TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Faith Adesuwa Idialu 195041IVGM

INFORMATION SECURITY IN DIGITAL MENTAL HEALTHCARE IN NIGERIA

Master's thesis

Supervisors: Prof. Dr. Dr. Robert Krimmer, PhD

Melita Sogomonjan, MScEng

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Faith Idialu 195041IVGM

INFOTURVE DIGITAALSES VAIMSES TERVISHOIUS NIGEERIAS

Magistritöö

Juhendaja: Prof. Dr. Dr. Robert Krimmer, PhD

Melita Sogomonjan, MScEng

Tallinn 2021

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature, and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Faith Adesuwa Idialu

10.05.2021

Abstract

In Nigeria, mental health is scarcely the concern of the government as more health challenges are unique to a large group of the population than mental health. While the foregoing is not an excuse to neglect mental health, the challenges have become a national burden. Considering this situation, there has been an increase in advocacy to change this narrative of stigmatization, outdated legislation on mental health, and unavailability of mental healthcare. At the front line of this revolution are non-profit organizations. Their goal is to close mental health treatment gaps by using digital healthcare initiatives. While their efforts are reaching many groups, the sensitivity of mental health data and risks associated with digital technology such as data breaches have left users wondering about the privacy and confidentiality of their data. This study has been carried out to evaluate what information security measures are used by digital mental healthcare providers in the country to protect the privacy and security of users' data in their organization. The existing countermeasures and legislation on information security are discussed to improve digital health governance, while an interview is used to assess the current state of information security governance in questions about privacy and security of mental healthcare organizations in Nigeria.

This thesis is written in English and is 62 pages long, including 7 chapters and 4 figures.

Annotatsioon

Infoturve digitaalses vaimses tervishoius Nigeerias

Nigeerias on vaimne tervis vaevalt valitsuse mure, sest on rohkem tervisealaseid väljakutseid, mis on paljudele elanikkonnale ainulaadsed kui vaimne tervis. Kuigi unustamine ei ole vabandus vaimse tervise hooletusse jätmiseks, on väljakutsed muutunud riiklikuks koormaks. Seda olukorda arvestades on suurenenud propageerimine, et muuta seda häbimärgistamise narratiivi, vananenud õigusakte vaimse tervise ja vaimse tervishoiu mittekättesaadavuse kohta. Selle revolutsiooni eesotsas on mittetulundusühingud. Nende eesmärk on sulgeda vaimse tervise ravi lüngad digitaalsete tervishoiualgatuste abil. Kuigi nende jõupingutused ulatuvad paljudesse rühmadesse, on vaimse tervise andmete tundlikkus ja digitaaltehnoloogiaga seotud riskid, näiteks andmete rikkumised, jätnud kasutajad mõtlema oma andmete privaatsuse ja konfidentsiaalsuse üle. See uuring on läbi viidud, et hinnata, milliseid infoturbe meetmeid kasutavad riigi digitaalsed vaimse tervise pakkujad kasutajate andmete privaatsuse ja turvalisuse kaitsmiseks oma organisatsioonis. Olemasolevaid vastumeetmeid ja infoturvet käsitlevaid õigusakte arutatakse kui viisi, kuidas parandada digitaalset tervishoiujuhtimist, samal ajal kui intervjuud kasutatakse infoturbe juhtimise hetkeseisu hindamiseks Nigeeria vaimse tervise organisatsioonide privaatsust ja turvalisust puudutavates küsimustes.

Lõputöö on kirjutatud inglisekeeles ning sisaldab teksti 62 leheküljel, 6 peatükki ja 4 joonist.

List of abbreviations and terms

PII	Personal Identifiable Information
CIA	Confidentiality, Integrity, and Accessibility
PHI	Protected Health Information
MANI	Mentally Aware Nigeria Initiative
NHA	National Health Act
NDPR	Nigeria Data Protection Regulation
ISG	Information Security Governance
HDG	Health Data Governance
RBAC	Role-Based Access Control
NIST	National Institute of Standards and Technology
CPC	Consumer Protection Council of Nigeria
PBR	Patient’s bill of right
ISO	International Security Organization
SDG	Sustainable Development Goals
ISCT	Information Security Control Theory

Table of contents

List of figures

1 Introduction

One of the benefits of information and communication technology (ICT) is giving otherwise unreachable groups in most developing countries access to healthcare information and services. Unlike traditional communication channels, information systems are more prone to data breaches (Cheng & Yao, 2017) causing healthcare organizations who want to reach their users to do so in a safe and secure technological environment. This responsibility of securing a user's data is examined within a digital non-profit mental health organization in Nigeria. This thesis examines the different socio-technical mechanisms employed in a non-governmental healthcare organization to protect mental health data in Nigeria.

1.1 Background

The Federal Republic of Nigeria, the most populous country in West Africa has a population of more than 200 million people (UNFPA, 2020). One of the challenges that the majority of its population faces is a lack of access to healthcare services especially as government-owned healthcare facilities are overburdened and underfunded. According to a study by the World Health Organization, health care is both inaccessible and unavailable in Nigeria's primary health care system (WHO, 2006).

Mental health in Nigeria has remained the least funded part of the health sector (Abdulmalik et al., 2016) and only a few government-owned mental facilities are available (Anyebe et al., 2019). At the moment there are only 8 federal government-owned mental health hospitals in the country. When compared, the availability of mental healthcare to almost 30% of the population suffering from mental illness (Onyemeukwe, 2016), it is clear that the problem of mental health in the country needs to be addressed. Moreover, mental illness has long been stigmatized in Nigerian society (Onyemeukwe, 2016), affecting the ability of many to openly seek help.

The Nigerian government has in recent times shown its interest in mental health by adopting the World Health Organization's recommendation of providing mental health services at the primary health care level. 'To determine the effectiveness of the former initiative, Anyebe et al. (2019) carried out a study to determine the current state of mental health services at the primary healthcare level in Northern Nigeria. The study revealed that primary healthcare coordinators interviewed were unaware of mental health services being offered to people. This raises many questions because mental health in primary healthcare itself is largely unavailable to many, not to mention the research result above.

1.2 Problem statement

Nigeria as being referred to as a country “in the process of saving her face in cybercrimes” (Odumesi, 2014, p. 116). Six years later, the country is being touted as a leading nation in cybercrimes (Garba & Bade, 2021). In October 2019, a research result of unsecured health databases in the world showed that the medical data of over 80,000 Nigerians were at risk because they were insecure and available online (Cybersecfill, 2019). This example of the magnitude of data breaches can affect both users and healthcare organizations by causing reputation damage to the institution and can affect the disposition or finances of people whose data are exploited in a data breach. Khan and Hoque (2016) assert that because digital health data of patients features protected health information (PHI), they have become the predominant interest of cybercriminals. Additionally, Verizon’s 2018 report on PHI data breach revealed that almost 60% of data breaches within healthcare were initiated by insiders (Widup, 2018). To ensure that a patient's PHI is protected against data breaches or exploitation by malicious actors, healthcare providers have the responsibility of implementing information security controls and policies. These controls and policies can guide the collection, storage and exchange of health data that guides the collection, storage and exchange of health data.

In a debate by experts brought together by the University of Manchester’s centre for health informatics and organized by Connected Health Cities, a poll showed that 75% of the audience thought that mental health data were more sensitive than physical health data (CHC, 2018). The sensitivity of mental health data requires healthcare organizations to handle user’s data workers to the utmost care. Managing the enormous amount of health data is often a challenging task in healthcare (Pandey et al., 2020) largely because health information is often exchanged within different actors in an organization and some cases data exchange can be with an external entity.

Healthcare providers can lose the trust that exists between them and users of unauthorized access or disclosure of personal health information leads to data exfiltration (Oloyede, 2018). Although the country has created several legislations on data privacy and security in healthcare organizations, the implementation has been challenging, leaving personal health data at an all-time risk (Seh et al., 2020). The lack of interest in information security and data security training among digital healthcare workers is one of the challenges facing digital health data (Bennett et al., 2010). Although technical solutions for data security exist, the role of employee behaviour and compliance to information security policies that guide technical controls are ones that organizations depend on to succeed (Aurigemma & Panko, 2012).

1.3 Research questions

There is a limited number of existing literature on information security within the healthcare industry in Nigeria. The majority of the available literature on information security in Nigeria is focused on the financial industry, largely because cybercriminals mostly target customers of banks and financial institutions.

Globally, digital mental health is a relatively evolving field within scholarly work and Nigeria is no exception. In writing up this chapter, I use privacy and confidentiality within information security in digital healthcare interchangeably. To achieve information security, efforts have to be both technical and human inclined. According to Erceg (2019, p 123), "Information security refers to the safeguarding of computer systems and data against unauthorized access, use, disclosure, interruption, alteration, perusal, inspection, recording, or destruction". The requirement for making these information systems security is the basic requirement to ensure the security of mental health data. Additionally, the safeguarding of information takes both technical mechanisms like firewall and expertise such as trained employees.

Information security in this work is used to refer to the measures that can protect the privacy and confidentiality of personal health information within the custody of digital mental healthcare providers. The goal of this thesis is to identify the information security posture of digital mental health organizations in Nigeria.

The research questions that this work seeks to address are:

1. What threats would most likely affect your organization?
2. What measures are in place to protect user's data within your organization?
3. What techniques are used to ensure employee compliance to existing information security measures?

2 Literature overview

In this chapter, an exploratory approach is used to review the existing literature on information security within the healthcare sector. This chapter provides the theoretical lens through which information security can be enhanced within an organization from a sociotechnical perspective.

2.1 Digital mental health platforms

Digital healthcare refers to the use of ICT like m-health to provide timely and quality healthcare services (Murray et al., 2016). Due to the increase in mobile technology adoption in developing countries, digital health has notable potential to increase the situation of healthcare because it eliminates the barriers to healthcare services (WHO, 2019). With the use of technological devices, citizens can access healthcare services provided by different organizations without travelling to the healthcare centres (Seh et al., 2020).

The Internet penetration rate in Nigeria increased to 101, 484%, with an estimate of over 203 million internet users as of the year 2020 (World statistics, 2020). The high number of internet users makes the use of digital mental health solutions a viable option for addressing the country's mental health crisis. In recent years, there has been an emergence of digital health platforms for mental health counselling, medical consultations and health monitoring in Nigeria (Onyemelukwe, 2018).

According to Wise (2017) digital mental health involves the application of ICT to aid and improve the delivery of mental health treatments, initiatives, and follow-ups. Although the use of the digital medium for mental health is relatively new, it has been a significant way to close treatment gaps in mental health in developing countries (Carter et al., 2020) Additionally, digital mental health platforms carry the potential to broaden access to mental healthcare which on a global scale will make people living with mental challenges have a better quality of life (Torous et al., 2019).

Within digital healthcare services, health organizations use several information systems like online databases to collect, retain and exchange users’ mental health information with necessary actors. These systems for managing data in themselves pose certain risk like technical / network disruptions to the information environment of healthcare organizations (Ayatollahi & Ghazal, 2017). These challenges create the need for implementing information security measures in healthcare organizations.

2.2 Information security in digital mental health

Personal identifiable information (PII) is a common denominator in any healthcare organization as it forms the basic identifiable information that healthcare organizations collect about their users before gaining knowledge of their health information. PII links the health information of a user to other facets of their lives like their contact or financial information. Securing both PII and personal health information entails protecting the privacy and confidentiality of digital mental health users by healthcare organizations providing digital mental health services (Househ et al., 2014).

Because mental illnesses are heavily stigmatized, prioritizing security issues within various information and communication technology-enabled interventions to combat mental illness is critical and has become a top priority for healthcare organizations (Bennett et al., 2010). Digital health information security is largely concerned with restricting unauthorized and inappropriate access to protected health data (Appari & Johnson, 2010).

Keeping patients' information private within the health sector is not a new responsibility introduced by technology. The medical profession has always been held to higher standards of information privacy by the Hippocratic oath that guides the medical profession. The inclusion of data safety and privacy as part of the standard for the evaluation of mobile mental health initiatives has been recommended by Torous et al. (2019). A common model used to assess the information security goal of an organization is the confidentiality, integrity and availability model, known as the CIA triad. Each component of the CIA triad is outlined below.

2.2.1 Confidentiality

Privacy has an impact on mental health as it creates a sense of trustworthiness in healthcare providers (George & Bhila, 2019). Concerns about the privacy of protected health information arise because of the increase in privacy violations around the world (Chan & Saqib, 2021). This affects the level of trust that individuals can place on healthcare organizations particularly those within the non-profit space. Ideally, users might be concerned about sharing their data with other organizations that NGOs receive funding from. There is no telling what the data can be used for, moreover, it exposes the users when data is passed from one organization to the other. Confidentiality is taken up by the organizations in charge of the users' data to protect it (Fernandes et al., 2010).

Most healthcare organizations have a privacy statement before the collection of data from their patients and regulations like the National Health Act (NHA) of Nigeria ensures their accountability. Maintaining the privacy and security of data requires a coordinated strategy that consists of employees at all levels including management and support teams in an organization (Renaud & Goucher, 2012).

2.2.2 Integrity

Data integrity is a major concern of healthcare organizations (Pandey et al., 2020). The sensitive nature of mental health data requires that data integrity be maintained in healthcare organizations. The information security risks present to both healthcare users and healthcare institutions requires a relationship between the available human capacity and data integrity strategies (Hult & Wynn, 2019). Where one of these is lacking, digital health data are at a higher risk. As with all sociotechnical endeavours, healthcare organizations have to invest efforts in monitoring data integrity, particularly because health data are often exchanged and accessed by multiple personnel in an organization. If data provided on a specific user are tempered with, there could be a delay in treatment given or even a misappropriation of treatments (Pandey et al., 2020), leaving both the user and healthcare provider vulnerable. So, organizations have the extra responsibility of ensuring compliance to data integrity measures but beyond this is the understanding of what data integrity represents. Studies have shown that organizations can enhance data integrity by including an integrity monitoring mechanism within their information system (Jaeger & Eckhardt, 2018; Hult & Wynn, 2019; Saminu, 2019).

The framework for managing data integrity proposed by Saminu (2019) shows how data integrity can be achieved by gaining management support as well as implementing both preventive and deterrent actions such as (i) information environment security, (ii) code of ethics, (iii) disincentive certainty, (iv) specialized security software, (v) operating system security, (vi) database management security and (vii) fourth-generation security software.

2.2.3 Availability

In healthcare, data availability is critical to service provision. When a security issue affects the availability of information, it can affect service delivery.

Another lens to which availability can be viewed is ensuring that users health data are safeguarded against natural or man-made disasters (Olanrewaju et al., 2013). To avoid this there is the need to create a backup of the data and also have a strategy to continue operation when any of these incidents occur. The availability of data regarding the security and privacy of data also addresses the need for only authorised users to have access to the available data. In this case, the use of authentication mechanisms like the password is encouraged in mental health organizations. This is also included within the security policies of the organization to ensure every staff knows what is expected of them in creating passwords, the use of office owned devices and authentication mechanisms for data exchange both internally and externally.

2.3 Organizational threat landscape

The National Institute of Standard and Technology (NIST) defines a threat as an event or condition that has the potential for causing asset loss and the undesirable impact and consequences from such loss (Ross et al., 2018). Threat identification is usually carried out in different organizations to determine what threats are unique to their information environment. Carrying out a threat analysis is compulsory in health information systems if they are to succeed in protecting health data (Samy et al., 2010).

The information collected by healthcare organizations varies from the patient's health condition to other personal information which can include payment information that can be of interest to attackers. The need for managers and system administrators to be aware of the threats to information assets and data that their organization is faced with has been emphasized by Whitman (2004). Additionally, the author surveyed top information security executives to identify the main threats to information security as the following:

(i) malicious software, (ii) human error, (iii) espionage, (iv) failure of hardware, (v) employee acts of thefts (vi) vandalism (v) forces of nature (vi) service deviations (vii)technology obsolescence (vii)exposure of trade secrets (viii) extortion of information.

In research to identify the threats to health information systems, Samy et al. (2010) carried out an identified five threat categories (i) hardware failures/errors, (ii) software failures/errors, (iii) technological obsolescence, (iv) acts of human errors/failures, (v) power failure or loss. Although the frequency of each of these threats differ, knowing where threats can develop gives healthcare organizations a road map on how to tackle them. Because threats exist both in the internal and external environment of healthcare organizations, a threat actors' motive, available resources, technical skills and access points determine the type of security control needed (NRC, 1997).

The healthcare sector notably suffers from more internal threats than external threats; almost 60% of data breaches in healthcare organizations were caused by internal actors (Curtis, 2018). The alarming level of insider threats calls for more socio-technical security measures within a healthcare organization.

2.4 Healthcare data breaches

Between 2005 to 2019, over 240 million individuals were affected by data breaches in healthcare (Seh et al., 2020). Verizon's 2018 data breach results show that the healthcare sector had a higher number of breaches in comparison to other industries (Verizon, 2018). Before a data breach occurs, there is usually the presence of a human actor that intentionally or unintentionally facilitates it. Unethical or non-compliance to information security policies by employees can create an avenue for privacy and confidentiality breaches (Jaegar & Eckhardt, 2018). From a healthcare organization's standpoint, Berryman et al. (2013) define the constitutive makeup of a breach in health data as an event that occurs when medical personnel or employee or outsider accesses protected health information that they have no medical clearance and purpose for. Data breaches can lead to the release of protected health information or the tempering of health data.

To reduce privacy breaches in healthcare organizations, Berryman et al. (2013) suggest that organizations implement an accountability mechanism. An accountability mechanism within an electronic health record tracks access and records any violation of the access-based requirement. This alert can generate reports that healthcare organization can use to demand accountability from employees.

Within the research on information security in digital healthcare, is a study carried out by Gajanayake et al. (2011) on information sharing in online health platforms. The researchers argue that the use of an accountability framework can assure patients of how their health information is shared securely with other healthcare professionals. The diagram below shows the fundamental components and functionality in an accountability framework adopted from the study by Gajanayake et al. (2011).

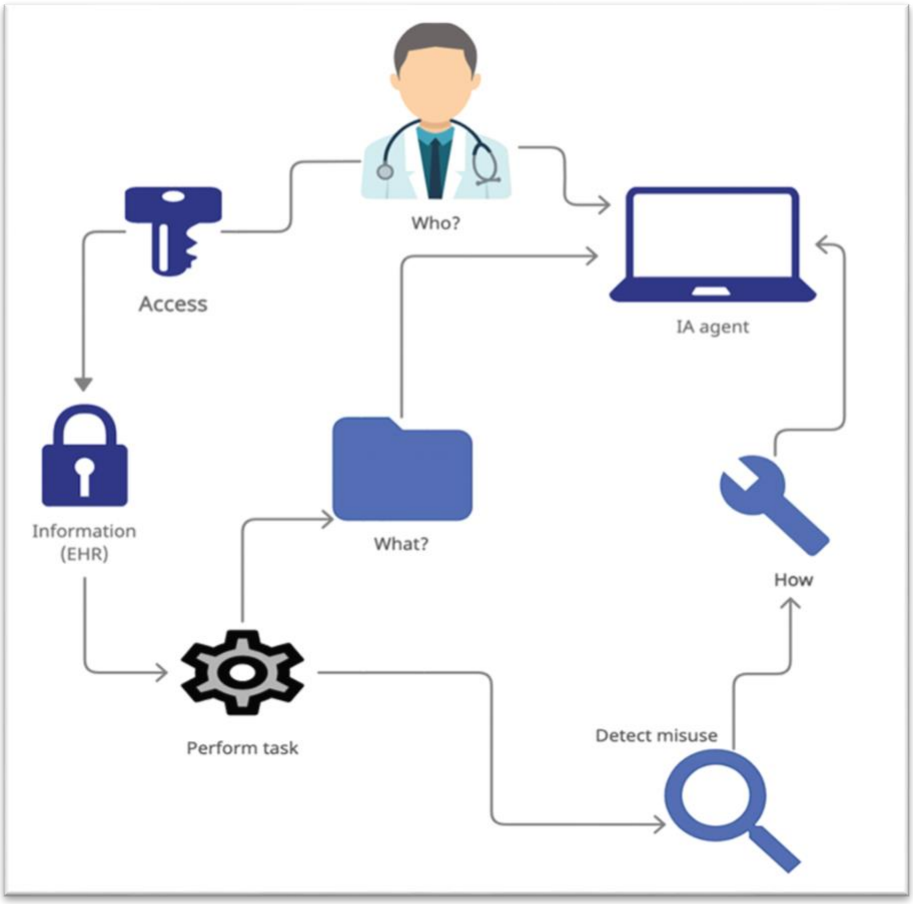

Figure 1. Components of an information accountability framework by Gajanayake et al., (2011)

The basic components can be embedded in a social network health sharing platform, where the accountability tool assesses the file or task. During the performance of the task, and the embedded sensor detects if there is any misuse and alerts the information accountability agent (IA agent). This type of layer of accountability can improve the security of digital mental health data in an organization because it goes beyond access-based roles to ensure that those with access do so within reasonable parameters.

Although designed for social networks, the accountability framework can reduce internal breaches within healthcare organizations as alerts generated can put healthcare workers on the raider before a data breach is exploited. Additionally, country or sector-related regulations provides healthcare organizations with procedures when a data breach occurs. For instance, Nigerian data protection regulation (NDPR) mandates data controllers to notify the national information technology development agency (NITDA) of data breaches within seventy-two hours of the breach (NDPR, 2019).

While reporting health data breaches is mandatory, there is a huge gap in compliance as most organizations in the country do not comply with it (Adeniran, 2021). This could be the reason why the documentation of health data breaches in the country is largely unavailable and the NDPR is only in its third year. Communication between healthcare providers and users over the internet (like in telemedicine & mobile health), there is a considerable amount of vulnerability to attacks particularly network attacks (Olanrewaju et al., 2013). In their study Olanrewaju et al. (2013) groups the attacks on telemedicine into active attacks or passive attacks. Figure 2 below has been modified to show the attack on telemedicine by the authors.

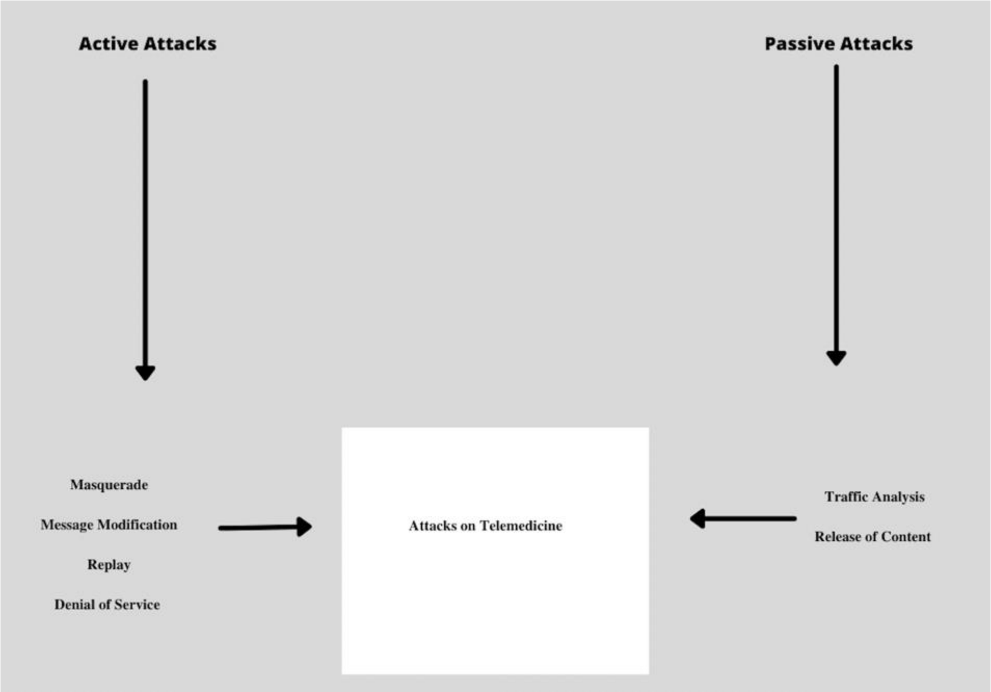

Figure 2. Attacks on telemedicine by Olanrewaju et al. (2013)

In an active attack, the objective of the threat agent is achieved via modification of the data or images or creating a loop to interrupt the transmission of information, on the other hand, a passive attack occurs when a threat agent can identify open ports so they can gain more information from the target. From the diagram, an active attack can lead to a denial of service while a passive attack leads to the release of confidential data held by the healthcare organization. Having an overview of how a threat actor operates can help healthcare organizations know what countermeasures to put in place to stop threat actors.

2.5 Information security countermeasures in healthcare organizations

The national information technology development agency of Nigeria (NITDA) introduced data protection guidelines in 2017. One of the principles in the data protection guideline is the responsibility of data controllers to implement the following to achieve information security: (i) technical protection from external threats, (ii) implement a firewall solution, (iii) adopt data encryption technology (iv) develop and implement information security policy, (v) integrate technical protection within emailing systems (vi) create staff training guides (NITDA, 2017). The organization expects the elements of this principle to be the minimal set of enforceable measures.

Information systems are used in healthcare organizations to carry out procedures, collect, store and exchange data (Tomšů,, 2020). These functions are critical to the operations of mental healthcare services. For healthcare organizations to thrive in a climate of constant cyber-attacks and data breaches, information security should be treated as an organizational culture and not just the responsibility of the IT team.

The threat of social engineering to organizations is exploited via employees. The preceding sections have discussed the threats within healthcare organizations and the actions that constitute data breaches. Insider and organizational threats can be addressed by implementing organizational policies that focus on information security training, technical security control, mechanisms for monitoring and communicating ethical information security (Peikari et al., 2018). These measures determine the security position of healthcare organizations (Peikari et al., 2018). The implementation of an information security program in an organization should consist of training/awareness, governance, technical and administrative controls (Page, 2017). These solutions for tackling information security in healthcare organizations are discussed below.

2.5.1 Information security policy

The first step towards managing information security in healthcare organizations is the creating of an information security policy (Singh et al., 2014). To achieve information security, healthcare organizations need a collaborative approach initiated from the strategic level of management to all levels of employees in the organization (Agrawal & Alharbe, 2019). It can also affect the culture of the organization because it makes all stakeholders aware of their responsibilities and penalties for non-compliance. For healthcare organizations to adequately ensure data protection, the use of an information security policy guides information assets and systems used in an organization.

Information security policy has been defined as a "document that contains the roles and responsibilities of employees and third parties within an organization, aimed at safeguarding the information assets at their disposal" (Bulgurcu et al., 2010, as cited by Chen et al., 2018, p. 314). There is no doubt that an information security policy is one of the tools that organizations are encouraged to adopt if they are to maintain the security of their information assets and the threats that employees can pose. An information security policy is usually the baseline document for ensuring that an organization has the necessary controls, guideline and ethical considerations to protect the organization from both internal and external threats (Hone & Eloff, 2002; Whitman et al., 2001).

2.5.2 Role-based access control model

The model of Role-Based Access Control (RBAC) stems from the foundation that different personnel within a healthcare institution have different job functions and level of interaction with patients. Therefore, access to the personal health information of patients should be assigned based on the need for such information.

A role is a structure that is used to authorize the properties of each subject (individual users). The authors refer to objects and transactions as fundamental concepts in RBAC, where the object refers to system resources and transaction is the operation that is performed on an object (Moyer & Abamad, 2001). RBAC incorporates differing tenets that aids the information security policy of an organization.

Defining the roles within organizations depends on the competence of each user, rules that determine where there are conflict of interest and the privileges given to administrators and users within the organization (Ferraiolo et al., 1995). One of the challenges of RBAC is that although different vendors have created rules for setting RBAC within their solutions, there has been a lack of standardization of RBAC in information systems (Sandhu et al., 2000). In an attempt to override this challenge, the National Institute of Standards and Technology (NIST) has made the first step by developing a role-based access control model that uses a four-step sequence to increase the capability of each functional role (Sandhu et al., 2000). This model compartmentalizes role-based access control based on the different structure which could be flat, hierarchical, constrained and symmetric within an organizational hierarchy.

Within the health information system, there is broad adoption of RBAC, as there is a need for strict controls over personal health information (Carvalho & Bandiera-Paiva, 2018). The healthcare sector as we have already seen in chapter 2 deals with highly private and sensitive information.

2.5.3 Information security control theory

Addressing the balance between information exchange and data protection, Anderson et al. (2017) proposed an information security control theory. In an era where data interoperability within healthcare is highly encouraged and rightly so, for we see its benefits, it is very easy to see the threats and risks that are associated with data exchange (Berryman et al., 2013). The information security control theory (ISCT) consists of two parameters (i) exposure control reasoning and (ii) ethical control reasoning that need to be considered when developing an information security policy based on which controls to establish within an organization (Anderson et al., 2017).

Exposure control reasoning within information security is hinged on the premise that different information assets are susceptible to different and in some cases multiple threats (Anderson et al., 2017). As part of creating an information security policy, information security managers will have to see what controls should be in place to tackle the threats that they are aware of. From an organizational perspective, information systems are exposed to different threats. Exposure control reasoning calls for controls to be initiated based on the threat that affects a particular information system. As stated by Anderson et al. (2017, p. 7) "exposure control reasoning aims to control such exposures by creating a set of controls that protect organizational assets from security exposures". This set of controls are based on already existing risk/threat analysis reports. Risk analysis gives an organization a holistic view of what they are up against when it comes to the data assets.

Ethical control reasoning is the justification of the risk control decision taken (risk treatment) after a risk treatment analysis has been conducted (Anderson et al., 2017). Applying ethical reasoning to determine which control should be in place, when cost and availability of the controls are taken into consideration (Anderson et al., 2017). This second step used in the information security control theory will form the basis of the information security policy within a given organization.

2.5.4 Anonymization and pseudonymization

In section 2.2, personally identifiable information in addition to individual health data makes it easy for data breaches to be used in malicious ways. One way to make mental health data more secure is the removal of PII from digital health data records, which can be achieved by anonymization and pseudonymization (Shoniregun et al., 2010). Both techniques are used to replace the identity of healthcare service users for non-identification by unauthorized individuals.

Anonymization is used in information or data where the altering of the identity of the individual doesn’t interfere with the policies or regulations of that industry. Anonymization of mental health data can be applied during the collection, retention and exchange or disclosure of health care data to other healthcare professionals because it removes the PII of the user from the records held by the healthcare organization (Shoniregun et al., 2010). Pseudonymization on the other hand allows the re-identification of the personal data of users in the digital health records held by the organization (Shoniregun et al., 2010).

2.5.5 Employee compliance/deterrence

The deterrence theory seeks to discourage employees from carrying out activities that violate the information security policy within an organization (Hovav & D’Arcy, 2012). Within the information security discipline, some researchers have focused on the concept of information security policy compliance in organizations to drive the literature within this field (Chen et al., 2018; Harris & Furnell, 2012; Fagade & Tryfonas, 2016). If employees can maintain ISP compliance, it is very likely to reduce the risk of breaches that can occur within an organization (Chen et al., 2018). According to the American national research council, information security threats can be combated by using deterrence and imposing technical obstacles (NRC, 1997).

2.5.6 Data encryption

Digital health data encryption in any given state (data in rest or data in transit), is one of the methods of data protection that are useful in healthcare organizations (Lord, 2020). Data encryption involves using cryptographic technology to turn data into codes and forms that only people with a special key can have access to. Data encryption can take two forms: symmetric and asymmetric encryption. Both of these types use a decryption key with the main difference being – symmetric data encryption uses a single public key while asymmetric encryption has a private key and public key. The generation and use of these keys are guided by data encryption standard algorithms.

2.6 The legal perspective of data privacy and security in healthcare

Apart from the technical and administrative controls that ensure information security in digital mental health organizations available legislation at the national and international levels can catalyze ensuring privacy and security in digital healthcare (Williams & Boren, 2008).

This section will highlight the international and Nigerian legislation that guides health data within the healthcare literature.

2.6.1 National health act

Nigeria's National Health Act of 2014, Act no. 8 provides a legal framework for the "regulation, development and management of a national health system and set standards for the providing health service in Nigeria and other related matters" (NHA, 2014, p.143).

NHA addresses the issue of privacy and confidentiality emphasizing the obligation of healthcare institutions to keep users' health records safe and confidential, allowing the disclosure of such information only with the owner's consent or court order. Additionally, the disclosure of users' health data can be allowed only to third parties like medical professionals and healthcare providers because such disclosure is beneficial to the user.

Sections 28 (1) and 28 (2) provides that a patient's health records can be assessed by healthcare providers with the consent of the user and the same consent be obtained for research purposes. The protection of health records by healthcare organizations are addressed under section 29 of the NHA. It states that "healthcare organizations in possession of user's health records shall implement control measures to prevent unauthorized access to those records and their systems for record-keeping" (NHA, 2014, p. 155). The section also imposes a 2-year jail term or a fine of N250, 000 (an equivalent of $816). In some case, both punishments can be meted out.

The study to assess the knowledge of health professionals on the NHA was carried out by the authors Enabulele and Enabulele (2016). The results showed that although the majority of the respondents were aware of the NHA, only a few of them had actual knowledge about the act. Although NHA exists, the implementation is largely hinged on how knowledgeable healthcare professionals and providers are about the act. Authors recommend the need for increasing the knowledge of the NHA by creating advocacy and documents to educate health professionals of the NHA.

2.6.2 Patient's bill of rights

The patient's bill of rights (PBR) was introduced in 2018 by the Consumer Protection Council of Nigeria (CPC). The PBR outlines the rights of patients that are contained in several other enacted legislation within the health sector in Nigeria. The goal of the document is to sensitize the Nigerian public on patient’s rights, patient’s responsibilities and provider responsibilities in the healthcare sector under the following areas: (i) access to information, (ii) patient-related information, (iii) fee-related information (iv) confidentiality, (v) quality of care, (vi) patients’ dignity, (vii) access to emergency care, (viii) visitation, (ix) patients’ refusal of care, (x) interruption of service by provider and (xi) complaints (ccpc.gov, 2018).

The PBR includes patients' rights to privacy and confidentiality of their health data. The CPC has created this act to protect the Nigerian people and the council emphasizes the need for professionalism in the healthcare sector.

3 Theoretical framework

In this chapter, a health data governance (HDG) framework is examined. With the flow of communication within the HDG framework, this chapter explains the need for information security governance within digital health. A comprehensive information security governance framework is adopted upon which the information security practices of digital mental healthcare platforms in Nigeria will be measured in this paper.

3.1 Digital health in Nigeria

The quest for the next major technological breakthrough is never-ending. Users are looking for more comfort and ease, and the healthcare industry is no exception in this technological race. Digital health contributes to the achievement of the third objective of the United Nations Sustainable Development Goal (SDG3) to ensure healthy lives and promote well-being for all of all ages (Konduri et al., 2018).

The United Nations Sustainable Development Goals encourages healthcare initiatives to rethink their modelling from traditional on-ground healthcare to digital healthcare (Asi & Williams, 2018) particularly in communities with a low number of healthcare workers and difficult access to healthcare services. Furthermore, Asi and Williams (2018) assert that digital health technologies are inherent to changing the narrative of health care services in developing countries. Not only is this a benefit for the communities, the government and health care providers can also leverage this where there is a shortage of healthcare workers. In developing countries like Nigeria, telemedicine comes as a band-aid to the challenges of access to healthcare (Adewale, 2004).

As the use of ICT in healthcare and the adoption of digital health by citizens increases, the lack of a good health system governance has been described as a factor affecting the implementation of digital health in Nigeria (Ibeneme et al., 2020).

To solve this challenge, it's pivotal for the government to consider a health data governance framework that will not only guide digital health outcomes such as citizens' access to mental healthcare and data integrity but improve the quality and delivery of healthcare services in the country.

3.2 Health data governance

While the procurement and adoption of ICT technologies in healthcare present a good opportunity to improve the health sector in Nigeria, digital health systems in themselves cannot reduce the challenges in the healthcare sector without good governance (Marcelo et al., 2018).

The concept of reliable technological solutions within digital health has been a huge concern to all the actors involved in the healthcare sector, considering the potential damage of data breaches like the 2020 ransomware attack on the Florida orthopaedic institute that breached the data of more than 600, 000 patients (Davies, 2020). This level of exposure to patients' data can harm both the health organization and those whose data have been breached.

The health data governance framework by Sogomonjan (2021), illustrated below (permission obtained from author to use original diagram) shows the central connecting point of all actors within a digital health solution is the communication process, it is, therefore, necessary to make this process reliable. Since information is the asset that connects all the players in the HDG below, these stakeholders are affected by problems that occur in the governance of healthcare information (Andronis & Moysey, 2013).

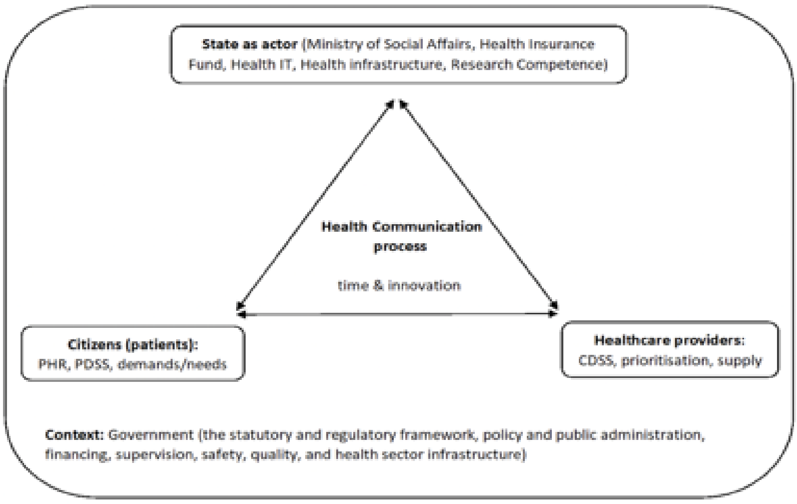
State as actor (Ministry of Social Affairs, Health Insurance Fund, Health IT, Health infrastructure, Research Competence)
Health Communication process
time & innovation
Citizens (patients): PHR, PDSS, demands/needs
Healthcare providers: CDSS, prioritisation, supply
Context: Government (the statutory and regulatory framework, policy and public administration, financing, supervision, safety, quality, and health sector infrastructure)

Figure 3. Data health governance framework by Sogomonjan (2020)

3.3 Information security as a means to improve health data governance

The entire relationship within the health data governance framework developed by Sogomonjan (2021), relies on communication from one actor to another. Communication cannot occur in isolation. It has a medium of communication, and within a digital health environment that communication is facilitated through information and communication technology. To that end, a representation of the mechanisms that must be in place to ensure that digital mental health data are safe within healthcare organizations is needed. To do this, a comprehensive information security governance framework (ISG) adopted for this study will be used to determine if the existing digital mental health providers in Nigeria have appropriate measures in place to ensure that health data are secured.

Data management is an important aspect of digital health as patient's personal information is highly confidential. Data confidentiality stands as the goal of the CIA triad for information security. Within the information security literature, there are different policies, tools, technologies that are used to not only ensure the confidentiality of data but also its integrity and accessibility.

The flow of data in any health system does not occur in isolation. It has a medium of communication and a channel of distribution. Additionally, healthcare organizations have the responsibility to secure this information as it goes through the information lifecycle. The security of information within healthcare organizations has become a top priority as the healthcare industry has not been spared from cyber-attacks. In the last five years, the identity theft resource centre recorded that the healthcare industry suffered 2050 data (Identity Theft Resource Center, 2021).

Although many policies, tools and technology exist, healthcare organizations must adopt a holistic approach towards information security because it gives healthcare organization insights on risk management and data security strategies for all actors in their information environment. As the amount of data within healthcare is enormous, these organizations need to maintain clear structural documentation of the responsibilities, authorization levels, and technical measures that exist to protect digital health data (Mears & von Solms, 2004).

3.4 Information Security Governance Framework

Information security governance within healthcare is essential for healthcare organizations to protect user data and inculcate the participation of employees in this process.

From a theoretical perspective of information security governance, several frameworks like the Capability Maturity Model, Information Security Organization's code of practice, and Information Security Architecture, have been used in several literature.

Although each of these ISG frameworks provide controls for information security at an organizational level from a technical and behavioural standpoint, Veiga and Eloff (2007) proposed a theoretical ISG framework, that consolidates the four approaches mentioned above. Their framework serves as a single point that comprises different control components for developing ISG in any organization. The authors assert that "the framework provides management the means to implement an effective and comprehensive information security governance program that addresses technical, procedural, and human components" (Veiga & Eloff 2007, p. 363). Below is a modified diagram of Veiga & Eloff's ISG framework.

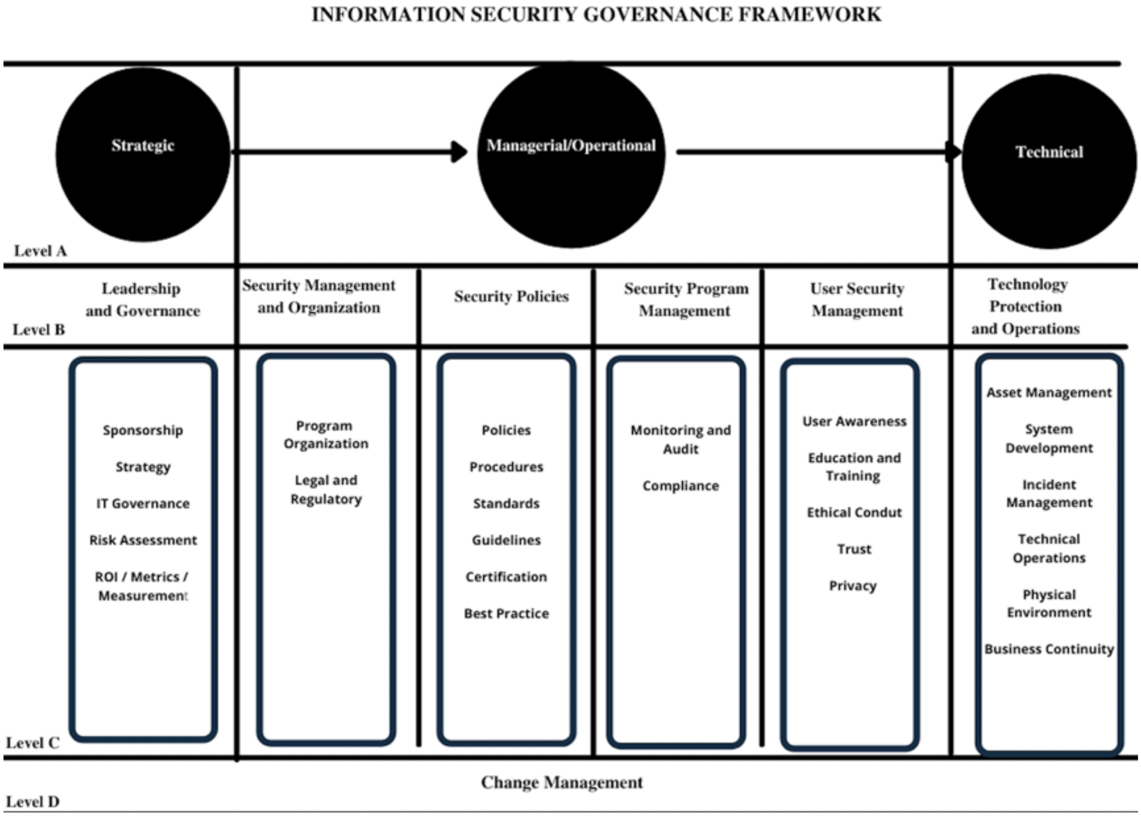

Figure 4. Information security governance framework by Veiga & Eloff (2007)

There are four levels within the information security governance that all work together to achieve information security excellence in an organization. The first level shows the internal structure of an organization based on the management hierarchy. The second level shows the core responsibilities of the different management levels in the organization. Since the goal of having the information security governance framework is to ensure the CIA of digital mental health data from all actors, the third level of the framework shows all the measures that need to be in place to achieve this goal. The fourth level focuses on change management, ensuring proper documentation of any changes within the information security governance of an organization.

The goal of creating and enforcing an information security policy within any organization is to ensure that employees can take the necessary actions to protect the data assets and systems from threats. Internal control of information is what is at the heart of information security policies set up by organizations.

3.4.1 Leadership and governance

The components of the leadership and governance category are (i) receiving executive-level sponsorship, (ii) strategy, (iii) IT governance, (iv) risk assessments and (v) ROI/ metrics/measurement of the information security strategy (Eloff & Veiga, 2007).

The place of attaining the executive committee is the first step towards information security governance as we see from the framework above. All the other components within this category rely on the acceptance of the executive leadership (von Solms, 2006). One of the ways that the responsibility of information security has rested on the shoulders of executive management is the introduction of regulations. An example is the 2002 Sarbanes-Oxley Act, the Act holds CEOs responsible for the financial statement of their company (Sarbanes-Oxley, 2002). Although this corporate governance measure is within the financial services, it's an apt example of what category A entails within the framework.

The top management of any healthcare provider has to be the foundation of the information security strategy. Concerns have been raised about the interest of developing countries to treat information security as a governance concern (Yaokumah, 2014). As such the integration of leadership and governance within an information security governance is important to achieve the overall security goal.

3.4.2 Security management and organization

The two components in this category are program organization and legal/regulatory management. According to the ISO 17799 (2005), the objective of the security management and organization category of the ISG framework is to manage information security within the organization's internal environment.

Within the healthcare sector, different legislations hold information security standards to healthcare providers like Nigeria's National Health Act (NHA, 2014). For digital mental health platforms to achieve their information security goals, they have to understand the information security-related legislation both nationally and internationally because the Internet super sits national boundaries.

3.4.3 Security policies

Before implementing a security policy or policies within an organization, category 2 has to be considered for the policies to be effective and meet compliance monitoring (Veiga & Eloff, 2007).

Security policies control how data are collected and exchanged electronically. For instance, the access control policy determines how specific roles can access information and the level of actions that they can perform with the information.

As for information security procedures, they are predicated on the already existing information security standards that exist in the configuration requirements for security tools and technologies (Veiga & Eloff, 2007).

3.4.4 Security program management

The components within this category are Monitoring & Audit and Compliance. These aspects are the programs that the organization will have to put in place to continuously monitor the information security policies that they have already established. According to Vroom and von Solms (2005), this category is an important aspect of the ISG, because organizations need to know how their strategies are faring. By having a security management program, reviews can be made and rules adjusted where necessary.

Additionally, "an effective information security program cannot be implemented without implementing an employee awareness and training program to address policy, procedures, and tools" (Peltier, 2007, p. 1). Employee training and awareness is the train that holds an information security-conscious organization together, as both leadership support and security education/training places information security as part of the organization's culture.

So, at the centre of any security management program is the employee, but technological monitoring has to be in place to facilitate the auditing of the security practices of the employees (Veiga & Eloff, 2007), otherwise, there is no way to determine how effective the training received changes the security mindset of the employees.

3.4.5 User security management

The necessity of having the components of the user security management category present in every organization is largely based on the premise that users (employees) are often the weakest links in information security in any organization (Seh et al., 2018).

“In work environments where users handle highly sensitive data (e.g., law, finance, medicine), one user’s inappropriate action can lead to a security breach affecting the entire organization” (Gross & Rosson, 2007, p. 1). The end users’ approach to information security is often responsible for how they act towards the data they handle. To minimize the insider's threat to company information, risks to privacy and the integrity of information, the organization has to communicate the rules that guide its ethical conduct (Veiga & Eloff, 2007).

Trust as an element of information security management is based on the existing security controls that the organizations have in place to protect the confidentiality of patient’s information. User security management within an organization can also leave end-users worry-free because they can trust that their health data are in capable hands (Gross & Rosson, 2007).

3.4.6 Technology protection and operations

Each component in this category has a corresponding technology that can protect the overall security of the organization. The applicable controls based on the environment and risks identified must be implemented (Veiga & Eloff, 2007). These controls are both physical and technological in their form.

The goal is to monitor these controls and ensure that they can support the information asset in the organization, in preventing or responding to information security issues by putting in place technical mechanisms like firewalls or physical mechanisms like access cards.

3.4.7 Change management in information security governance

Beyond having the security controls in place, is the need for all personnel to be aware of the position of the organization on information security; otherwise, these controls would be ineffective. Change management is the adoption of new information security practices and controls by employees (Panorama Consulting Group, 2020). Although information security is not needed as knowledge for performing a job function, for example, accounting; the assumption that employees are aware of information security measures is detrimental (Niekerk & Solms, 2010). Therefore, organizations adopting information security governance should ensure that change management is in place that transforms the organizational culture towards information security. Organizational cultures have a strong impact on how employers behave, and this is no different in the information security management concept (Tang et al., 2016).

3.5 Conclusion

Security breaches affect the digital healthcare sector and digital mental healthcare are a part of the bigger picture - digital health. I have adopted the health data governance framework, as a model that can improve digital healthcare. The health data governance framework focuses on communication among different actors but fails to include how digital health information communicated from one actor to another is protected. Without any form of information security, the exchange of data from one actor to another is susceptible to information security threats resulting in data breaches.

Although the author of the health data governance framework identifies time and innovation as components of the communication process in digital healthcare, management of information (information security) seems to not be a vital concern of the health data governance framework. Could this be the reason for a significant number in the rate of security breaches experienced in the healthcare sector? This question is a part of what this thesis seeks to investigate.

Information security in digital mental health communication cannot be ignored. The information security governance framework developed by Veiga & Eloff (2007) provides organizations with a roadmap for implementing information security controls at all levels and is adopted for this study because it enables me to investigate the availability of information security governance within digital mental healthcare in Nigeria.

Having discussed the relevant literature and theoretical frameworks that guide this thesis, the next chapter will introduce us to the selected organization used for this case study research.

4 Case study research methodology

This thesis employs a case study research methodology. This method has been selected for this thesis because it provides an explanatory approach to answer what, how, and why questions (Crowe et al., 2011).

The case study research methodology has been defined by Crowe et al. (2011) “as a research approach that is used to generate in-depth, multi-faceted understanding of a complex issue in its real-life context”. Case study methodology focuses on a particular issue to help the researcher understand real-world problems as well as gainful insight into solutions (Noor, 2008). Furthermore, Meyer (2001) suggests that the case study methodology can help researchers view how contextual phenomenon operates in real life by including theories, concepts and frameworks. The existing framework in this study allows the researcher to employ a deductive case study approach. The deductive case study approach allows the user to make observations in their work based on existing theories (Runeson et al., 2012)

4.1 Research design

The case used for this study was a single case. According to Yin (2018), a single-case design is preferred over a multiple case study design when the goal of the researcher is to test the application of relevant theories.

In this study, the theoretical framework that underpins information security governance presented and validated via interviews from participants. The challenges to information security within digital health as well as measures to protect user’s data from security breaches are discussed in the literature review while semi-structured interviews were carried out to determine if digital mental healthcare providers in Nigeria utilize information security governance to protect the privacy and confidentiality of user's data.

4.2 Case selection

According to Yin (2018), a selection criterion for the choice of case study is having access to data. These criteria were considered at the beginning of this work. I made contact with Mentally Aware Nigeria Initiative (MANI) to determine if access would be granted for the study. Additionally, the choice of case study is relevant because MANI has expanded its online platform to address mental health in the covid-19 situation, with an initiative called Project-Covid. ng. Among the various non-governmental mental health initiatives available in Nigeria, MANI is considered the right choice for this thesis, because its initiative is fully digital. From its inception in 2016 till date more than 5000 people (Wanyony, 2019) have benefitted from its free services via its website, social media platforms, suicide/stress hotlines and website.

4.3 Data collection

Semi-structured interviews were used for data collection after completing the review of relevant literature. This method of data collection is adequate because it allows the researcher to have an in-depth knowledge of the participants' experiences (Yin, 2018). The aim of using semi-structured interviews in case study research is to obtain information from the participants who have personal experience, expertise and opinion that are relevant to the research topic (DeJonckheere et al., 2019). Since the goal is not to attain statistical representation (DeJonckheere et al., 2019). The researcher incorporated a theoretical purposive sampling to determine the number of participants for this study. Purposive sampling refers to the selection of participants determined by a specific purpose that could include their role or experience (Ishak & Bakar, 2014). The purpose of selecting the participants was based on a theoretical sampling of their role within the organization in connection to the first level of the ISG theoretical framework adopted for this study.

Considering the size of the organization, a total number of 4 participants informed this study: Strategic roles (n=1), Managerial and operational roles (n=2), and Technical roles (n=1). Before conducting the interviews, each participant was informed of the following ethical considerations orally: (i) confidentiality of their identity, (ii) the purpose of this study and (iii) access to the final work of the researcher.

Data validity in this work is ensured using theoretical sampling to ensure that the data collected in the literature review phase of this study was used to determine the source of data from the case study.

4.4 Data analysis

Within the choice of case study, the researcher directed the questions based on the professional role of the participants, this was done to ensure that I could analyze the response to the components of the ISG framework.

The researcher employs the framework analysis approach developed by Ritchie & Spencer (1994) to provide interpretation and description of the outcome of qualitative data. The framework analysis consists of five steps: (i) familiarization, (ii) identification of thematic framework, (iii) indexing, (iv) charting and (v) mapping and interpretation (Ritchie & Spencer, 1994).

I carry out these steps, in an attempt to be able to manage the voluminous amount of data that is made available from the interviews conducted. According to Srivastava and Stanley (2009), the framework analysis allows researchers to document the analytical and interpretive stages of the work that can be accessed by people other than the researcher. This feature of the framework analysis is adept to meet the need of this work to make it available to both academic and organizational institutions as a means of increasing the body of knowledge on digital mental health in Nigeria. Furthermore, the choice of data analysis method was influenced by the research questions which were postulated to evaluate the availability of ISG in digital mental health organizations in Nigeria.

Framework analysis tends to be adequate for research questions that are contextual, diagnostic, evaluative and strategic in style (Ritchie & Spencer, 1994).

I also ensured that the outcome of data analysis was not manipulated to fit the theoretical framework for the study, as the result of a case study could either assert or oppose the adopted theoretical framework (George & Bennett, 2005).

Although criticism exists as to the use of case study methodology (Idowu, 2016), its reliability has been proven by employing theoretical sampling and even validation from respondents Crowe et al. (2011).

4.5 Limitations

Realistically, no choice of research methodology is void of limitations (Crowe, 2011), but I ensured that the limitations to this work were unavoidable. The interviews were conducted in April 2021, during the time of the pandemic. Since Estonia was on lockdown I was unable to travel to Nigeria, which made it hard to trace the number of people that I would have needed, but the 4 interviews conducted were sufficient as the participants were experts in their fields. I, therefore, carried out interviews via internet voice calls, which impedes the observation of the body language of the participants. The length of the interview was also affected because the participants were responsible for bearing the cost of Internet connections which is expensive in developing countries like Nigeria. Additionally, triangulation of information was more time consuming and difficult over the Internet which would otherwise have been different if I was present in the location of the case study.

Researchers' bias exists because I am from the country of the case study and is aware of institutional challenges that the country is faced with and this can interfere with the study. To overcome this bias the researcher made efforts to be intersubjective and discussed with her supervisors her role as the interviewer and findings of the study.

5 Findings

Using the framework analysis approach the data collected have been analyzed and the interpretation is presented and discussed in this chapter.

Within the deductive approach used for this thesis, themes and codes for analyzing the data are preselected based on existing literature, theories or the details of the research questions (Gale et al., 2013). In the case of this work, the theoretical framework in chapter 3 of this work is used for the thematization of the interview results. Upon transcribing the interviews, anonymization is used to conceal the identity of the participants where Q = participant number.

5.1 Identification of themes

The following themes and sub-themes have been identified for data interpretation: (i) the role of leadership in ISG (sponsorship, organizational culture), (ii) managing security (program organization and regulation), (iii) security policies (organizational policies, security policies), (iv) user security management (training, compliance), (v) technological protection and operations (access based, anonymization).

5.1.1 The role of leadership in ISG

Organizational leaders within healthcare are responsible for directing the trajectory of different cultures and that includes information security. The participants all explained that information security wasn't the responsibility of the IT team alone, but every member of the organization.

"Oh no, everybody has to be involved in it, everybody has to be security-conscious on so many things, because like I've been saying the same major thing about our organizations is confidentiality. Our client needs to know that when you come to us your information is safe, whatever we discuss is safe. So, everybody has to be involved it's more like covering every base to avoid leakage from any part" (Q3).

Additionally, all the participants agreed that MANI is an information security-conscious organization. This question was asked to further access the organizational culture towards information security.

“Because, you know, we are dealing with people personal information and then the team understands confidentiality and ethics that guide that. So, it’s highly prioritized at MANI. So that is why during the training for the counsellors we also do that to make sure that they are aware although the counsellors that we have are also people in mental health, we also reiterate that often, so they know how important it is because we are dealing with humans” (Q3).

5.1.2 Managing security (program organization and regulation)

On managing security, the participants revealed that a system of quality control is used to ensure adherence to the organizations' position on confidentiality of data.

“So, the counsellors themselves won’t have access to the data but the people who serve as the admin members so that they will be able to post the cases and access plan. These are people that have been properly trained about the importance of data management” (Q4).

5.1.3 Security policies (organization policies)

Within the case study organization, internal policies based on country legislation exist that ensures the activities of employees do not interfere with the confidentiality of users’ data.

“Yes, because like for every country there is always something guiding everybody to ensure that you are staying within the scope and we know that if there’s an issue, our client can end up suing us, so we ensure that there are some of these things that guide us” (Q2).

Part of the organization’s method of ensuring data confidentiality included in the contract with its employees and volunteers.

“Confidentiality is written in our contracts also, before you sign the contract you get to know that, before you are accepted to work with us there are some things in the contract that you have to read through and know that this information about MANI, it is for MANI, it is so, it is something that we ensure that everybody that works with us has including our janitor has a contract based on confidentiality. So that you will know that any information here is for MANI, there's a law that says that you can't transfer it, you can't take it outside the organization, and it has to stay within the organization" (Q2).

5.1.4 User security management (training and compliance)

MANI has a system of constant learning and knowledge sharing on information security. "Okay, we still had training last month, around March 15 to March 19. We believe a lot of things are changing and we have to keep things updated every time so we schedule training to exchange information and also stay updated, ignorance cannot be used as an excuse" (Q4).

"So, part of the training that we give to everyone that joins the organization is the importance of privacy and data information. The same thing goes for the service users as well, the fact that you have had a counsellor attend to you does not give you the right to go out there on social media and talk about this person? This person also deserves some level of privacy because they have opened themselves to you so give them that respect as well as we also give you the respect of not putting any information about you out there" (Q4).

To ensure compliance with the information security measures in place, the organization has a documented deterrence policy as well as carrying out unscheduled checks on employee work devices.

"Yes, for each policy that says you flout this rule, there are consequences for it. For every action, you take there's always a consequence whether it's a negative one or a positive one. So, we have like now, to check and be certain that they are complying with our policies. We do random checks, we inform everybody that the organization can do a random check on your system even maybe when you're going home, we can decide to say just hold on we would like to do a search and go through your things to be sure that you're not taking things out of the organization and if you're caught, there's always a repercussion for everything" (Q2).

5.1.5 Technological protection and operations

Although the organization does not have an in-house team of IT staff, they utilize an external IT consultant who is responsible for carrying out regular checks/update on all the information systems within the organization. To restrict unapproved access to digital mental health data, the organization has put in place, access-based controls.

"So, we have an admin officer, I think she has been with MANI for a long time, and she has been doing the job so far, she and then selected few people have access to that and they do not have access to edit. Yes, they do not have access to edit. They just have access to view the sheets so they can't edit. So that's why they can't delete or alter any information that has been imputed by clients" (Q3).

"Okay, so in MANI what we do more is that when you come online your conditions are there but our volunteers and the counsellors they get to just have the name, phone number and how the person wants us to be of help to him or her. So, they don't have full access to, just some of the information that is necessary for them to help with the counselling sessions are extracted and sent to them" (Q2).

The use of anonymization helps to reduce the impact on their users in case of a data breach occurs.

"So, you fill with the name that you're comfortable with. So, you still have a level of anonymity. Not anonymity in the sense that you necessarily do not want to tell us your real name so that way you're comfortable to give us access to talk to you because you asked for the help. So that way, those are certain ways that we've been able to bring in data protection in the sense of you don't need to tell us your real name if you don't want to. We don't know if it's your real name. Before you fill it we are going to call you. If you tell us that your name is Jack we'll call you Jack when the counsellor is addressing you. It's you who knows whether that's your real name or your alias" (Q4).

Data retention policy is also used as a mechanism to discourage employees and volunteers from keeping the information gathered on any user during counselling sessions.

“Okay, yes, I know that the counselling team, you know mostly we do counselling sessions on WhatsApp, so we inform them once you’re done chatting with the client you are to clear up your chat. We don’t keep screenshots of anything or send screenshots to anyone and before you come in all these rules and laws have been laid and you end up agreeing to before you are being inducted fully as a counsellor or volunteer counsellor at MANI” (Q2).

The use of external IT staff was also explained by the participants.

“There are consultants that come in from time to time to you know maybe check on the level of security on the website, on the backend, on the level of security for like instance our internets and all the things that require like, the things the finance departments do to make sure they're protected and stuff. So, as I said to the best of my knowledge, they're mostly consultants and we don't have in-house IT personnel” (Q1).

5.2 Perception, knowledge & awareness of threats to mental health data

General questions were asked to determine employee awareness of information security threats. The participants were all aware of the threats to digital mental health data.

“The truth of the matter is that NGO’s get targeted, I don’t know about outside Nigeria but in Nigeria NGO’s get targeted because they have this notion that we get a lot of money and then because of that they want to know where we get the money from or what we are doing with the money and all that. So, I don’t think NGO’s are immune from media harassment or data privacy breaches” (Q4).

“So far, we have never had a data breach on user’s data. If you are going to probably let’s say somebody posted our counsellors information online but it’s not from our end. So far, no. Yes, because like I said earlier confidentiality is a major thing in everything we do, and we really will not be where we are today if the information of our clients or anybody is just getting out anywhere, so we are conscious of that” (Q2).

When it came to questions on data breaches, the organization had not experienced any that affected user's information, but they were issues with users exposing the information from session to the public.

"We had an experience recently. I think someone used our service and wasn't satisfied and instead of reporting back to us the person went on social media and was tagging us and complaining and all that and before we knew it one of these social media influencers picked it up and was kind of "dragging us" if I can use that word. And I find that very funny because this is a volunteer service, right? You could as well have given us the feedback that you were not satisfied and then there was a feedback form, but you didn't. But of course, we could not go out there to start saying all that, so we had to release a statement, get in touch with the person and all that" (Q4).

6 Discussion

This chapter connects the findings from the previous chapter to the information security framework discussed in chapter 3 of this thesis. The information security governance theoretical framework is used to discuss the research questions posed in this thesis. Level three of the ISG framework is divided into 7 headings with their components listed in level 4 of the ISG framework. Following the thematization in the previous chapter, I make connections between the research question and the ISG framework.

6.1 Discussion on research questions

The objective of this thesis was to assess the security posture of digital mental health organizations in Nigeria, to do this, three research questions were posed at the beginning of this thesis.

The research questions presented in chapter 1 are discussed below in sequential order.

(a) What threats would most likely affect your organization?

The findings revealed that the MANI is mostly concerned about external threats like hackers. All four participants were aware of internal threats but mostly pointed that external threats would more likely occur because the internal environment of their organization has established user security management.

In the ISG framework adopted in this study, the authors Veiga and Eloff (2007), identifies trust as a component of user security management. I observed from the findings that because of the sensitivity of mental health data, the participants were mostly in their job position because of their passion to improve mental healthcare. Personal value has been identified as one of the factors that influence the information security behaviours of employees (Abraham, 2011). Thus, before an ISG can be effective in improving health data governance, employees perception towards user's data are important. One of the components of user security management is user awareness, education and training on information security governance.

The ability of the participants to identify what threats would be of the most impact to their organization shows the level of education and awareness that the participants have regarding information security within their organization as they all seemed to maintain that because their organization is information security conscious, the probability of an internal threat actualizing its goals is low. Trust is one of the components that should be present within the managerial and operational level of the organization (Veiga & Eloff, 2007), the participants emphasized the trust exist within the organization and is maintained by putting in place necessary security controls which were also identified as part of the mechanism for ensuring trust in the ISG framework.

(b) What measures are in place to protect user's data within your organization?

Data protection methods here refer to both technological and sociological mechanisms in place. The findings revealed that access-based controls, organizational security policies and quality control were used to protect users' data internally.

Because MANI offers first aid mental health care and works with a large number of volunteers, their security policies do not allow counsellors to keep a record of their sessions with users, additionally, each users' data are handled by a separate set of employees who have access rights to the database. In comparison to the ISG framework, the findings have shown that the organization employs security policies and compliance at the managerial / operation level. This ensures that the communication channel is not closed between the employees and managers because everyone knows what the policy states. Additionally, Compliance allows managers to trace how employees operate daily without flouting laid down policies.

In Nigeria, the NHA serves as the legal/regulatory guide that meets the ISG's requirement on security management. Apart from information security policies and technical access-based controls, the organization uses a quality control mechanism to ensure the integrity of user's data. Although the information technology arm of the organization is maintained by an external organization, data assets are managed internally, which meets the technological protection that the ISG framework pursues. Part of the component of the user security management in the ISG framework is ensuring ethical conduct. Professionalism in handling data / technical assets was identified in the findings, in a recent event where an unsatisfied user revealed information on their session to the public, the organization places the ethical conducts that protect user's information as a priority. MANI does this by demanding that all communication and processes meet the standards of their partners both nationally and internationally.

(c) What techniques are used to ensure employee compliance to existing information security measures?

The organization uses a deterrence method to ensure compliance to policies and continuous monitoring is done by carrying out unnotified security checks and penalties for activities that can affect the confidentiality and privacy of users. This method could be viewed as both compliance and monitoring. The audit made on information assets assigned to employees allows the healthcare organization to determine the level of compliance and adherence to the information security that each employee displays. Within the ISG framework, both monitoring and compliance are identified as part of the requirements needed in managing the security program in an organization. Security policy compliance can radically make healthcare organizations more proactive than reactive to possible threats (Kwon & Johnson, 2012).

Additionally, the findings revealed that the organization is constantly training their employees on information security based on current events or knowledge gaps. All participants agreed that the organization is information security conscious, this is because confidentiality is highly priced by the leaders at the organization. From the ISG framework, Von Solms (2006) asserts that the only way for the information security governance framework to work in an organization, the strategic arm of the management would need to give their full support.

7 Summary and future research

As the potential of digital mental health continues to grow in Nigeria, so also does the threat landscape that can potentially damage the reputation of organizations whilst affecting users in different capacities.

Although technological mechanisms can be used to secure digital mental health data, throughout the study reference has been made to internal threats and so a socio-technical approach like the ISG framework carries the potential to improve health data governance. The results showed that although digital mental health in Nigeria is at its early stages, organizations dealing with special categories of personal data are committed to protecting the confidentiality of data. By implementing ISG into health data governance, more healthcare organizations have an opportunity to ensure the safety and confidentiality of digital health data.

7.1 Future research

At the beginning of this study, some of the challenges to mental health in Nigeria were highlighted and the promise of digital healthcare to close the gap was introduced. This thesis has explained how digital mental health, although with tremendous potential, can become a source of pain if mental health data are exposed to the wrong hands. This thesis is one of the few academic studies on digital mental healthcare in Nigeria and the opportunities for future research would be to look at how digital mental healthcare organizations are well prepared to manage cybersecurity incidents. Within information security, the question is not if an organization will be attacked but when, this is because malicious actors like hackers are constantly finding new vulnerabilities on health information systems. Therefore, future research that explores how mental healthcare organizations in Nigeria are prepared when their information environment is compromised by hackers.

Acknowledgements

My sincere gratitude goes to my King and Lord, the Almighty God who sustains me.

I would like to thank my amazing supervisors Prof Dr. Dr. Robert Krimmer and Melita Sogomonjan for their patience, guidance and encouragement during this research work, the beginning was hard and there have been many days when I am still amazed that this research got completed. I remain grateful to you both, for your commitment to my success.

I also thank the admission team at the Department of E-governance Technologies and Services for the opportunity to study in Estonia under a full tuition waiver as well as the Dora pluss scholarship received from the Tallinn University of Technology.

This work received support through the H2020 research and innovation programme under grant agreement No 857622.

References

[1] Abdulmalik, J., Kola, L., & Gureje, O. (2016). Mental health system governance in Nigeria: Challenges, opportunities and strategies for improvement. *Global Mental Health*, *3*, e9. https://doi.org/10.1017/gmh.2016.2

[2] Adewale, O. S. (2004). An internet-based telemedicine system in Nigeria. *International Journal of Information Management*, *24*(3), 221–234. https://doi.org/10.1016/j.ijinfomgt.2003.12.014

[3] Agrawal, A., & Alharbe, N. R. (2019). Need and Importance of Healthcare Data Integrity. *International Journal of Engineering and Technology*, *11*(4), 854–859. https://doi.org/10.21817/ijet/2019/v11i4/191104033

[4] Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. *Journal of Management Information Systems*, *34*(4), 1082–1112. https://doi.org/10.1080/07421222.2017.1394063

[5] Andronis, K., & Moysey, K. (2013). Data governance for health care providers. In *Health Information Governance in a Digital Environment* (Vol. 193, pp. 299–301). IOS Press. https://books.google.ee/books?hl=en&lr=&id=IfDAAQAAQBAJ&oi=fnd&pg=PA299&dq=(Andronis+%26+Moysey+2013&ots=1PSl6gOnod&sig=4LOCXOAERXTYoj7IoNazpJdbd4Q&redir_esc=y#v=onepage&q=(Andronis%20%26%20Moysey%202013&f=false

[6] Anyebe, E. E., Olisah, V. O., Garba, S. N., & Amedu, M. (2019). Current Status of Mental Health Services at the Primary Healthcare Level in Northern Nigeria. *Administration and Policy in Mental Health and Mental Health Services Research*, *46*(5), 620–628. https://doi.org/10.1007/s10488-019-00950-1

[7] 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

[8] Asi, Y. M., & Williams, C. (2018). The role of digital health in making progress toward Sustainable Development Goal (SDG) 3 in conflict-affected populations. *International Journal of Medical Informatics*, *114*, 114–120. https://doi.org/10.1016/j.ijmedinf.2017.11.003

[9] Aurigemma, S., & Panko, R. (2012). A Composite Framework for Behavioral Compliance with Information Security Policies. *2012 45th Hawaii International Conference on System Sciences*, 3248–3257. https://doi.org/10.1109/HICSS.2012.49

[10] Ayatollahi, H., & Shagerdi, G. (2017). Information Security Risk Assessment in Hospitals. *The Open Medical Informatics Journal*, *11*(1), 37–43. https://doi.org/10.2174/1874431101711010037

[11] Bennett, K., Bennett, A. J., & Griffiths, K. M. (2010). Security Considerations for E-Mental Health Interventions. *Journal of Medical Internet Research*, *12*(5), e61. https://doi.org/10.2196/jmir.1468

[12] Berryman, R., Yost, N., Dunn, N., & Edwards, C. (2013). *Data Interoperability and Information Security in Healthcare*. Transactions of the International Conference on Health Information Technology Advancement, USA.

[13] Bulgurcu, Cavusoglu, & Benbasat. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523. https://doi.org/10.2307/25750690

[14] Carter, H., Araya, R., Anjur, K., Deng, D., & Naslund, J. A. (2021). The emergence of digital mental health in low-income and middle-income countries: A review of recent advances and implications for the treatment and prevention of mental disorders. *Journal of Psychiatric Research*, *133*, 223–246. https://doi.org/10.1016/j.jpsychires.2020.12.016

[15] Chan, E. Y., & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior*, *119*, 106718. https://doi.org/10.1016/j.chb.2021.106718

[16] Chen, X., Chen, L., & Wu, D. (2018). Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective. *Journal of Computer Information Systems*, *58*(4), 312–324. https://doi.org/10.1080/08874417.2016.1258679

[17] Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions: Enterprise data breach. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211. https://doi.org/10.1002/widm.1211

[18] Connected health cities. (16 C.E., 2018). *Is mental health data more sensitive than physical health data?* https://www.connectedhealthcities.org/2018/01/mental-health-data-sensitive-physical-health-data/

[19] *Patients' Bill Of Rights (PBoR)*, Federal Ministry of health, Nigeria (testimony of Cosumer Protection Council). https://www.fccpc.gov.ng/uploads/files/patients-bill-of-rights-full-version.pdf

[20] Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, *11*(1), 100. https://doi.org/10.1186/1471-2288-11-100

[21] Curtis, A. (2018, June 8). Why is the Healthcare Industry the Biggest Victim of Identity Theft and Data Breaches? *Infoarmor Blog*. https://blog.infoarmor.com/employers/why-healthcare-industry-biggest-victim-of-identity-theft-and-data-breaches

[22] Cybersecfill. (2019). *80000 Nigerians medical data at risk*. https://www.cybersecfill.com/80000-nigerians-medical-data-at-risk/

[23] de Carvalho Junior, M. A., & Bandiera-Paiva, P. (2018). Health Information System Role-Based Access Control Current Security Trends and Challenges. *Journal of Healthcare Engineering*, *2018*, 1–8. https://doi.org/10.1155/2018/6510249

[24] DeJonckheere, M., Lindquist-Grantz, R., Toraman, S., Haddad, K., & Vaughn, L. M. (2019). Intersection of Mixed Methods and Community-Based Participatory Research: A Methodological Review. *Journal of Mixed Methods Research*, *13*(4), 481–502. https://doi.org/10.1177/1558689818778469

[25] DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: A balance of relationship and rigour. *Family Medicine and Community Health*, *7*(2), e000057. https://doi.org/10.1136/fmch-2018-000057

[26] Enabulele, O., & Enabulele, J. (2016). Nigeria’s National Health Act: An assessment of health professionals’ knowledge and perception. *Nigerian Medical Journal*, *57*(5), 260. https://doi.org/10.4103/0300-1652.190594

[27] Erceg, A. (2019). Information security: Threat from employees. *Tehnički Glasnik*, *13*(2), 123–128. https://doi.org/10.31803/tg-20180717222848

[28] Fagade, T., & Tryfonas, T. (2016). Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks. In T. Tryfonas (Ed.), *Human Aspects of Information Security, Privacy, and Trust* (Vol. 9750, pp. 128–139). Springer International Publishing. https://doi.org/10.1007/978-3-319-39381-0_12

[29] National Health Act, no. 8, 101 (2014). https://nigeriahealthwatch.com/wp-content/uploads/bsk-pdf-manager/2018/07/01_-Official-Gazette-of-the-National-Health-Act-FGN.pdf

[30] Fernandes, A. C., Cloete, D., Broadbent, M. T., Hayes, R. D., Chang, C.-K., Jackson, R. G., Roberts, A., Tsang, J., Soncul, M., Liebscher, J., Stewart, R., & Callard, F. (2013). Development and evaluation of a de-identification procedure for a case register sourced from mental health electronic records. *BMC Medical Informatics and Decision Making*, *13*(1), 71. https://doi.org/10.1186/1472-6947-13-71

[31] Ferraiolo, D., Cugini, J., & Kuhn, R. (1995). Role-Based Access Control (RBAC): Features and Motivations. *Proceedings of the 11th Annual*. Computer Security Applications Conference, New Orleans, LA,. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=916537 (Accessed May 7, 2021)

[32] Gajanayake, R., Iannella, R., & Sahama, T. (2011). Sharing with Care: An Information Accountability Perspective. *IEEE Internet Computing*, *15*(4), 31–38. https://doi.org/10.1109/MIC.2011.51

[33] Gale, N. K., Heath, G., Cameron, E., Rashid, S., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology*, *13*(1), 117. https://doi.org/10.1186/1471-2288-13-117

[34] Garba, A. A., & Bade, A. M. (2021). The Current state of cybersecurity readiness in Nigeria organizations. *International Journal of Multidisciplinary and Current Educationall Research*, *3*(1), 154–162.

[35] George, A., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.

[36] George, J., & Bhila, T. (2019). Security, Confidentiality and Privacy in Health of Healthcare Data. *International Journal of Trend in Scientific Research and Development, 3*(4).

[37] Gross, J. B., & Rosson, M. B. (2007). End user concern about security and privacy threats. *Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS ’07*, 167. https://doi.org/10.1145/1280680.1280711

[38] Harris, M., & Furnell, S. (2012). Routes to security compliance: Be good or be shamed? *Computer Fraud & Security*, *2012*(12), 12–20. https://doi.org/10.1016/S1361-3723(12)70122-7

[39] Höne, K., & Eloff, J. H. P. (2002). Information security policy—What do international information security standards say? *Computers & Security*, *21*(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7

[40] Househ, M. S., Borycki, E. M., Rohrer, W. M., & Kushniruk, A. W. (2014). Developing a framework for meaningful use of personal health records (PHRs). *Health Policy and Technology*, *3*(4), 272–280. https://doi.org/10.1016/j.hlpt.2014.08.009

[41] Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, *49*(2), 99–110. https://doi.org/10.1016/j.im.2011.12.005

[42] Hult, V. H., & Wynn, E. (2019). *Information integrity and human infrastructure in digital health care*. 1–10. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1355381&dswid=560

[43] Ibeneme, S., Ongom, M., Ukor, N., & Okeibunor, J. (2020). Realigning Health Systems Strategies and Approaches; What Should African Countries Do to Strengthen Health Systems for the Sustainable Development Goals? *Frontiers in Public Health*, *8*, 372. https://doi.org/10.3389/fpubh.2020.00372

[44] Identity Theft Resource Center. (2021, March 17). *Data breach charts*. https://notified.idtheftcenter.org/s/ 2021

[45] Idowu, O. E. (2016). Criticisms, constraints and constructions of case study research strategy. *Asian Journal of Business and Management*, *4*(5).

[46] *Internet users Distribution in the World -2020 Q3*. (2020, September 20). Internet World Stats. https://www.internetworldstats.com/stats.htm

[47] Jaeger, L., & Eckhardt, A. (2018). When Colleagues Fail: Examining the Role of Information Security Awareness on Extra-Role Security Behaviors. *Association for Information Systems AIS Electronic Library*.

[48] Khan, S. I., & Hoque, A. (2016). Digital health data: A comprehensive review of privacy and security risks and some recommendations. *Computer Science Journal of Moldova*, *24*(2(7)), 273–292.

[49] Konduri, N., Aboagye-Nyame, F., Mabirizi, D., Hoppenworth, K., Kibria, M. G., Doumbia, S., Williams, L., & Mazibuko, G. (2018). Digital health technologies to support access to medicines and pharmaceutical services in the achievement of sustainable development goals. *DIGITAL HEALTH*, *4*, 205520761877140. https://doi.org/10.1177/2055207618771407

[50] Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*, *20*(1), 44–51. https://doi.org/10.1136/amiajnl-2012-000906

[51] Lord, N. (2020, September 17). Healthcare Cybersecurity: Tips for Securing Private Health Data by Nate Lord. *Digital Guardian*. https://digitalguardian.com/blog/healthcare-cybersecurity-tips-securing-private-health-data#:~:text=Encryption%20is%20one%20of%20the,gain%20access%20to%20the%20data

[52] Marcelo, A., Medeiros, D., Roth, S., & Wyatt, P. (2018). *Transforming Health Systems Through Good Digital Health Governance*. Asian Development Bank. https://doi.org/10.22617/WPS189244-2

[53] Mohd Ishak, N., & Abu Bakar, A. Y. (2014). Developing Sampling Frame for Case Study: Challenges and Conditions. *World Journal of Education*, *4*(3), p29. https://doi.org/10.5430/wje.v4n3p29

[54] Moyer, M. J., & Abamad, M. (2001). Generalized role-based access control. *Proceedings 21st International Conference on Distributed Computing Systems*, 391–398. https://doi.org/10.1109/ICDSC.2001.918969

[55] Murray, E., Hekler, E. B., Andersson, G., Collins, L. M., Doherty, A., Hollis, C., Rivera, D. E., West, R., & Wyatt, J. C. (2016). Evaluating Digital Health Interventions. *American Journal of Preventive Medicine*, *51*(5), 843–851. https://doi.org/10.1016/j.amepre.2016.06.008

[56] National Research Council. (1997). *For the Record: Protecting Electronic Health Information* (p. 5595). National Academies Press. https://doi.org/10.17226/5595

[57] *Nigeria Data Protection Regulation*. (2019). The National Information Technology Development Agency (NITDA. https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf

[58] Noor, K. B. M. (2008). Case study: A strategic research methodology." American journal of applied sciences. *American Journal of Applied Sciences*, *5*(11), 1602–1604.

[59] Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116–125. https://doi.org/10.5897/IJSA2013.0510

[60] Olanrewaju, R. F., Ali, N., Khalifa, O., & Manaf, A. A. (2013). CT in telemedicine: Conquering privacy and security issues in health care services. *Electronic Journal of Computer Science and Information Technology*, *4*(1).

[61] Oloyede, R. (2018, November 23). *Nigeria: Privacy And Security In Nigeria's Health-Care Sector* [Knowledge platform]. Modaq. https://www.mondaq.com/nigeria/privacy-protection/757682/privacy-and-security-in-nigeria39s-health-care-sector

[62] Onuiri, E. E., Idowu, S. A., & Komolafe, O. (2015). Electronic Health Record Systems and CyberSecurity Challenges. *2nd Covenant University Conference*. African Development Issues (CU-ICADI), Ota, Nigeria.

[63] Onyemelukwe, C. (2016). Stigma and Mental Health in Nigeria: Some Suggestions for Law Reform. *Journal of Law, Policy and Globalization*, *55*, 63–68.

[64] Page, B. B. (2017). Exploring Organizational Culture for Information Security in Healthcare Organizations: A Literature Review. *2017 Portland International Conference on Management of Engineering and Technology (PICMET)*, 1–8. https://doi.org/10.23919/PICMET.2017.8125471

[65] Pandey, A. K., Khan, A. I., Abushark, Y. B., Alam, Md. M., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Key Issues in Healthcare Data Integrity: Analysis and Recommendations. *IEEE Access*, *8*, 40612–40628. https://doi.org/10.1109/ACCESS.2020.2976687

[66] Panorama Consulting Group. (2020, January 22). Why Cybersecurity Requires a Change Management Plan. *Panorama Consulting*. https://www.panorama-consulting.com/why-cybersecurity-requires-a-change-management-plan/

[67] Patel, N. (2020). SOCIAL ENGINEERING AS AN EVOLUTIONARY THREAT TO INFORMATION SECURITY IN HEALTHCARE ORGANIZATIONS. *Jurnal Administrasi Kesehatan Indonesia*, *8*(1), 56. https://doi.org/10.20473/jaki.v8i1.2020.56-64

[68] Peikari, H. R., T., R., Shah, M. H., & Lo, M. C. (2018). Patients’ perception of the information security management in health centers: The role of organizational and human factors. *BMC Medical Informatics and Decision Making*, *18*(1), 102. https://doi.org/10.1186/s12911-018-0681-z

[69] Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, *14*(2), 37–49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6

[70] Renaud, K., & Goucher, W. (2012). Health service employees and information security policies: An uneasy partnership? *Information Management & Computer Security*, *20*(4), 296–311. https://doi.org/10.1108/09685221211267666

[71] Ritchie, J., & Spencer, L. (1994). Qualitative data analysis for applied policy research. In A. Bryman & R. G. Burgess (Eds.), *Analyzing qualitative data* (pp. 173–194). Taylor & Francis. https://doi.org/10.4324/9780203413081_chapter_9

[72] Ross, R., McEvilley, M., & Oren, J. C. (2018). *Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, volume 1* (NIST SP 800-160v1; p. NIST SP 800-160v1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v1

[73] Runeson, P., Host, M., Rainer, A., & Regnell, B. (2012). *Case study research in software engineering: Guidelines and examples. John Wiley & Sons.* John Wiley & Sons.

[74] Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. INFORMATION MANAGEMENT JOURNAL-PRAIRIE VILLAGE. *The Information Management Journal*, *39*(4).

[75] Saminu, A. (2019). A Framework for Effective Information System Security Management in Katsina State Healthcare Organizations. *International Journal of Engineering Applied Sciences and Technology*, *4*(7), 88–94.

[76] Sandhu, R., Ferraiolo, D., & Kuhn, R. (2000). The NIST model for role-based access control: Towards a unified standard. *ACM Workshop on Role-Based Access Control*, *10*. https://web2.utc.edu/~Li-Yang/cpsc4660/rbac-00.pdf

[77] Sarbanes-oxley act. Washington DC., (20o2) (testimony of Paul Sarbanes & Michael G Oxley). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.474.2105&rep=rep1&type=pdf

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

[79] Shoniregun, C. A., Dube, K., & Mtenzi, F. (2010). Introduction to e-Healthcare Information Security. In S. Jajodia (Ed.), *Electronic Healthcare Information Security* (Vol. 53, pp. 1–27). Springer US. https://doi.org/10.1007/978-0-387-84919-5_1

[80] Singh, N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, *27*(5). https://www.emerald.com/insight/content/doi/10.1108/JEIM-07-2013-0052/full/html?journalCode=jeim

[81] Sogomonjan, M. (2020). *Reducing the administrative burden of primary healthcare system through implementing digital mental health services in Estonia*. Tallinn University of Technology.

[82] Srivastava, A., & Thomson, S. B. (2009). Framework analysis: A qualitative methodology for applied policy research. *Journal of Administration and Governance*, *4*(2).

[83] Suleiman, D. (2016). Mental health disorders in Nigeria: A highly neglected disease. *Annals of Nigerian Medicine*, *10*(2), 47. https://doi.org/10.4103/0331-3131.206214

[84] Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management*, *17*(2), 179–186. https://doi.org/10.1007/s10799-015-0252-2

[85] Tomšů, M. (2020). Analysis of the information environment in healthcare organizations in terms of information security. *Košická Bezpečnostná Revue (*, *10*(2), 171–184.

[86] Torous, J., Andersson, G., Bertagnoli, A., Christensen, H., Cuijpers, P., Firth, J., Haim, A., Hsin, H., Hollis, C., Lewis, S., Mohr, D. C., Pratap, A., Roux, S., Sherrill, J., & Arean, P. A. (2019). Towards a consensus around standards for smartphone apps and digital mental health. *World Psychiatry*, *18*(1), 97–98. https://doi.org/10.1002/wps.20592

[87] Ugochukwu, O., Mbaezue, N., Lawal, S. A., Azubogu, C., Sheikh, T. L., & Vallières, F. (2020). The time is now: Reforming Nigeria’s outdated mental health laws. *The Lancet Global Health*, *8*(8), e989–e990. https://doi.org/10.1016/S2214-109X(20)30302-8

[88] United Nations Food Population Fund. (2020). World Population Dashboard Nigeria. *World Population Dashboard Nigeria*. https://www.unfpa.org/data/world-population/NG

[89] Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

[90] Veiga, A. D., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136

[91] Verizon Enterprise. (2018). *2018 Data Brech Investigations Report* (11th edition). Verizon. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

[92] von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security*, *25*(3), 165–168. https://doi.org/10.1016/j.cose.2006.03.004

[93] Wanyony, S. (2019, September 23). 4 Organizations Improving Mental Health in Nigeria. *The Borgen Project*. https://borgenproject.org/mental-health-in-nigeria/

[94] Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, *24*(1), 43–57. https://doi.org/10.1016/j.ijinfomgt.2003.12.003

[95] Whitman, M. E., Anthony, T. M., & Robert, A. J. (2001). Information Systems Security and the Need for Policy. In *Information Security Management: Global Challenges in the New Millennium* (Ed. Gurpreet Dhillon, pp. 10–20). IGI Global.

[96] *WHO guideline: Recommendations on digital interventions for health system strengthening*. (2019). World Health Organization. https://www.ncbi.nlm.nih.gov/books/NBK541902/

[97] WHO-AIMS. (2006). *WHO-AIMS report on Mental Health System in Nigeria*. World Health Organization and Ministry of Health. https://www.who.int/mental_health/evidence/nigeria_who_aims_report.pdf

[98] Widup, S. (2018, February 3). New report puts healthcare cybersecurity back under the microscope. *Verizon News*. https://www.verizon.com/about/news/new-report-puts-healthcare-cybersecurity-back-under-microscope

[99] Williams, F., & Boren, S. (2008). The role of the electronic medical record (EMR) in care delivery development in developing countries: A systematic review. *Journal of Innovation in Health Informatics*, *16*(2), 139–145. https://doi.org/10.14236/jhi.v16i2.685

[100] Wise, J. (2017). Mental health: Patients and service in crisis. *BMJ*, j1141. https://doi.org/10.1136/bmj.j1141

[101] World Health Organization. (2018). *Interview with Victor Ugo, founder, Mentally Aware Nigeria Initiative*. https://www.who.int/health-topics/urban---health/cities-spotlight/mental-health-in-cities/interview-with-victor-ugo

[102] Yaokumah, W. (2014). Information security governance implementation within Ghanaian industry sectors: An empirical study. *Information Management & Computer Security*, *22*(3), 235–250. https://doi.org/10.1108/IMCS-06-2013-0044

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis

I Faith Adesuwa Idialu with the date of birth: 08/05/1989

1. Allow the Tallinn University of Technology without any charges (plain licence) for my work ("Information Security in Digital Mental Healthcare in Nigeria"), supervised by (Prof Dr. Dr. Robert Krimmer and Melita Sogomonjan).
   1.1. To be reproduced for preservation and electronic publication of the graduation thesis, incl. to be entered in the digital repository of the library of Tallinn University of Technology until the end of the copyrighted time limit;
   1.2. to be available to the public through the Tallinn University of Technology online environment, including the digital repository of the library of Tallinn University of Technology until the end of the copyrighted limit.
2. I am aware, that all rights, named in section 1, will remain to the author.
3. I confirm that by allowing the use of the Plain licence no intellectual rights of third parties will be violated as set in the personal data protection Act and other legislation.

10.05.2021