data is classified as internal information; the information requested could easily be related to other data sets to inappropriately determine other factors such as revenue generated; the request would compel them to

access their health management system inappropriately and patient numbers fluctuated due to the COVID-19 pandemic and may be extremely misleading.

It is however evident from analysis of the table above that number of patients attended to per month may not be the only factor used in determining whether a health facility will use a health management information system. Health facility code – 026 was using a health management information system irrespective of attending to only 150 to 200 patients per month. On the other hand, Health facility code – 027, attending to a similar number was not using a health management information system. This analysis agrees that organisations require personalised information systems and associated technology to fully exploit data, a critical sustainability and success factor (Rafeq,2019).

4.2.3 Facilities Using Health Management Information System

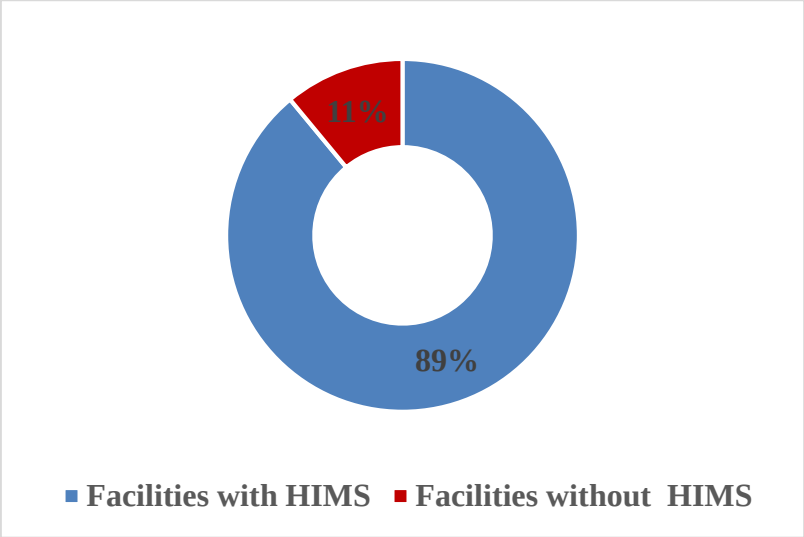
The study sort to identify and confirm which of the health facilities were using a health management information system with the objective of establishing their suitability in relation to providing accurate and reliable information regarding the study objectives . The findings were documented in the table below:

Table 4.3 Facilities Using Health Management Information System

Category	Frequency	Percentage
Facilities with information system	33	89
Facilities without information system	4	11
Total	**37**	**100**

Source: Author (2021)

Figure 4.3 Facilities Using Health Information Management System



Source: Author (2021)

It is evident from the table and figure above that 89% of respondents were using a health information management system. On the other hand, 11% were using other forms of personalised facility efficient and suitable record management systems like physical patient files in combination with Microsoft Excel or Microsoft Access databases. It was therefore concluded that majority of the respondents were using health information management system. This finding affirms the fact that information technology and health are becoming more interconnected in Kenya, a front runner in innovative Information Technology solutions (KHSSP, 2016).

4.2.4 Data Privacy and Protection Roles

The study sort to establish the data protection and privacy roles played by the health facilities with the objective of understanding the extent to which the health facilities appreciated their role and responsibilities in relation to information security and patient data privacy. 100% of the respondents indicated that they performed both the data controller and processor roles. These facilities not only process the data but also determine the purpose and means of processing personal data, either alone or in collaboration with third parties. The researcher observed that the respondents were extremely familiar with the terms and roles, awareness of which may be attributed to the health facilities efforts, in light of the Kenya Data Protection Act, which came into effect on 25 November 2019. Discussions with the respondents confirmed that they were fully aware of the implications that failure to adhere to the Kenya Data Protection Act 2019 could result in fines of up to KES 5 million or 1% of previous year's turnover in the case of an organisation, whichever is lower (Dentons et al., 2019).

4.2.5 Health Facility Respondents by Job Positions and Titles

The study sought to establish and analyse health facility respondents by job positions and titles with the objective of establishing their suitability in relation to providing accurate and reliable information regarding the study objectives. Findings were documented in the table below:

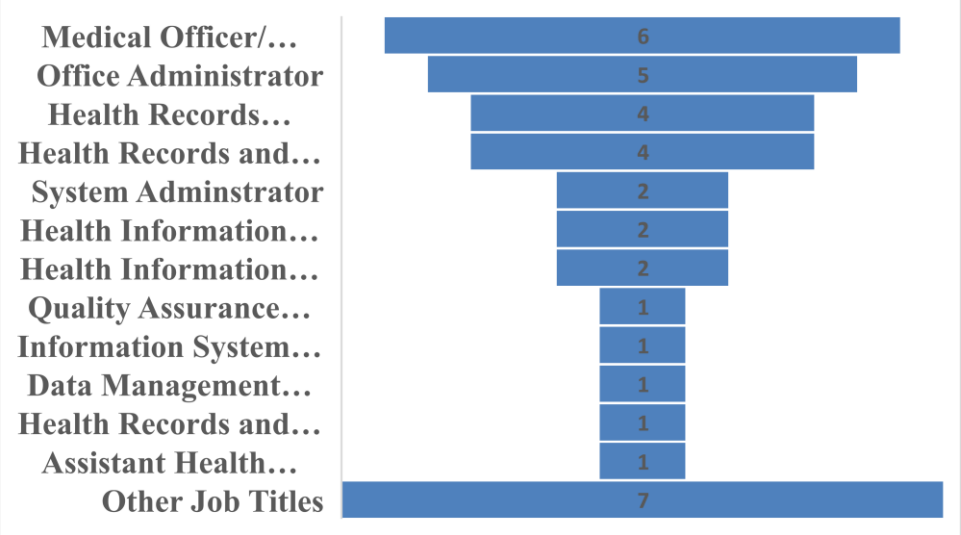
Table 4.4 Health Facility Respondents by Job Positions and Titles

Respondent Job Title	Frequency	Percentage
Medical Officer/ Doctor in Charge	6	16
Office Administrator	5	14
Health Records Officer	4	11
Health Records and Information Officer	4	11

Respondent Job Title	Frequency	Percentage
System Administrator	2	5
Health Information System Manager	2	5
Health Information Management Officer	2	5
Quality Assurance Officer	1	3
Information Systems Client Support Officer	1	3
Data Management Assistant	1	3
Health Records and Information Technologist	1	3
Assistant Health Records & Information Management Officer	1	3
Other Job Titles	7	19
Total	**37**	**100**

Source: Author (2021)

Figure 4.4 Health Facility Respondents by Job Positions and Titles



Source: Author (2021)

Table 4.4 and Figure 4.4 above illustrate that the job positions and titles of the respondents varied from facility to facility. The title with the highest frequency was Medical Officer or Doctor at 16% followed by Office Administrator at 14%. Other notable titles were System Administrator at 5% and Quality Assurance Officer at 3%. The researcher observed that in most instances medical officers and administrators who make up the top 2 of the respondents at 30% were extremely cautious and suspicious in comparison to those respondents with a strong information technology and security background. Medical officers and administrators were also not easily available most probably due to the customer facing nature of their core responsibilities. The devise health workforce should fully embrace IT because healthcare data violations are likely to increase with digital transformation due to facilities information security practices,

which while vigorous, are often less elaborate in comparison to other industries, like the financial sector (Risk Based Security, 2020). ICT is a powerful tool for increasing labour capacity, assisting in the recruitment and retention of experts while also reducing expenses. It increases the standard patient healthcare by promoting experiential practice, which has a significant impact on health outcomes (Kenya Healthcare Federation, 2021).

4.3 Information Security Strategies

4.3.1 Facilities with Formally Accepted Information Security Strategy

The study sought to establish the frequency of health facilities with formally accepted and operational information security strategies and policies. Strategies and policies reflect health facilities mission, values, and culture, as well as the facilities expectations on its health workers. Enforcing these strategies and policies after they're in place is even more crucial. 100% of the respondents using health information management systems confirmed that they have formally accepted information security strategies. The respondents confirmed that their strategies incorporated a number of information security policies like records management, data retention, data privacy, incident management and business continuity policies. An information security design should incorporate guidelines on policies and procedures, security governance, risk management, compliance, organisational culture, user awareness and training; and should be based on the effective implementation of security technology (Killmeyer, 2006).

4.3.2 Information Security Governance

The study sought to establish aspects of information security governance that health facilities considered in their formally accepted information security strategies. Analysis of Governance considerations entailed discussions on health facility controls such as implementation of policy, authority, organisational structure, resource allocation ,ownership and oversight. The findings were documented in table below:

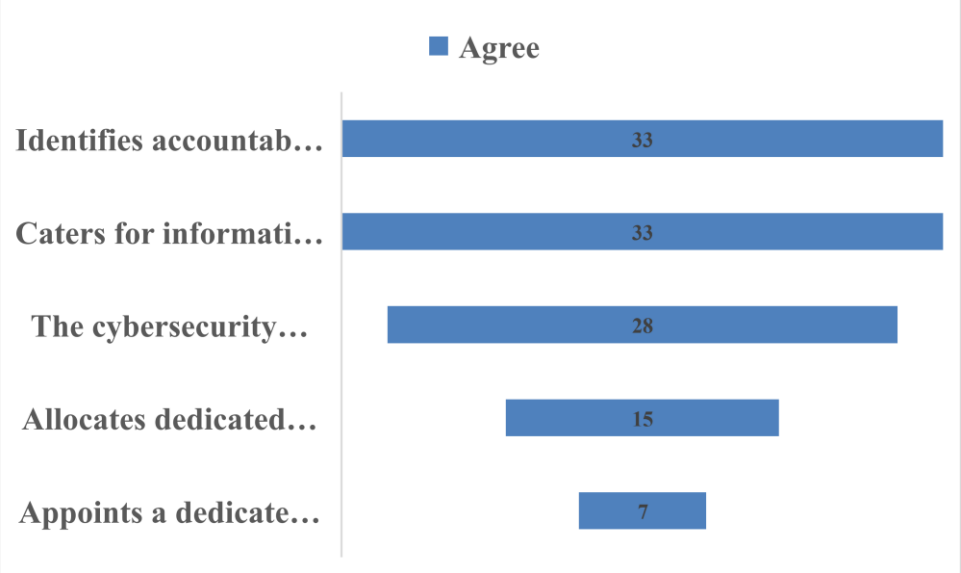
Table 4.5 Aspects of Information Security Governance Considered

Aspects of Information Security Governance	Agree	%	Disagree	%	Total	%
Appoints a dedicated cybersecurity leader	7	21	26	79	33	100
The cybersecurity leader is part of the top management	28	85	5	15	33	100

Aspects of Information Security Governance	Agree	%	Disagree	%	Total	%
Allocates dedicated and appropriate resources	15	45	18	55	33	100
Identifies accountable and responsible persons	33	100	0	0	33	100
Caters for information security programmes/policies execution	33	100	0	0	33	100
Average percentage – Agree		**70**				

Source: Author (2021)

Figure 4.5 Aspects of Information Security Governance Considered



Source: Author (2021)

Table 4.5 and Figure 4.5 above illustrate aspects of information security governance that health facilities information security strategies took into consideration. From the analysis, 100% of the respondents agreed that their strategies identify accountable, responsible persons and cater for information security programmes/policies execution. In this study, only 21% agreed that their strategy appoints a dedicated cybersecurity leader and that they had other leadership roles in the facility like risk management or security. Health facilities can achieve their goals and competitive advantage via effective Governance which entails enterprise controls such as implementation of policy, authority, organisational structure, ownership and oversight. Executive support and dedication from leadership is therefore critical (Krag, 2006). 45% of the respondents confirmed that their strategy allocates dedicated and appropriate resources. This finding agrees with a study by Serianu & Paladion (2016) indicating that there is

a disparity between lower cybercrime budget allocations in comparison to information technology budgets by organisations.

4.3.3 Information Security Risk Management

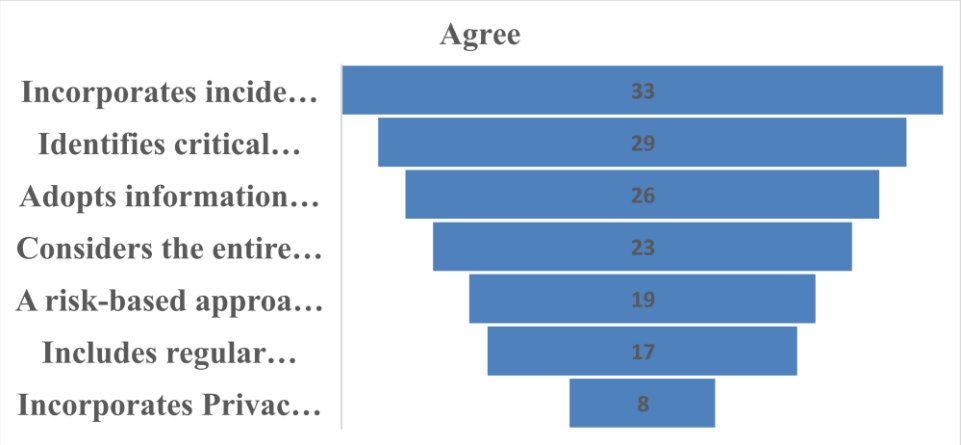
The study sought to establish aspects of information security risk management that health facilities consider in their formally accepted information security strategies and policies. The notion of hospital risk management began in the 1970s in the United States, following a court judgment that established the hospital's corporate obligation for quality of care and held medical staff liable for quality of treatment. The findings were documented in the table below:

Table 4.6 Aspects of Information Security Risk Management Considered

Aspects of Information Security Risk Management	Agree	%	Dis-agree	%	Total	%
A risk-based approach is adopted in prioritising programmes	19	58	14	42	33	100
Identifies critical information infrastructures and services	29	88	4	12	33	100
Incorporates Privacy Impact Assessment (PIA)	8	24	25	76	33	100
Adopts information classification	26	79	7	21	33	100
Considers the entire information lifecycle	23	70	10	30	33	100
Incorporates incident response, BCM and DR	33	100	0	0	33	100
Includes regular testing for the adequacy of security measures	17	52	16	48	33	100
Average percentage – Agree		**67**				

Source: Author (2021)

Figure 4.6 Aspects of Information Security Risk Management Considered



Source: Author (2021)

Table 4.6 and Figure 4.6 above illustrate aspects of information security risk management that health facilities took into consideration. From the analysis, 100% of the respondents agreed that their strategies incorporated incident response, business contingency and disaster recovery. It is critical to appoint incident response teams and emergency response teams with authority (Horne, 2017). 88% of the facilities agree that they identified critical information infrastructures and services. An effective Information security strategy promotes protection of critical infrastructures and critical information infrastructures (Horne, 2017). However, only 52% agreed that their strategy included regular testing for the adequacy of information security measures which is an area that requires improvement because according to ECRI Institute (2015), medical errors caused by incorrect data entry or manipulation can be reduced by thoroughly testing health information systems, including any upgrades and changes made and providing comprehensive training to health information system users.

Only 24% agreed that their information security strategy incorporates Privacy Impact Assessment (PIA). The above findings are aligned with findings of scholars such as Haumann (2015), Hai et al (2017) and Sneha (2017) who observed that generally there is still room for improvement by organisations in regards to embracing privacy According to Symanovich (2019), Jeimy (2014) and HIV, gov (2018), in as much as privacy and security are linked, protection without privacy is possible, but privacy without security is impossible. Security is about data protection, while privacy is about user identity protection (Jeimy, 2014). Today an organisation wide collaborative risk management approach is the key to sustainability (PwC,2017).

4.3.4 Information Security Compliance

The study sought to establish aspects of information security compliance that health facilities considered in their formally accepted information security strategies and policies. The findings were documented in the table below:

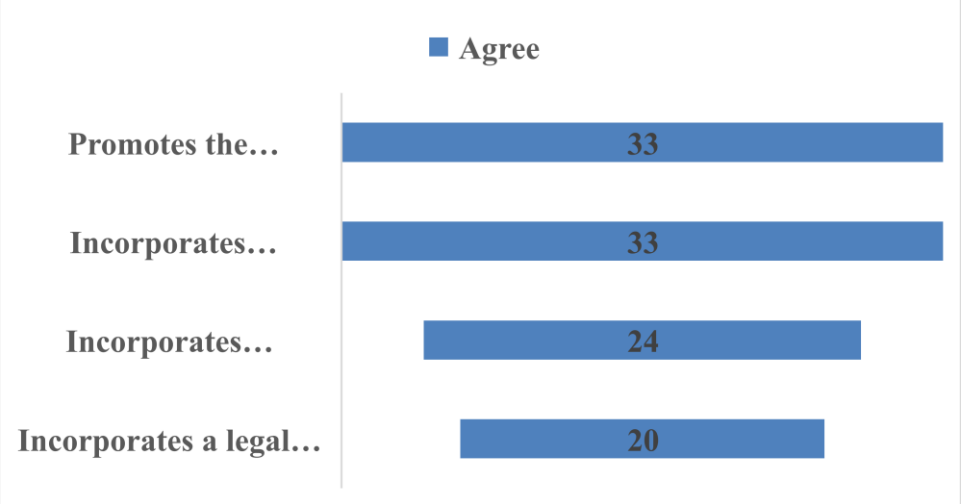
Table 4.7 Aspects of Information Security Compliance Considered

Aspects of Info Sec Compliance	Agree	%	Disagree	%	Total	%
Incorporates a legal and regulatory framework	20	61	13	39	33	100
Promotes the establishment of compliance mechanisms	33	100	0	0	33	100
Incorporates continuous internal audit, monitoring and improvement	33	100	0	0	33	100

Aspects of Info Sec Compliance	Agree	%	Disagree	%	Total	%
Incorporates independent external audits and assurance	24	73	9	27	33	100
Average percentage – Agree		**83**				

Source: Author (2021)

Figure 4.7 Aspects of Information Security Compliance Considered



Source: Author (2021)

Table 4.7 and Figure 4.7 above illustrate aspects of information security compliance that health facilities took into consideration. From the analysis, 100% of the respondents agreed that their strategies incorporated continuous internal audit, monitoring and improvement therefore, promoted the establishment of compliance mechanisms. An organisational information security strategy should formulate compliance mechanisms to detect, prevent, and mitigate threats in tandem with their legal requirements, security policies and standards, and technical compliance requirements (ITU,2018). From the analysis, 73% of the respondents agreed that their strategies incorporated independent external audits and assurance. An independent audit is needed to ensure that appropriate steps have been designed and are being implemented to minimise organisation's assets exposure to various risks including consequences associated with data privacy breaches (GrantThornton, & Territoriale, n.d). Lastly , only 61% of the respondents agreed that their strategies incorporated a legal and regulatory framework, a finding which agrees with a survey based on responses from 94 financial intuitions that found that regulatory enforcement was the third most common of the top three threats (Woo & Cudworth, 2018).

4.4 Performance of Data Privacy

4.4.1 Data Accountability and Protection

The study sought to assess performance of data privacy principles observed by health facilities in Nairobi. Data privacy requires compliance with data accountability and data protection principles. The findings were documented in the table below:

Table 4.8 Data Accountability and Protection

Data Accountability and Protection Requirements	Agree	% - Agree	Dis-agree	% -Dis agree	Total	%
Does your health facility carry out a comprehensive risk assessment that recommends accountability measures and responsibility allocation?	33	100	0	0	33	100
Is patient data at rest and in transit protected by physical, logical, system and technical security safeguards?	33	100	0	0	33	100
Are all steps taken to eliminate errors and ensure that patient data processing is accurate, complete and up-to-date?	33	100	0	0	33	100
Do your patient data privacy control measures include implementation of user training programmes and adherence to approved codes of conduct?	33	100	0	0	33	100

Source: Author (2021)

Table 4.8 above illustrates how health facilities performed in data privacy in relation to accountability and protection of data. From the analysis, 100% of the respondents indicated that they fully complied with data accountability and protection requirements. The facilities performed a comprehensive risk assessment that recommended accountability measures and allocation of responsibility; they ensured that patient data at rest and in transit is protected by physical, logical, system and technical security safeguards; they took all steps to eliminate errors and ensure that patient data processing is accurate and complete. Lastly 100% of the respondents indicated that they implemented up-to-date user training programmes and adherence to approved codes of conduct. In summary the health facilities indicated that they are fully compliant with data accountability and protection principles. Management can uphold integrity, confidentiality and availability of data by providing appropriate administrative,

technological and physical safeguards. Personal data in transit, at rest, and storage should be protected against risks like unauthorised access, disclosure, use, destruction, damage or loss (Jeimy, 2014).

4.4.2 Legal and Regulatory Requirements

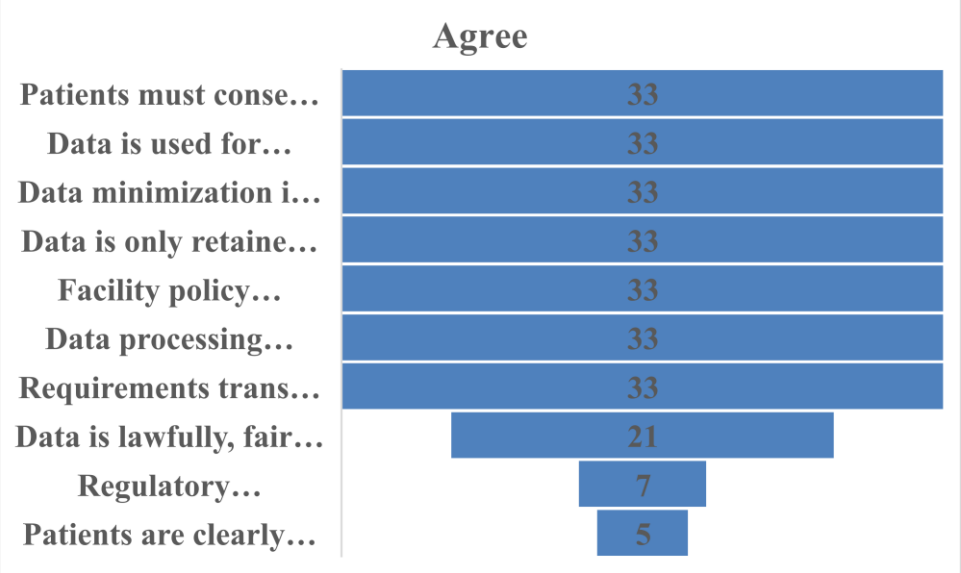
The study sought to assess performance of data privacy principles observed by health facilities in Nairobi. Data privacy requires compliance with legal and regulatory requirements. The findings were documented in the table below:

Table 4.9 Legal and Regulatory Requirements

Legal and Regulatory Requirements	Agree	% - Agree	Dis agree	% -Dis agree	Total	%
Data is lawfully, fairly and transparently processed	21	64	12	36	33	100
Patients are clearly informed before their data is shared	5	15	28	85	33	100
Patients must consent before their data is shared	33	100	0	0	33	100
Data is used for limited purposes only	33	100	0	0	33	100
Data minimization is observed	33	100	0	0	33	100
Data is only retained for the period originally and legally required	33	100	0	0	33	100
Facility policy establishes patient data retention schedules	33	100	0	0	33	100
Data processing requirements relating to a minor	33	100	0	0	33	100
Requirements for transfer of data out of Kenya	33	100	0	0	33	100
Regulatory notification and communication of breach	7	21	26	79	33	100
Average percentage – Agree		**80**				

Source: Author (2021)

Figure 4.9 Legal and Regulatory Requirements



Source: Author (2021)

Table 4.9 and Figure 4.9 above illustrate how health facilities performed in relation to data privacy legal and regulatory requirements. From the analysis, 100% of the respondents indicated that they fully complied with the following principles; seeking patients consent before their data is shared, using data for limited purposes only, data minimization, legal requirements for data retention aligned with their data retention schedules, data processing requirements relating to minors and requirements for transfer of data out of Kenya**.** 36% of the respondents disagreed that data is lawfully, fairly and transparently processed due to lack of patient transparency. 85 % of the respondent disagreed that patients are clearly informed before their data is shared. In as much as they seek patient consent in advance, they do not inform them each time their data is shared. An example is data shared with insurance companies or for emergency purposes. 79% of the respondents disagreed that they have notified the regulator on data breaches. Further discussions indicated that these respondents have never had a breach and as such have not communicated in the same.

The findings stated above agree with a number of studies covered by this research in relation to data privacy legal and regulatory requirements. Laws are essential in preventing selling and transfer of personal data. Transparency and fairness are vital in guaranteeing that data is used as expected. Consent is a legal basis for processing data and individuals must be appraised (Fortes, 2016). 2,000 consumers were surveyed online and submitted that; only 10% feel that they have full control over their personal

information; 25% trust that companies manage their data responsibly and; 87% will take business elsewhere if they suspect data abuse (PwC, 2017). An assessment of privacy application by more than 100 leading customer brands in the market confirmed that 94% of customers believe trust is more significant than convenience and that explaining how information is used and shared enhances trust (Australian & Index, 2016)

4.4.3 Key Performance Indicators Met Successfully

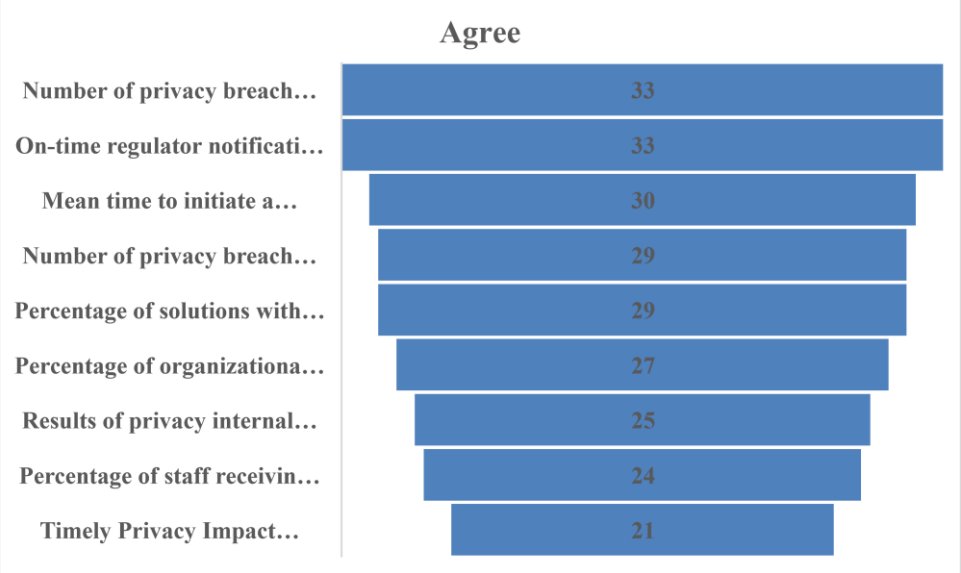
The study sought to assess performance of data privacy principles observed by health facilities in Nairobi. Facilities indicated Key Performance Indicators (KPIs) that they had successfully achieved this year. The findings were documented in table below:

Table 4.10 Key Performance Indicators Met Successfully

Key Performance Indicators Met Successfully	Agree	% - Agree	Dis agree	% -Dis agree	Total	%
Percentage of organizational budget dedicated to privacy	27	82	6	18	33	100
Timely Privacy Impact Assessment (PIA) completion rate	21	64	12	36	33	100
Percentage of staff receiving privacy training	24	73	9	27	33	100
Number of privacy breach complaints by customers	29	88	4	12	33	100
Number of privacy breach complaints by the regulator	33	100	0	0	33	100
On-time regulator notification for privacy breaches	33	100	0	0	33	100
Results of privacy internal audits	25	76	8	24	33	100
Mean time to initiate a response to a data breach incident	30	91	3	9	33	100
Percentage of solutions with encryption, anonymization, or pseudonymization capabilities	29	88	4	12	33	100
Average percentage – Agree		**85**				

Source: Author (2021)

Figure 4.10 Key Performance Indicators Met Successfully



Source: Author (2021)

Table 4.10 and Figure 4.10 illustrate how health facilities performed, in the current year, in relation to their health facilities data privacy KPIs. From the analysis, 100% of the respondents indicated that they successfully achieved regulatory KPIs in terms of customers complaints escalated to the regulator and breaches experienced. 91% successfully achieved mean time to initiate a response to a data breach incident, 88% successfully achieved number of privacy breach complaints by customers, 88% successfully achieved percentage of solutions with encryption, anonymization, or pseudonymization capabilities and 82% successfully achieved percentage of organizational budget dedicated to privacy. On the other hand, some of the health facilities indicated that they had not achieved their KPIs in the following aspects; 24% did not meet their expected privacy internal audit score or rating, 27% did not meet their expected staff privacy training numbers and lastly, 36% did not complete Privacy Impact Assessments (PIA) in a timely manner.

Successful achievement of regulatory KPIs recorded above in the table and figure above contradicts studies by Deloitte (2019) and Risk Based Security (2020) that indicated that significant information security breaches have been observed and recorded. An online survey by Hai et al. (2017) submitted that there was room for improvement in safeguarding patient confidentiality. HIPAA (2019) confirmed that healthcare breaches were caused by loss, theft, disclosure and hacking. Majority of healthcare breaches are linked to internal actors with legitimate access to systems. Many health-care workers

are ignorant of the security risks that exist throughout the integrated network delivery system, which includes many third-parties (Hachiya, 2005). Timely privacy assessments are crucial because they entail determining, prioritizing, and treatment application to reduce, track, and control the likelihood and impact of unforeseen occurrence so as to maximize the achievement of opportunities (ITU,2018).

4.5 Data Protection and Privacy Adoption Challenges

The study sought to establish and critically interrogate patient data protection and privacy implementation challenges faced by health facilities in Nairobi. A study by Bostrom and Heinen (1977) submits that most management information systems failures and challenges have been associated with organisational behavioural problems. The findings were documented in the table below:

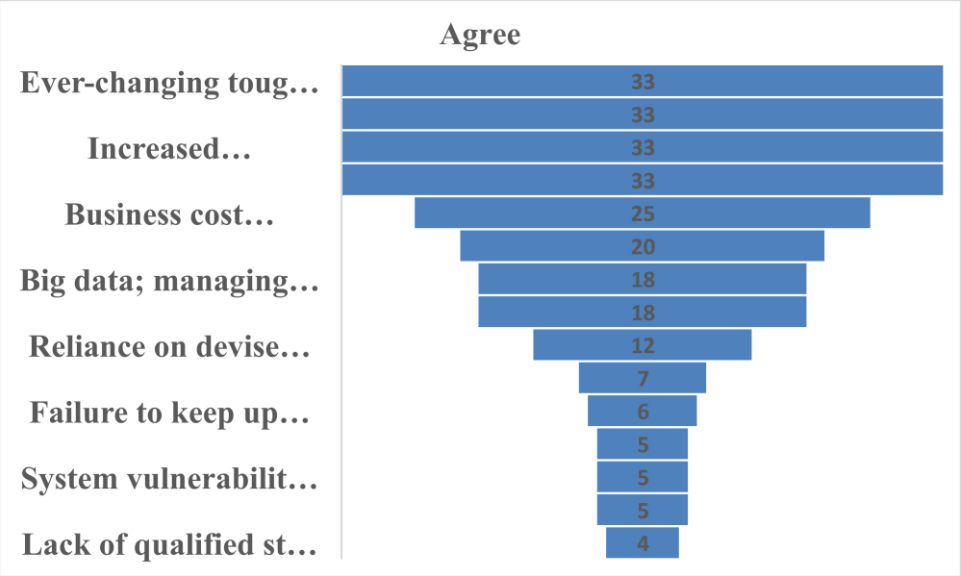
Table 4.11 Data Protection and Privacy Adoption Challenges

Data Protection and Privacy Adoption Challenges	Agree	% - Agree	Dis agree	% -Dis agree	Total	%
Ever-changing tough regulatory environment in healthcare	33	100	0	0	33	100
Fast pace of digital innovation and transformation	33	100	0	0	33	100
Big data; managing high volumes of rich and sensitive data	18	55	15	45	33	100
Reliance on devise workforce, with different backgrounds	12	36	21	64	33	100
Reliance on devise third parties and outsources services	18	55	15	45	33	100
Increased interconnection and data sharing with third parties	33	100	0	0	33	100
Poor risk management, compliance and assurance processes	5	15	28	85	33	100
Business cost-reduction or optimization requirements	25	76	8	24	33	100
Lack of qualified staff in the market	4	12	29	88	33	100
Poor user awareness, training and acceptance of systems	20	61	13	39	33	100
System vulnerability- Insider access abuse	7	21	26	79	33	100

Data Protection and Privacy Adoption Challenges	Agree	% - Agree	Dis agree	% -Dis agree	Total	%
System vulnerability- Outsider abuse	5	15	28	85	33	100
Financial fraud and motivation	5	15	28	85	33	100
Failure to keep up with software updates and patches	6	18	27	82	33	100
Increase in Cyber threats - Cyber-crime – Cyber-attacks	33	100	0	0	33	100

Source: Author (2021)

Figure 4.11 Data Protection and Privacy Adoption Challenges



Source: Author (2021)

Table 4.11 and Figure 4.11 illustrate data protection and privacy adoption challenges that the health facilities faced. From the analysis, 100% of the respondents indicated that the following were their biggest challenges; ever-changing tough regulatory environment in healthcare, fast pace of digital innovation and transformation, increased interconnection and data sharing with third parties and increase in Cyber threats, Cyber-crime and Cyber-attacks. As information technology progresses, organisations become more reliant on it and are subsequently, more susceptible to security challenges associated with maintaining information systems confidentiality, integrity and availability (Serianu & Paladion, 2016).

76% agreed that business cost-reduction or optimization requirements were a challenge. Information must be handled in the same manner as other business critical resources

(Brotby & ITGITM, 2008). 61% indicated that poor user awareness, training and acceptance of systems was an issue. A study by Kweri (2013) recommended training, ability up-grading and awareness mechanisms for personnel to constantly adapt to rising technological challenges affecting the bank's management information system. 55% of the respondents were concerned about big data - managing high volumes of rich and sensitive data. Information security strategies should proactively ensure compliance, by implementing privacy by design and default, while enabling enterprises effectively use big data in support of sustainability and competitiveness (ISACA, 2020). Lastly, 55% were concerned about reliance on devise third parties and outsources services. "Incidents linked to hackers, rivals and other outsiders have decreased. Those attributed to insiders, such as third parties and workers, however, have remained roughly the same or increased" (PwC,2017).

4.6 Discussion of the Findings

Analysis of the demographic information confirmed that majority (89%) of the respondents were using health information management systems. Health facilities have varying personalised and specialised needs and as such the number of patients attended to per month was not the only or key factor used in justification of system acquisition. 100% of the respondents performed both the data controller and processor roles. Top study respondents by job title or role were medical officers and administrators at 30%.

Analysis of governance, risk management and compliance strategies confirmed that 100% of the respondents have formally accepted information security strategies and policies. Only 21% of the respondents have a dedicated cybersecurity leader. 45% of the respondents confirmed appropriate resource allocation.

On risk management , 100% agreed that their risk management strategy is resilient. 88% of the respondents agreed that their risk management strategy considered critical information infrastructures and services. 79% confirmed that they adopted information classification while 70% agreed that their risk management strategy incorporated the entire data life cycle management. Further discussions identified challenges associated with assurance of data shared with third parties.

There was however room for improvement in risk management as only 58% agreed that a risk-based approach was used in prioritising programs, 52% agreed that their strategy included regular testing for the adequacy of information security measures and 24%

that their information security strategy incorporated Privacy Impact Assessment (PIA). It is therefore realistic for a facility to enjoy security, by protecting its assets, without taking into consideration the impact of this activity on the patients' privacy.

On compliance, 100% of the respondents agreed that their strategies incorporated continuous internal audit, monitoring and improvement and therefore, promoted the establishment of compliance mechanisms. 73% agreed that their strategies incorporated independent external audits and assurance.61% of the respondents agreed that their strategies incorporated a legal and regulatory framework.

An analysis of data privacy performance confirmed that 100% of the respondents fully complied with data accountability and protection requirements by performing comprehensive risk assessments, securing data at rest and in transit, ensuring that patient data processing is accurate and complete, implementing up-to-date user training programmes and adherence to approved codes of conduct.

On data privacy legal and regulatory requirements 100% of the respondents indicated that they fully complied with the following principles; seeking patients consent before patient data is shared, using patient data for limited purposes only, patient data minimization, alignment of legal requirements for data retention with health facilities data retention schedules, observation of data processing requirements relating to minors and requirements for transfer of data out of Kenya.

However, on data privacy legal and regulatory requirements, 36% of the respondents disagreed that data is lawfully, fairly and transparently processed due to the fact that patients lacked transparency of how their data is processed. 85 % of the respondents disagreed that patients are clearly informed before their data is shared. Further discussions confirmed that in as much as health facilities seek patient consent in advance, they do not inform them each and every time their data is shared. An example is data shared with insurance companies or for emergency purposes. 79% of the respondents disagreed that they have notified the regulator on data breaches.

On achievement of data privacy KPIs, 100% of the respondents indicated that they successfully achieved regulatory KPIs in terms of customers complaints escalated to the regulator and breaches experienced. 91% successfully achieved mean time to initiate a response to a data breach incident, 88% successfully achieved number of

privacy breach complaints by customers, 88% successfully achieved percentage of solutions with encryption, anonymization, or pseudonymization capabilities and 82% successfully achieved percentage of organizational budget dedicated to privacy. On the other hand, some of the health facilities indicated that they had not achieved their KPIs in the following aspects; 36% did not complete Privacy Impact Assessments (PIA) in a timely manner, 27% did not meet their expected staff privacy training numbers and lastly, 24% did not meet their expected privacy internal audit score or rating.

Lastly, the top five challenges experienced by health facilities in adoption of data protection and privacy were indicated as ever-changing tough regulatory environment in healthcare (100%), fast pace of digital innovation and transformation (100%), increased interconnection and data sharing with third parties (100%) and increase in cyber threats, attacks and crime (100%). 76% of the respondents agreed that business cost-reduction or optimization requirements were a challenge.

CHAPTER FIVE: SUMMARY, CONCLUSION AND RECOMENDATIONS

5.1 Introduction

This section looks at the summary of findings, conclusions, recommendations, limitations drawn from the study and suggestions for further research.

5.2 Summary of the Findings

The study conducted an evaluation of information security strategies implemented by health facilities in Nairobi and proposed appropriate methods to ameliorate patient data privacy. Majority (89%) of the respondents' health facilities were using customised health information management systems and performed both the data controller and processor roles. The respondents' job titles varied from medical officer in charge of facility, health records officer to system administrator. The conclusions based on analysis of the respondents' data significantly improved the credibility of the research finding suggesting that majority of the respondents had the necessary background and knowledge.

The study identified a number of opportunities for the participating health facilities as pertains to their information security strategies. Opportunities identified on information security governance and risk management included; appointment of dedicated information security leaders, implementation of a risk-based approach in prioritising programs, allocation of appropriate resources and regular testing for the adequacy of information security measures. Compliance opportunities identified by the study included enhanced independent external audits or assurance and comprehensive timely incorporation of applicable legal and regulatory frameworks.

The study confirmed that generally, the health facilities complied with data protection and privacy legal and regulatory requirements and identified a number of opportunities for the participating health facilities as pertains to performance of data privacy. These opportunities included adoption of privacy information classification, assurance of the entire data life cycle including data shared with third parties, it also identified opportunities to enhance transparency as pertains to patient data and to clearly inform patients before their data was shared. Further, it was clear that some of the health facilities desired to better achieve their data privacy key performance indicators (KPIs).

Data privacy KPIs that performed poorly included implementation of proactive, timely and continuous privacy impact assessments, staff training numbers and internal audit scores or rating. A notable finding of the study was that the facilities did not register any significant data breach occurrences contrary to observations made by studies of scholars like Rafeq (2019), KHSSP (2017).The study also appreciated the fact that such sensitive information might have been classified confidential or for limited internal use of the health facilities.

Key challenges experienced by the health facilities in adoption of data protection and privacy were; ever-changing tough regulatory environment, fast pace of digital innovation and transformation, increased interconnection and data sharing with third parties and increase in cyber threats, attacks and crime. Business optimisation or cost-reduction requirements were a challenge for some of the participating health facilities.

5.3 Conclusion

In keeping up with our times there are but only four words that completely embody this study, Coronavirus Disease 2019 pandemic. It's an understatement to say that with the COVID-19 pandemic, health facilities information systems and their underlying technologies have undergone significant transformation. It has been clearly seen that these facilities are operating in a highly sensitive, competitive, turbulent, innovative and digital environment. The extent to which these systems have aided the health sector and the Kenyan Government in managing this pandemic is evident. Information privacy and security are mandatory principles regulating system development and procedures that support the Government of Kenya national e-health strategy.

It can therefore be argued from the study findings that health facilities have become more reliant on information systems and are subsequently, more susceptible to security challenges. Cyber criminals thrive on distractions and opportunities such as the COVID-19 pandemic and healthcare data violations are likely to increase. Health facilities must therefore address these information security and data privacy risks to prevent patient harm and preserve the human life. Information security includes technical, managerial and operational measures. However, the human or user aspect of information security and data privacy have an immense effect on the achievement or failure of health facilities. As such health workers security awareness, lobbing and advocacy are key information security and patient data privacy strategies. Effective

implementation of information security and patient data privacy strategies enables resilience and significantly reduces disaster impact on health facility services. These strategies also enable regulatory compliance, patient confidence and patient care.

The study concluded that although the health facilities implemented robust information security strategies they did not achieve some of their data privacy requirements. The study did not register any significant patient data breach occurrences.

5.4 Recommendations from the Study

From the findings, it is evident that information security and patient data privacy are a critical sustainability and success factor for health facilities in Nairobi. The facilities should scrutinise and find solutions to the challenges identified by the study that might hinder full adoption of their information security and patient data privacy strategies. Health facilities can assure attainment of their business goals and objectives by aligning their information security, privacy and business strategies.

5.5 Limitation of the Study

The objectives of the research were achieved but with various limitations. The COVID-19 pandemic has seen health facilities implement bureaucratic procedures in relation to physical access to their facilities and provision of research data. In one instance, the researcher was asked attach their COVID-19 vaccination certificate to the data collection application. In another instance, the researcher was asked to pay an official fee but declined, and excluded the facility as none participating, since this contravenes the KHN- UON Ethics and Research Committee requirements.

Because of the confidentiality policy of some facilities, the respondents either did not answer the questionnaires or failed to give all the required information. This explains why the researcher was only able to receive a 76% response rate. The researcher made all efforts to assure the respondents that the information is only meant for educational purposes by presenting the letter of introduction and using the consent form to brief comprehensively.

Time taken and approvals required for any research associated with health facilities, even those not medical in nature, is a limitation. Following approval by the KHN-UON ERC, the researcher was unable to secure county health facilities approval due to

time limitation. The study therefore focused on some national, public and private health facilities.

Due to the sensitive nature of work some of the facility personnel were busy running their day-to-day activities and it was difficult to administer data collection. The researcher booked appointments and embraced the use of questionnaires filled in at convenient times and collected thereafter.

The research only focused on the respondents but ignored other employees whose role was critical in the implementation of information security and patient data privacy. This could have left out important information that was vital for the study.

5.6 Suggestions for further Research

The need for further research into information security and patient data privacy is compounded by the fact that privacy is a relatively new phenomenon in Kenya. The Kenya Data Protection Act having come into effect on 25 November 2019.

A similar study can be carried out to cover county health facilities not only in Nairobi but also those in other counties in Kenya.

The extent to which health facilities have implemented their health management information systems is another aspect that can be studied in the future. The research indicated that health facilities have implemented customised or personalised solutions. In some instances, facilities used their health management information systems to automate the entire patient journey but in others only part of the journey was automated.

REFERENCES

Abouelmehdi, K., Beni-Hessane, A. & Khaloufi, H. *Big healthcare data: preserving security and privacy.* J Big Data 5, 1 (2018). https://doi.org/10.1186/s40537-017-0110-7

Ada, S., Sharman, R., & Gupta, M. (2008). *Theories used in information security research: Survey and agenda. Handbook of Research on Social and Organisational Liabilities in Information Security*, 279–292. https://doi.org/10.4018/978-1-60566-132-2.ch017

Advisera. (2017). *Clause-by-clause explanation of ISO 27001.* https://iso9001mgtsystem.files.wordpress.com/2017/01/clause_by_clause_explanation_of_iso_27001_en-1.pdf

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). *Information Security Compliance in Organisations: An Institutional Perspective. Data and Information Management*, 1. https://doi.org/10.1515/dim-2017-0006

Ana-Maria, S., Bîzoi, M., & Filip, F G. (2010*). Audit for Information Systems* Security. Informatica Economica Journal, 14. https://www.researchgate.net/publication/43121542_Audit_for_Information_Systems_Security

Andreas, P., & Marit H. (2011) *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, unobservability, pseudonymity, and identity management.* TU Dresden and ULD Kiel, Tech. Rep. https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

Appari, A., & Johnson, M. E. (2010). *Information security and privacy in healthcare: current state of research. International Journal of Internet and Enterprise Management*, *6*(4), 279. https://doi.org/10.1504/ijiem.2010.035624

Asnar, Y., & Massacci, F. (2015). *A Method for Security Governance, Risk, and Compliance (GRC): A Goal-Process Approach* https://doi.org/10.1007/978-3-642-23082-0

Australian, D., & Index, P. (2016). Deloitte Australian Privacy Index 2016 Trust without borders "Privacy is an international conversation, particularly as information flows have become more complex, and established regulatory. 1–28. https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-australian-privacy-index-2016-100516.pdf

Barney, J. (1991). *Firm Resources and Sustained Competitive Advantage. Journal of Management*, 17(1), 99–120. https://doi.org/10.1177/014920639101700108

Barzilay, M. (2019). *IT Security Audit.* https://www.researchgate.net/publication/333682624_IT_Security_Audit

Blumberg, B., Cooper, D.R. & Schindler, P.S. (2005) *Business Research Methods. McGraw Hill, Berkshire*, 770. http://sutlib2.sut.ac.th/sut_contents/H139963.pdf

Borg and Crall (2006) *Research Methodology 1st edition, Oxford University Press.* https://www.coursehero.com/file/p7ujs00/31-chapter-three-Research-Methodology-31-Introduction-This-chapter-presents-the/

Bostrom, R., & Heinen, J. (1977). *MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. MIS Quarterly*, 1(3), 17-32. https://www.jstor.org/stable/248710

Brotby, W.K., & IT Governance Institute (ITGITM) (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd Edition Paperback. ISACA. https://csbweb01.uncw.edu/people/ivancevichd/classes/MSA%20516/Extra%20Readings%20on%20Topics/IS%20Governance/Info%20Security%20Governance.pdf

Brotby, W.K., & IT Governance Institute (ITGITM) (2008). *Information Security Governance: Guidance for Information Security Managers (the 'Work')* https://www.amazon.com/Information-Security-Governance-Guidance-Managers/dp/1933284730

Chesley, D. L., & Amitrano, M. (2016). *Resilience. A journal of strategy and risk*. https://www.pwc.ch/de/publications/2016/pwc_ceo_survey_resilience_e.pdf

Consolidated Technologies, Inc. (2019). Security Threats in HealthCare Systems. https://consoltech.com/blog/security-threats-healthcare-systems/

Creswell, J.W., & Plano Clark, V. (2007). *Designing and conducting mixed methods research. Thousand Oaks, CA: Sage.* https://journals.sagepub.com/doi/abs/10.1177/1094428108318066

Da Veiga, A., & Eloff, J. H. P. (2007). *An information security governance framework.* http://130.18.86.27/faculty/warkentin/securitypapers/Leigh/ZafarClark2009%20Other%20References/DaVeigaEloff2007_ISM24_InfoSecGovncFramework.pdf

Deloitte. (2019). Banking spotlight Global risk management Executive summary. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-global-risk-management-survey-banking-spotlight.pdf

Dentons Hamilton Harrison & Mathews. (2019) New law – the Data Protection Act https://www.dentonshhm.com/en/insights/alerts/2019/november/13/new-law-the-data-protection-act

DLA Piper. (2017). *Data Protection Full Handbook.* (April 2017). https://blogs.dlapiper.com/privacymatters/data-protection-day-2017/

ECRI Institute. (2015). *Wrong-Record, Wrong-Data Errors with Health IT Systems*. *ECRI Institute PSO*, *7*(2), 1–10. https://www.ecri.org/Resources/In_the_News/PSONavigator_Data_Errors_in_Health_IT_Systems.pdf

Force, N. C. S. S. T. (2004). *Information Security Governance: A Call to Action. Corporate Governance Report*, (April), 49. https://library.educause.edu/resources/2004/1/information-security-governance-a-call-to-action

Fortes B. V. (2016). *The Right to Privacy and Personal Data Protection in Brazil: Time for Internet Privacy Rights? Brussels Privacy Hub. Working Paper. Vol.2.No 5.* February 2016. https://www.academia.edu/22477201/the_right_to_privacy_and_personal_data_protection_in_brazil_time_for_internet_privacy_rights

GrantThornton, & Territoriale, R. A. (1990). *IT Audit Manual*. 37–54. https://www.worldcat.org/title/grant-thornton-audit-manual/oclc/731717116

Hai, N. K., Lawpoolsri, S., Jittamala, P., Huong, P. T. T., & Kaewkungwal, J. (2017). *Practices in security and confidentiality of HIV/ AIDS patients' information: A national survey among staff at HIV outpatient clinics in Vietnam. PLoS ONE*, *12*(11), 1–16. https://doi.org/10.1371/journal.pone.0188160

Hachiya, H. (2005). *Medical Information Security. Journal of Medical Ultrasonics = 超音波医学*, *32*(6), 503–504. https://www.researchgate.net/publication/229046598_Medical_Information_Security/citation/download

Haumann, M. (2015). Social Media & Privacy: A Facebook Case Study. https://www.researchgate.net/publication/294836170_Social_Media_Privacy_A_Facebook_Case_Study

Henning, E., Van Rensburg, W. & d Smit, B. (2004) *Finding Your Way in Qualitative Research*. Van Schaik Publishers, Pretoria. https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1140852

HIPAA. (2019) Causes of August 2019 *Healthcare Data Breaches.* https://www.hipaajournal.com/august-2019-healthcare-data-breach-report/

HIV.gov. (2018). The Difference between Security and Privacy and Why It Matters to Your Program. https://www.hiv.gov/blog/difference-between-security-and-privacy-and-why-it-matters-your-program

Hong, K.-S., Chi, Y.-P., Chao, L., & Tang, J.-H. (2003). *An integrated system theory of information security management. Information Management Computer* Security, 11, 243–248. https://doi.org/10.1108/09685220310500153

Horne, R. (2017). Governing cyber security risk: it's time to take it seriously. (January). https://www.pwc.co.uk/cybersecurity/sevenprinciples

Intel Corporation. (2011). Healthcare Security: User Experience, Compliance, and Risk. https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/healthcare-security-user-experience-compliance-and-risk.pdf

International Telecommunication Union -ITU. (2018). *Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity. NATO Cooperative Cyber Defence Centre of Excellence Report*, 76. https://www.itu.int/pub/d-str-cyb_guide.01-2018

ISACA. (2020). Privacy beyond compliance (the "work"). https://www.isaca.org/resources/news-and-trends/industry-news/2020/three-ways-your-approach-to-privacy-is-at-risk

Ismail, S., Sitnikova, E., & Slay, J. (2014). Using integrated system theory approach to assess security for SCADA systems cyber security for critical infrastructures: A pilot study. https://doi.org/10.1109/fskd.2014.6980976

IT Governance Institute (ITGITM). (2008). *Information Security Governance: Guidance for Information Security Managers.* http://www.csun.edu/~yz73352/657/sent-0710/InfoSec-Guidance-for-Mgrs-Research-21May08.pdf

Jeimy, C. (2014). *Privacy and Information Security: The Territorial Challenges*. https://iapp.org/news/a/privacy-and-information-security-the-territorial-challenges1/

Kamau, W. & Kisika, S. (2019) Kenya's Health Structure and The Six Levels of Hospitals -Reporting on Good Governance in Kenya - RoGGKenya. https://actionfortransparency.org/kenyas-health-structure-and-the-six-levels-of-hospitals-roggkenya/

KEMRI.(2019). Towards Universal Health Coverage in Kenya : Are We on the Right Path? HERU Policy Brief, (January). Retrieved from https://kemri-wellcome.org/zp-content/uploads/2019/04/200-measuring-progress-towards-universal-healthcare-coverage.pdf

Kenya Healthcare Federation.(2021)The role of Information Communication and Technology in achieving Universal Health Coverage. Retrieved from https://khf.co.ke/blog/2021/01/07/ict-for-efficient-health-delivery/

Kerlinger, F. N. (1979) Behavioural Research: A Conceptual Approach. New York: Holt, Rinehart, and Winston, 1979. 336 22 xi pp. $12.95. Educational Researcher. 1979;8(10):22-24. https://journals.sagepub.com/doi/abs/10.3102/0013189X008010022

KHSSP. (2017). Transforming Health: Accelerating attainment of Health Goals: The Kenya Healthcare Sector Strategic and Investment Plan – KHSSP July 2012 –

June 2017. Ministry of Medical Services and Ministry of Public Health & Sanitation. https://www.who.int/pmnch/media/events/2013/kenya_hssp.pdf

Killmeyer, J. (2006). *Information Security Architecture. Information Security Architecture,* 1–23. https://doi.org/10.1201/9780203488751.ch1

Kitheka, P. M. (2013). *Information Security Management Systems in Public Universities in Kenya: A Gap Analysis Between Common Practices and Industry Best Practices*. http://erepository.uonbi.ac.ke/handle/11295/56607

Kiura, S. M. & Mango, D. M. (April, 2017). *Information Systems Security Risk Management Model in Kenya Private Chartered Universities. European Journal of Computer Science and Information Technology*,5(2), pp. 1-15. ISSN: 2054-0965 https://www.eajournals.org/wp-content/uploads/Information-Systems-Security-Risk-Management-ISSRM-Model-in-Kenyan-Private-Chartered-Universities.pdf

Krag, B. (2006). Guidance for Boards of Directors and Executive Management Guidance for Boards of Directors and Executive Management. https://csbweb01.uncw.edu/people/ivancevichd/classes/MSA%20516/Extra%20Readings%20on%20Topics/IS%20Governance/Info%20Security%20Governance.pdf

Kweri, J. M. (2013). Determinants of Data Security in Management Information Systems: Case Study of Commercial Banks in Nairobi, Kenya. https://ir-library.ku.ac.ke/handle/123456789/7121

Melek, A. (2009). Protecting what matters: The 6th annual global security survey. Deloitte Touche Tohmatsu, 60. https://www.iasplus.com/en/binary/dttpubs/2009securitysurvey.pdf

Ministry of Medical Services, & Ministry of Public Health and Sanitation. (2011). *Kenya National e-Health Strategy 2011-2017*. Retrieved from http://publications.universalhealth2030.org/uploads/kenyanation_ehealth_strategy.pdf

Moffit, R. E., & Steffen, B. (2017). Health Care Data Breaches: A Changing Landscape. Maryland Health Care Commission, (December). https://mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT_DataBreachesBrief_Brf_Rpt_090717.pdf

Mugenda, M. O. & Mugenda, G. A. (2010). Social Science Research: Theory and Principles. Nairobi: Applied. http://www.journalijar.com/uploads/877_IJAR-4007.pdf

Muhamad Khairulnizam, Z., Mohamad Noorman, M., Mad Khir Johari, A. S., & Norizan, A. (2018). Theoretical Modelling of Information Security: Organisational Agility Model based on Integrated System Theory and Resource Based View. *International Journal of Academic Research in Progressive*

Education and Development, *7*(3), 390–400. https://doi.org/10.6007/IJARPED/v7-i3/4379

Murphy, S. P. (2015). *Healthcare Information Security and Privacy. New York, United States: McGraw-Hill*. https://www.barnesandnoble.com/w/healthcare-information-security-and-privacy-sean-murphy/1124320957

Nelson, R. R., & Romer, P. M. (2009). Science, economic growth, and public policy. *The Economic Impact of Knowledge*, pp. 43–60. Retrieved from https://doi.org/10.1080/05775132.1996.11471873

Njuguna, D., & Wanjala, P. (2019). *A Case for Increasing Public Investments in Health. Ministry of Health Policy Brief*. https://www.health.go.ke/wp-content/uploads/2019/01/Healthcare-financing-Policy-Brief.pdf

Nyaga, B. N. (2016). *Information Security and Delivery in Health Sector: Case Study of Chogoria Hospital*. http://erepository.uonbi.ac.ke/bitstream/handle/11295/98874/Nkatha%20_Information%20Security%20And%20Service%20Delivery%20In%20Health%20Sector%20Case%20Study%20Of%20Chogoria%20Hospital.pdf?sequence=1

Nyawanga, J. O. (2005). *Meeting the Challenge of Cyber Threats in Emerging Electronic Transaction Technologies in Kenyan Banking Sector*. http://erepository.uonbi.ac.ke/bitstream/handle/11295/94405/Nyawanga%2C%20James%20O_Meeting%20the%20challenge%20of%20cyber%20threats%20in%20emerging%20electronic%20transaction%20technologies%20in%20in%20Kenyan%20banking%20sector.pdf?sequence=1&isAllowed=y

O'Brien, J. A., & Marakas, G. (2011). *Management Information Systems. Paperback, McGraw-Hill Higher Education.* https://www.mheducation.com/highered/product/management-information-systems-o-brien-marakas/M9780073376813.html

Orshesky, C. (2003). *Beyond technology - The human factor in business systems. Journal of Business Strategy*, 24, 4, 43-47 https://www.researchgate.net/publication/247620822_Beyond_technology_-_The_human_factor_in_business_systems

Privacy International. (2018). *The Keys to Data Protection: A guide for policy engagement on data protection*, (August), 100. https://privacyinternational.org/sites/default/files/201809/Data%20Protection%20complete.pdf

Privacy International. (2019). *State of Privacy Kenya | Privacy International*. https://privacyinternational.org/state-privacy/1005/state-privacy-kenya

PricewaterhouseCoopers. (2017). Consumer Intelligence Series: Protect.me. http://www.czechmarketplace.cz/news/consumer-intelligence-series-protect-me

PricewaterhouseCoopers. (2017). PwC Risk in Review 2017. (April). https://www.pwccn.com/en/risk-assurance/publications/ra-managing-risk-from-the-front-line-2017-risk-in-review-study.pdf

PricewaterhouseCoopers. (2019). Elevating internal audit's role: The digitally fit function. *2019 State of the Internal Audit Profession Study*. https://www.pwc.com/us/en/services/consulting/risk-regulatory/library/internal-audit-transformation-study.html

PricewaterhouseCoopers. (2019). *GRC enablement solution: Integrating your Risk Management and Internal Audit functions through digitisation.* https://www.pwc.com/sg/en/risk-assurance/assets/grc-enablement-solution-2019.pdf

PricewaterhouseCoopers. (2020). *23rd Annual Global CEO Survey. Navigating the rising tide of uncertainty. PwC, 1–49.* https://www.pwc.com/ks/en/publications/ceosurvey/Kosovo%20Annual%20CEO%20Survey%20Report.pdf

Rafeq, A. (2019). COBIT Design Factors: *A Dynamic Approach to Tailoring Governance in the Era of Digital Disruption. ISACA industry news.* https://www.isaca.org/resources/news-and-trends/industry-news/2019/cobit-design-factors

Rhee, H.-S., Kim, C., & Ryu, Y. (2009). *Self-efficacy in information security: Its influence on end users' information security practice behaviour. Computers & Security*, *28*, 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Risk Based Security. (2020). *2020 Q1 Report Data Breach QuickView. 2020 Q1 Report Data Breach QuickView*. Retrieved from https://pages.riskbasedsecurity.com/en/2020-q1-data-breach-quickview-report

Serianu, & Paladion. (2016). *Nigeria Cyber security report 2016. United States International University - Africa, 1–60.* https://www.serianu.com/downloads/NigeriaCyberSecurityReport2016.pdf

Sirma, J., Muiru M. & Kipchillat C. (2014). *Impact of Information Security Policies on Computer Security Breach Incidences in Kenyan Public Universities, 4(9),* 42–50. https://www.semanticscholar.org/paper/Impact-of-Information-Security Policies-on-Computer-Sirma Muiru/3992d131877f5d59335f8c6848757dca9779c0da

Singh, B., & Ghatala, M. H. (2016). *Risk Management in Hospitals Risk Management in Hospitals.* (February). https://doi.org/10.7763/IJIMT.2012.V3.266

Sneha, P. (2017). *Five added benefits of GDPR compliance. Privsec.* https://www.grcworldforums.com/gdpr/five-added-benefits-of-gdpr compliance/15.article

Task Force Health Care. (2016). Kenyan Healthcare Sector; opportunities for the Dutch Life Sciences & *Health Sector. Kenyan Healthcare Sector, 86.* http://khf.co.ke/wp-content/uploads/2018/03/2016-Kenyan-Healthcare-Sector-Report.pdf

Trist, E. L. (1981). *The sociotechnical perspective: the evolution of sociotechnical systems as a conceptual framework and as an action research program In A. H.Van De Ven & W. F. Joyce (Eds.). Perspectives on organization design and behaviour*. New York : John Wiley & Sons , 19-75.

United Nations General Assembly. (1990). *Guidelines for the Regulation of Computerized Personal Data Files. United Nations General Assembly Resolutions*, 45(95). https://www.refworld.org/pdfid/3ddcafaac.pdf

Verizon. (2019) 2019 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/dbir/2019/results-and-analysis/

Waithaka, S. (2016). *Factors Affecting Cyber Security in National Government Ministries in Kenya.* http://erepository.uonbi.ac.ke/bitstream/handle/11295/100423/Waithaka_Factors%20Affecting%20Cyber%20Security%20In%20National%20Government%20Ministries%20In%20Kenya.pdf?sequence=1

Wernerfelt, B. (1995). *The Resource-Based View of the Firm: Ten Years After. Strategic Management* Journal, 16(3), 171-174. http://web.mit.edu/bwerner/www/papers/TheResource-BasedViewoftheFirm-TenYearsAfter%20.pdf

Wikipedia Dictionary (2020). https://en.wikipedia.org/wiki/Dictionary

Woo, R. H., & Cudworth, R. (2018). *Stronger, fitter, better Crisis management for the resilient enterprise*. https://www2.deloitte.com/lu/en/pages/risk/articles/crisis-management-plan-resilient-enterprise.html

Zeng, X., Reynolds, R., & Sharp, M. (2009). *Redefining the Roles of Health Information Management Professionals in Health Information Technology*. 1–11. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2781729/

APPENDIX 1: DATA COLLECTION TOOL -QUESTIONNAIRE

INFORMATION SECURITY STRATEGIES AND PATIENT DATA PRIVACY AMONG HEALTH FACILITIES IN NAIROBI.

Health facility Code _____

SECTION A: GENERAL INFORMATION

1. Kindly indicate number of patients attended to per month in the facility _____

2. Does the facility have a Health Management Information System (HMIS)?
   YES **[ ]**
   NO **[ ]**

3. If NO, please briefly describe how patient records/ data is managed and secured?
   _____
   _____
   _____
   _____

4. Please tick all data protection/ privacy roles applicable to your health facility
   Data Controller **[ ]**
   Data Processor **[ ]**
   Data Controller and Processor **[ ]**

5. What is your job title? _____

SECTION B: INFORMATION SECURITY STRATEGIES

1. Does the facility have formally accepted health information security strategy?
   YES [ ]
   NO [ ]
2. What aspects of information security governance does the strategy take into consideration ? Tick all applicable
   Appoints a dedicated cybersecurity leader [ ]
   The cybersecurity leader is part of the top management [ ]
   Allocates dedicated and appropriate resources [ ]
   Identifies accountable and responsible persons [ ]

Caters for information security programmes/policies execution [ ]

3. What aspects of information security risk management does the strategy take into consideration ?

   A risk-based approach is adopted in prioritising programmes/policies [ ]
   Identifies critical information infrastructures and services [ ]
   Incorporates Privacy Impact Assessment (PIA) [ ]
   Adopts information classification [ ]
   Considers the entire information lifecycle [ ]
   Incorporates incident response, business contingency and disaster recovery [ ]
   Includes regular testing for the adequacy of information security measures [ ]

4. What aspects of information security compliance does the strategy take into consideration ?

   Incorporates a legal and regulatory framework [ ]
   Promotes the establishment of compliance mechanisms [ ]
   Incorporates continuous internal audit, monitoring and improvement [ ]
   Incorporates independent external audits and assurance [ ]

SECTION C: PERFORMANCE OF DATA PRIVACY

1. Does your health facility carry out a comprehensive risk assessment that recommends accountability measures and responsibility allocation?

   YES [ ]
   NO [ ]

2. Is patient data at rest and in transit protected by physical, logical, system and technical security safeguards?

   YES [ ]
   NO [ ]

3. Are all steps taken to eliminate errors and ensure that patient data processing is accurate, complete and up-to-date?

   YES [ ]
   NO [ ]

4. Do your patient data privacy control measures include implementation of user training programmes and adherence to approved codes of conduct?
   YES [ ]
   NO [ ]

5. What legal and regulatory aspects of data security and privacy, does your facility take into consideration ?
   Data is lawfully, fairly and transparently processed [ ]
   Patients are clearly informed before their data is shared [ ]
   Patients must consent before their data is shared [ ]
   Data is used for limited purposes only [ ]
   Data minimization is observed [ ]
   Data is only retained for the period originally and legally required [ ]
   Facility policy establishes patient data retention schedules [ ]
   Data processing requirements relating to a minor [ ]
   Requirements for transfer of data out of Kenya [ ]
   Regulatory notification and communication of breach [ ]

6. Kindly indicate which data privacy key performance indicators (KPIs) your facility has been able to successfully meet this year ?
   Percentage of organizational budget dedicated to privacy [ ]
   Timely Privacy Impact Assessment (PIA) completion rate [ ]
   Percentage of staff receiving privacy training [ ]
   Number of privacy breach complaints by customers [ ]
   Number of privacy breach complaints by the regulator [ ]
   On-time regulator notification for privacy breaches [ ]
   Results of privacy internal audits [ ]
   Mean time to initiate a response to a data breach incident [ ]
   Percentage of solutions with encryption, anonymization, or pseudonymization capabilities [ ]

SECTION D: CHALLENGES FACED WHEN IMPLEMENTING DATA PROTECTION AND PATIENT DATA PRIVACY

Kindly tick data protection and privacy adoption challenges that your health facility faces

Ever-changing tough regulatory environment in healthcare	[ ]
Fast pace of digital innovation and transformation	[ ]
Big data; managing high volumes of rich and sensitive data	[ ]
Reliance on devise workforce, with different backgrounds	[ ]
Reliance on devise third parties and outsources services	[ ]
Increased interconnection and data sharing with third parties	[ ]
Poor risk management, compliance and assurance processes	[ ]
Business cost-reduction or optimization requirements	[ ]
Lack of qualified staff in the market	[ ]
Poor user awareness, training and acceptance of systems	[ ]
System vulnerability- Insider access abuse	[ ]
System vulnerability- Outsider abuse	[ ]
Financial fraud and motivation	[ ]
Failure to keep up with software updates and patches	[ ]
Increase in Cyber threats - Cyber-crime – Cyber-attacks	[ ]

APPENDIX 2: LIST OF HEALTH FACILITIES IN NAIROBI

NO.	HEALTH FACILITY CODE	KEPH LEVEL	CATEGORY
1	HFC-001	Level 6	Hospital
2	HFC-002	Level 6	Hospital
3	HFC-003	Level 5	Hospital
4	HFC-004	Level 4	Hospital
5	HFC-005	Level 4	Hospital
6	HFC-006	Level 4	Hospital
7	HFC-007	Level 4	Hospital
8	HFC-008	Level 4	Hospital
9	HFC-009	Level 4	Hospital
10	HFC-010	Level 4	Hospital
11	HFC-011	Level 4	Hospital
12	HFC-012	Level 4	Hospital
13	HFC-013	Level 4	Hospital
14	HFC-014	Level 4	Hospital
15	HFC-015	Level 3	Nursing Home
16	HFC-016	Level 3	Medical Clinic
17	HFC-017	Level 3	Medical Center
18	HFC-018	Level 3	Medical Center
19	HFC-019	Level 3	Medical Center
20	HFC-020	Level 3	Medical Center
21	HFC-021	Level 3	Health Center
22	HFC-022	Level 3	Health Center
23	HFC-023	Level 3	Health Center
24	HFC-024	Level 3	Health Center
25	HFC-025	Level 2	VCT
26	HFC-026	Level 2	Medical Clinic
27	HFC-027	Level 2	Medical Clinic
28	HFC-028	Level 2	Medical Clinic
29	HFC-029	Level 2	Medical Clinic
30	HFC-030	Level 2	Medical Clinic
31	HFC-031	Level 2	Medical Clinic
32	HFC-032	Level 2	Medical Clinic
33	HFC-033	Level 2	Medical Clinic
34	HFC-034	Level 2	Medical Clinic
35	HFC-035	Level 2	Medical Clinic
36	HFC-036	Level 2	Medical Clinic
37	HFC-037	Level 2	Medical Clinic
38	HFC-038	Level 2	Medical Clinic
39	HFC-039	Level 2	Medical Clinic
40	HFC-040	Level 2	Medical Clinic

NO.	HEALTH FACILITY CODE	KEPH LEVEL	CATEGORY
41	HFC-41	Level 2	Medical Clinic
42	HFC-042	Level 2	Dispensary
43	HFC-043	Level 2	Dispensary
44	HFC-044	Level 2	Dispensary
45	HFC-045	Level 2	Dispensary
46	HFC-046	Level 2	Dispensary
47	HFC-047	Level 2	Dispensary
48	HFC-048	Level 2	Dispensary
49	HFC-049	Level 2	Dispensary