UNIVERSITY OF KWAZULU-NATAL
COLLEGE OF LAW AND MANAGEMENT STUDIES
SCHOOL OF LAW, HOWARD COLLEGE

Securing the privacy of patients' electronic personal information in South African hospitals during COVID-19

Ashwini Singh
219052945

This mini-dissertation is submitted in partial fulfilment of the requirements for the degree of Master of Laws in Medical Law

Supervisor: Dr FD Mnyongani
Co-Supervisor: Dr H Patrick

2021

DECLARATION REGARDING ORIGINALITY

I, Ashwini Singh, declare that:

A. The research reported in this dissertation, except where otherwise indicated, is my original research.

B. This dissertation has not been submitted for any degree or examination at any other university.

C. This dissertation does not contain any other person's data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

D. This dissertation does not contain any other person's writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

   a. their words have been re-written, but the general information attributed to them has been referenced;

   b. where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

E. Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was written by myself alone and have fully referenced such publications.

F. This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the sources are detailed in the dissertation/thesis and in the References sections.

Signed: 

Date: 29 November 2021

ABSTRACT

South African organisations have been noticeably ill-prepared in their prevention of data breaches, even amidst the coronavirus public health predicament, where a palpable onslaught of cyberattacks targeting the healthcare sector has arisen locally and globally. The true victims of hospital data breaches in particular remain the patients, who are ultimately deprived of their constitutional right to privacy when electronic records containing their personal information become 'free real estate' to cybercriminals. The crux of deterrence of such cybercrime is within the principle of prevention via the utilisation of appropriate cybersecurity and information security controls at an organisational level. With the newly promulgated Protection of Personal Information Act (2013) and Cybercrimes Act (2020), greater legal scrutiny is placed upon South African hospitals to defend the privacy of patients' data stored on their systems. As per the National Health Act (2003), hospitals have a further obligation to maintain the confidentiality of their patients' records. This study proposes effective cybersecurity and information security practices that lend support in ensuring the confidentiality, integrity and accessibility of patients' electronic personal information records in South African private hospitals. Compliance thereof would definitively result in enhanced service delivery and data security for these hospitals and patients alike, whilst adhering to the national legislative requirements.

ACKNOWLEDGEMENTS

When I was in high school, my programming teacher once said that problems were opportunities for creativity. I still admire this sentiment.

Every day, we are presented with challenges. In addition, every day, we are given opportunities to energise our creativity and overcome these challenges.

In the words of philosopher Sun Tzu:

> "In the midst of chaos, there is also opportunity."
> – *The Art of War*

I dedicate this dissertation to all individuals who have resiliently fought against cybercrime, even in the face of a global health crisis.

I would like to thank my supervisors, Dr Patrick and Dr Mnyongani, for their guidance and advisory throughout the writing of this dissertation.

I further thank my parents and my sister for their support throughout my studies, and for the much-needed humour.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

4G	4th Generation
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
CD	Compact Disc
COVID-19	Coronavirus
DDoS	Distributed Denial-of-Service
DoH	Department of Health
DoS	Denial-of-Service
ECTA	Electronic Communications and Transactions Act 25 of 2002
EHR	Electronic Healthcare Record
EPR	Electronic Patient Record
ERM	Enterprise Risk Management
EVDS	Electronic Vaccination Data System
GG	*Government Gazette*
GHz	Gigahertz
GN	Government Notice
HPCSA	The Health Professions Council of South Africa
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization

ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LTE	Long-Term Evolution
MAC	Media Access Control
NHA	National Health Act 61 of 2003
NIST	National Institute of Standards and Technology
POPIA	Protection of Personal Information Act 4 of 2013
PSK	Pre-Shared Key
QR	Quick Response
ROM	Read-Only Memory
SSID	Secure Set Identifier
SSL	Secure Sockets Layer
TKIP	Temporal Key Integrity Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WHO	World Health Organization

CHAPTER ONE

INTRODUCTION AND BACKGROUND

1.1. THE CORONAVIRUS

1.1.1. The prevalence of the coronavirus in South Africa

The coronavirus[1] (COVID-19) is an infectious disease that is primarily transmitted through droplet infection.[2] The South African Department of Health[3] (DoH) reported that COVID-19 emanated from China in 2019 and has spread globally since.[4] According to the World Health Organization[5] (WHO), COVID-19 retained pandemic status[6] throughout the years of 2020 and 2021 due to its devastating international mortality rate.[7]

Consequently, the South African government announced a period of national lockdown as per the Disaster Management Act 57 of 2002 on 15 March 2020.[8] The initial regulations governing the national lockdown in South Africa were stipulated in GN 398 *GG* 43148 of 25 March 2020, which subsequently received amendments. As of early November 2021, the DoH reported that more than two million South Africans were infected with COVID-19, which resulted in over 89 000 deaths nationally.[9]

---

[1] Hereafter referred to as 'COVID-19'.
[2] WebMD 'Coronavirus and COVID-19: What You Should Know' available at *https://www.webmd.com*, accessed on 31 October 2021.
[3] Hereafter referred to as the 'DoH'.
[4] DoH 'About COVID-19 (Coronavirus)' available at *https://sacoronavirus.co.za*, accessed on 28 July 2021.
[5] Hereafter referred to as the 'WHO'.
[6] WHO 'Coronavirus' available at *https://www.who.int*, accessed on 25 July 2021.
[7] WHO 'WHO Coronavirus (COVID-19) Dashboard' available at *https://covid19.who.int*, accessed on 31 October 2021.
[8] DoH 'Statement by President Cyril Ramaphosa on measures to combat COVID-19 epidemic' available at *https://sacoronavirus.co.za,* accessed on 28 July 2021.
[9] DoH 'Update on Covid-19 (Saturday 30 October 2021)' available at *https://sacoronavirus.co.za*, accessed on 1 November 2021.

1.1.2. The Electronic Vaccination Data System and coronavirus vaccine certificates

Owing to the devastating impact of COVID-19, vaccines were developed in order to prevent further infections and deaths.[10] In May 2021, the DoH proceeded to offer COVID-19 vaccinations to members of the public, with vaccination priority provided to persons over the age of 60.[11] The DoH utilised a website known as the 'Electronic Vaccination Data System'[12] (EVDS) to enable eligible persons to self-register for an appointment where the vaccine could be administered – this booking process involved the input of the individual's personal information into the EVDS.[13] Afterwards, the DoH implemented the successive phases[14] of its vaccine rollout strategy, whereby other age groups were permitted to register for a COVID-19 vaccine via the EVDS.

On 8 October 2021, the DoH launched digital vaccine certificates for persons who received the COVID-19 vaccine.[15] This Vaccine Certificate System required that individuals verify and submit their personal information in order to be issued a digital vaccine certificate confirming the person's vaccination status.[16] By 11 October 2021, more than 500 000 vaccine certificates were issued and downloaded in South Africa.[17] The DoH advised that digital vaccine certificates were to be kept confidential and not shared publicly because they contained personal information.[18] These COVID-19 vaccine certificates further included Quick Response[19] (QR) codes, which were intended to be readable exclusively by the authorities.[20]

---

[10] South African Government 'COVID-19 Coronavirus vaccine' available at *https://www.gov.za*, accessed on 2 November 2021.
[11] Joan van Dyk & Aisha Abdool Karim 'Phase 2 of SA's Covid-19 vaccine rollout starts: This is how it works' available at *https://www.news24.com*, accessed on 2 November 2021.
[12] Hereafter referred to as the 'EVDS'.
[13] South African Government 'Electronic Vaccination Data System (EVDS) Self Registration Portal' available at *https://www.gov.za*, accessed on 2 November 2021.
[14] South African Government 'COVID-19 Coronavirus vaccine strategy' available at *https://www.gov.za*, accessed on 2 November 2021.
[15] Jan Vermeulen 'South Africa's Covid-19 vaccine certificate goes live' available at *https://mybroadband.co.za*, accessed on 2 November 2021.
[16] DoH 'South African COVID-19 Vaccine Certificate System' available at *https://vaccine.certificate.health.gov.za*, accessed on 2 November 2021.
[17] Hanno Labuschagne 'This is how many vaccine certificates were issued last week' available at *https://mybroadband.co.za*, accessed on 2 November 2021.
[18] Jan Vermeulen 'Warning over vaccine certificate personal information' available at *https://mybroadband.co.za*, accessed on 2 November 2021.
[19] Hereafter referred to as 'QR' codes.
[20] BusinessTech 'South Africa is getting an updated vaccine certificate at the end of October – here are 9 other things to know' available at *https://businesstech.co.za*, accessed on 2 November 2021.

Kaspersky[21] describes QR codes as barcodes capable of storing data that can be easily read via a digital device.[22] QR codes can contain photos, text, internet links and digital media.[23] The DoH digital vaccine certificate issuance was initiated in accordance with existing COVID-19 passports,[24] certificates[25] and passes[26] available in other countries.

1.2. LITERATURE REVIEW

1.2.1. Patients and healthcare users

Section 27(1)(a) of the Constitution of the Republic of South Africa, 1996[27] states that everyone has the right of access to healthcare services. The National Health Act 61 of 2003[28] (NHA) predominantly utilises the term 'user' to refer to any person who receives treatment, with the terms 'inpatient' and 'outpatient' used to refer to persons receiving treatment from health establishments in particular.[29] Similarly, Section 1 of the Eastern Cape Provincial Health Act 10 of 1999 utilises 'health service user' as a reference to any person who uses public or private health services. Likewise, Section 1 of the KwaZulu-Natal Health Act 1 of 2009 employs 'health care user' to refer to any person who benefits from using healthcare services.

Comparatively, the Health Professions Council of South Africa[30] (HPCSA) refers to healthcare users as 'patients' throughout their guidelines regarding the keeping of patient records.[31] The WHO defines a patient as a 'person who is the recipient of healthcare.'[32] Given

[21] A cybersecurity company founded in 1997.
[22] Kaspersky 'QR Code Security: What are QR codes and are they safe to use?' available at *https://www.kaspersky.co.za*, accessed on 2 November 2021.
[23] Ibid.
[24] COVID Passport 'What is the COVID Passport for travelling?' available at *https://www.covidpasscertificate.com*, accessed on 2 November 2021.
[25] European Commission 'EU Digital COVID Certificate' available at *https://ec.europa.eu*, accessed on 2 November 2021.
[26] International Air Transport Association 'IATA Travel Pass Initiative' available at *https://www.iata.org*, accessed on 2 November 2021.
[27] Hereafter referred to as the Constitution.
[28] Hereafter referred to as the 'NHA'.
[29] NHA, s 1.
[30] Hereafter referred to as the 'HPCSA'.
[31] HPCSA 'GUIDELINES ON THE KEEPING OF PATIENT RECORDS BOOKLET 9' available at *https://www.hpcsa.co.za*, accessed on 26 August 2021.
[32] WHO 'Definitions of Key Concepts from the WHO Patient Safety Curriculum Guide (2011)' available at *https://www.who.int*, accessed on 26 August 2021.

the aforementioned minor differentiations, it is evident that the terms 'healthcare user' and 'patient' can be used interchangeably to refer to persons who use health services.

1.2.2. Hospitals and health establishments

The NHA classifies a hospital as a type of health establishment.[33] The NHA defines a 'health establishment' as any public or private facility used for inpatient or outpatient diagnosis, treatment or rehabilitation services.[34] The NHA further distinguishes between private health establishments (which are not owned by the state) and public health establishments (which are owned by the state).[35] This study will focus on private hospitals in particular, which are a type of private health establishment.

1.2.3. Records, data and personal information

Section 1 of the Protection of Personal Information Act 4 of 2013[36] (POPIA) endorses that a record consists of any recorded information, regardless of the form or medium to which the information was recorded. Similarly, Section 1 of the Cybercrimes Act 19 of 2020 states that data is classified as 'electronic representations of information in any form', which includes electronic records. The POPIA specifies that records can include:[37]

(i) written material;

(ii) information produced, recorded or stored by computer equipment (such as hardware or software);

(iii) books, maps, plans, graphs or drawings;

(iv) photographs, films, tapes or other devices containing visual images.

Moreover, the types of records detailed in the POPIA must be in the possession of a responsible party irrespective of when the record was created, and irrespective of whether or

[33] NHA, s 1.
[34] Ibid.
[35] Ibid.
[36] Hereafter referred to as the 'POPIA'.
[37] POPIA, s 1.

not the responsible party created the record.[38] A 'responsible party' is regarded as any private or public body (or person) who establishes a need for the processing of personal information.[39] The POPIA elaborates by defining 'personal information' as 'information relating to an identifiable, living, natural person'.[40] Examples of personal information include (but are not limited to):[41]

(a) information relating to a person's race, gender, sex, pregnancy, marital status, ethnicity, sexual orientation, age, mental health, disability, religion, culture, language;

(b) information relating to a person's education, medical, financial, criminal or employment history;

(c) any contact information that identifies the person, viz: email addresses, physical addresses and phone numbers;

(d) a person's biometric information;

(e) a person's opinions, views or preferences;

(f) any private or confidential correspondence sent by the person.

Any personal information is subject to processing, which includes the collection, dissemination and destruction of personal information belonging to a data subject.[42] The POPIA stipulates that a 'data subject' is 'the person to whom personal information relates'.[43] Section 26 of the POPIA restricts the processing of special personal information concerning a data subject's: religious beliefs, race, ethnicity, political persuasion, biometric information, trade union membership, health or sex life.[44] The POPIA further restricts the processing of proceedings whereby there are allegations of the data subject having committed a criminal offence.[45] However, the ensuing Section 27 of the POPIA states that the aforementioned restrictions on the processing of a data subject's special personal information can be waived if:

[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] Ibid.
[42] Ibid.
[43] Ibid.
[44] POPIA, s 26(a).
[45] POPIA, s 26(b).

(a) the data subject consents to the processing of special personal information;[46]

(b) the processing of a data subject's special personal information is required for a legal obligation or for the exercise or defence of a right;[47]

(c) the processing of a data subject's special personal information is required for compliance with an international public law obligation;[48]

(d) the processing of a data subject's special personal information is for historical, statistical or research purposes that are in the public interest and it is impossible to obtain consent;[49]

(e) the special personal information of the data subject has already been made public by the data subject;[50]

(f) Sections 28 and 33 of the POPIA are being complied with.[51]

Section 28 of the POPIA states that the prohibition on the processing of a data subject's special personal information is not applicable if such processing is conducted by religious organisations[52] or by other institutions where it is necessary for the spiritual welfare of the data subject, given the data subject has not objected to this processing.[53] Likewise, Section 33 of the POPIA states that the prohibition on the processing of a data subject's special personal information relating to criminal behaviour or biometric information is not applicable if such information is utilised by bodies who are required by the law to apply criminal law.[54] Similarly, further exceptions to processing limitations have been detailed within the POPIA.[55] Specifically, in terms of Section 32(1)(a) of the POPIA, the prohibition on the processing of personal information concerning a data subject's health or sex life does not apply to processing by medical professionals, healthcare insitutions or facilities (including private hospitals) if such processing is necessary for the proper treatment and care of the data subject.

---

[46] POPIA, s 27(1)(a).
[47] POPIA, s 27(1)(b).
[48] POPIA, s 27(1)(c).
[49] POPIA, s 27(1)(d).
[50] POPIA, s 27(1)(e).
[51] POPIA, s 27(1)(f).
[52] POPIA, s 28(1)(a).
[53] POPIA, s 28(1)(c).
[54] POPIA, s 33(1).
[55] These exceptions to the processing limitations are listed in s 29, s 30 and s 31 of the POPIA.

1.2.4. Electronic patient records and electronic healthcare records

The Norms and Standards Regulations Applicable to Different Categories of Health Establishments 2017 particularise that a health record is 'any record made by a health care provider, at the time of or shortly after seeing the user'.[56] Ademola Abidoye *et al* indicate that an Electronic Patient Record[57] (EPR) 'contains all the health-care-related information on one person' and that 'EPRs take the current paper-based documents and convert them to a digital format so that they are available in an electronic form'.[58]

Whereas, Ademola Adesina *et al* consider an Electronic Healthcare Record[59] (EHR) as 'digitally stored health care information about an individual within [a] time frame with the purpose of supporting continuity of care, education and research and ensuring confidentiality at all times', and it is further noted that an EPR forms part of an EHR.[60] EHRs can contain a patient's medical history, the results of their medical examinations, and personal information as per the POPIA.[61] The HPCSA considers the following items as part of a health record: referral letters from healthcare practitioners, laboratory reports, insurance forms and audio-visual records.[62]

1.2.5. Consent for the processing of personal information

In accordance with Section 11(1) of the POPIA, personal information may only be processed if the data subject consents to its processing. In the instance of children[63] as data subjects, a child's personal information can only be processed with the consent[64] of a competent person.[65]

---

[56] GN 67 *GG* 41419 of 2 February 2018, reg 1.
[57] Hereafter referred to as an 'EPR'.
[58] Ademola P Abidoye, Ademola O Adesina & Kehinde K Agbele *et al* 'Ensuring the security and privacy of information in mobile health-care communication systems' (2011) 107(9/10) *SAJS* 3.
[59] Hereafter referred to as an 'EHR'.
[60] Ademola Adesina, Kehinde Agbele & Henry Nyongesa 'ICT and Information Security Perspectives in E-Health Systems' (2010) 4(1) *Journal of Mobile Communication* 18.
[61] POPIA, s 1.
[62] HPCSA op cit note 31 at para 2.1.
[63] As per Section 1 of the Children's Act 38 of 2005, a child is defined as a person under the age of 18 years. Section 28(3) of the Constitution states the same.
[64] POPIA, s 35(1)(a).
[65] Parents or guardians qualify as competent persons.

In terms of Section 35(2) of the POPIA, a responsible party who wishes to process the personal information of a child must make an application to do so and receive approval thereof.[66]

However, the POPIA provisions for alternative circumstances whereby consent can be provided for the processing of a child's personal information, which include: if there is prior consent[67] from a competent person; if it is necessary for the defence or exercise[68] of a legal right or obligation, including international public law[69] obligations; if it is for historical, statistical or research[70] purposes; if the personal information has already been made public by the child.[71]

1.2.6. Information security and cybersecurity

Avast[72] describes cybersecurity as the practice of protecting networks, systems, devices and data from unauthorised access.[73] Cisco[74] clarifies that information security is the facet of cybersecurity that deals specifically with data security where the objective is to protect and secure information against unauthorised access, modification and destruction.[75] IBM[76] elucidates that data security is the particular practice of defending electronic information against unauthorised access, corruption and theft.[77]

The triad of principles guiding information security, cybersecurity[78] and data security[79] are: confidentiality, integrity and availability of electronic information (data). Data availability focuses on the availability of the system (where data is stored) for the purposes of data

[66] Information Regulator (South Africa) 'APPLICATION FORM FOR AUTHORISATION TO PROCESS PERSONAL INFORMATION OF CHILDREN' available at *https://www.justice.gov.za*, accessed on 3 November 2021.
[67] POPIA, s 35(1)(a).
[68] POPIA, s 35(1)(b).
[69] POPIA, s 35(1)(c).
[70] POPIA, s 35(1)(d).
[71] POPIA, s 35(1)(e).
[72] A cybersecurity company founded in 1988.
[73] Avast 'What Is Cybersecurity' available at *https://www.avast.com,* accessed on 14 August 2021.
[74] A technology company founded in 1984.
[75] Cisco 'What is Information Security?' available at *https://www.cisco.com*, accessed on 17 June 2021.
[76] A technology corporation founded in 1911.
[77] IBM 'What is data security?' available at *https://www.ibm.com*, accessed on 3 November 2021.
[78] The Open University *Introduction to cybersecurity* (2016) 19.
[79] Ademola P Abidoye *et al* op cit note 58 at 4.

retrieval.[80] In contrast, data integrity is the practice of preventing the corruption of electronic recorded information (data),[81] and safeguarding the accuracy and consistency of this data throughout its lifecycle.[82] The International Organization for Standardization[83] (ISO) and International Electrotechnical Commission[84] (IEC) ISO/IEC 27002 standards prescribe information security and technology practices for prevention and response to information security risks.[85]

1.2.7. Privacy and confidentiality

Section 14 of the Constitution grants individuals the right to privacy. At the same time, Section 14(1) of the NHA states that all information concerning a healthcare user is to be kept confidential. An exception is declared in Section 14(2) of the NHA, which allows for the disclosure of a healthcare user's information if:

(a) the healthcare user consents to such disclosure in writing;[86]

(b) such disclosure is required by a court or the law;[87]

(c) non-disclosure of the information would be a threat to public health.[88]

David Sue *et al* identify confidentiality as a standard to which patients must be protected from disclosure of their information without their consent.[89] Jerome Singh differentiates between the concepts of privacy and confidentiality, whereby privacy is a lack of intrusion into personal information and confidentiality is exclusively in relation to the obligation of a trusted individual to refrain from disclosing sensitive information without permission.[90] Ames Dhai

[80] Ademola P Abidoye *et al* op cit note 58 at 4-5.
[81] Ademola P Abidoye *et al* op cit note 58 at 4.
[82] T Thulare, M Herselman & A Botha 'Data Integrity: Challenges in Health Information Systems in South Africa' (2020) 14(11) *International Journal of Computer and Information Engineering* 423.
[83] Hereafter referred to as the 'ISO'.
[84] Hereafter referred to as the 'IEC'.
[85] ISO *ISO/IEC 27002* (2013).
[86] NHA, s 14(2)(a).
[87] NHA, s 14(2)(b).
[88] NHA, s 14(2)(c).
[89] David Sue, Derald Wing Sue & Diane Sue *et al Understanding Abnormal Behavior* 11 ed (2016) 561.
[90] Jerome Amir Singh 'LAW AND THE HEALTH PROFESSIONAL IN SOUTH AFRICA' in Keymanthri Moodley (ed) *Medical ethics, law and human rights: A South African perspective* (2017) 151.

and David McQuoid-Mason maintain that practising confidentiality involves a relationship whilst upholding privacy does not.[91]

The HPCSA further contends that patients can expect that healthcare practitioners will hold their information in confidence, and that such confidentiality is crucial to ensuring the proper treatment of the patient.[92] The Patients' Rights Charter[93] authored by the DoH confirms a patient's right to confidentiality of information regarding that patient's healthcare and treatment, with the exception being disclosure by order of the court.[94]

1.2.8. Cybercrime

Sophos[95] considers a cybercriminal as a specific type of 'threat actor' whose objective is to compromise the cybersecurity of others via cybercrimes.[96] Kaspersky refines the scope of a cybercrime to any criminal activity targeting computers, networks and related devices.[97] NordVPN[98] regards a cyberattack as a specific type of cybercrime whereby an individual intentionally attacks a device or network using electronic means.[99]

The term 'hacking' has been colloquially used to refer to cyberattacks in which hackers (cybercriminals) unlawfully gain access to electronic information, devices, networks and systems without authorisation.[100] Uniquely, AVG[101] details that data breaches in particular consist of information exposure resulting from unauthorised access to the personal information

---

[91] Ames Dhai & David McQuoid-Mason *Bioethics, Human Rights and Health Law* 2 ed (2020) 87.
[92] HPCSA 'CONFIDENTIALITY: PROTECTING AND PROVIDING INFORMATION BOOKLET 5' available at *https://www.hpcsa.co.za,* accessed on 2 September 2021, para 4.1.
[93] DoH 'Patients' Rights Charter' available at *http://www.kznhealth.gov.za,* accessed on 10 August 2021.
[94] Supplementary legislation that supports a patient's right to the confidentiality of their healthcare information include: Section 13(1) of the Mental Health Care Act 17 of 2002; Section 7(1)(g) of the KwaZulu-Natal Health Act 1 of 2009; Section 13(1)(d) of the Children's Act 38 of 2005 and; Section 12(g) and Section 14(1) of the Eastern Cape Provincial Health Act 10 of 1999.
[95] A security software company founded in 1985.
[96] Sophos 'What is a Threat Actor and Why Should You Care?' available at *https://home.sophos.com*, accessed on 3 September 2021.
[97] Kaspersky 'Tips on how to protect yourself against cybercrime' available at *https://www.kaspersky.co.za*, accessed on 3 September 2021.
[98] A Virtual Private Network provider founded in 2012.
[99] NordVPN 'What is a cyber attack?' available at *https://nordvpn.com*, accessed on 3 September 2021.
[100] Malwarebytes 'Hacking definition: What is hacking?' available at *https://www.malwarebytes.com*, accessed on 3 September 2021.
[101] A cybersecurity company founded in 1991.

of product users.[102] Conversely, a Denial-of-Service[103] (DoS) or Distributed Denial-of-Service[104] (DDoS) cyberattack is one aimed at interrupting and overwhelming a system to the point of the system shutting down or going offline.[105] The purpose of a DoS or DDoS cyberattack is to make services provided by the targeted system unavailable to those who require them, which can have financial repercussions for the service provider.[106]

Another prominent method of perpetrating cybercrime is through the use of malware, which are malicious applications capable of causing damage to devices.[107] Specifically, a ransomware is a type of malware that holds devices, databases or networks ransom until the monetary amount demanded by the cybercriminal is paid by the victim.[108] In a number of ransomware cyberattacks, cybercriminals have threatened to delete all the data on the compromised system or device if the ransom was not paid by a specific date.[109] A report by Fortinet[110] found that ransomware cyberattacks increased globally by 1070% between July 2020 and June 2021, with an alarming number of organisations willing to pay the ransom to regain access to devices infected with ransomware.[111]

1.2.9. Cyberattack motives

In 2016, ITWeb[112] noted that different variants of malware required a comprehensive approach to cybersecurity and that South African organisations that were using outdated security tools (lacking updates) were vulnerable to cyberattacks.[113] In 2017, Panda Security[114] reported that South Africa ranked as one of the most attractive targets for cybercrime in the world, citing

[102] AVG 'Cybersecurity Basics' available at *https://www.avg.com*, accessed on 3 September 2021.
[103] Hereafter referred to as 'DoS'.
[104] Hereafter referred to as 'DDoS'.
[105] Fortinet 'What is a Cyber Attack?' available at *https://www.fortinet.com*, accessed on 15 November 2021.
[106] Ibid.
[107] Microsoft 'Understanding malware & other threats' available at *https://docs.microsoft.com*, accessed on 3 September 2021.
[108] McAfee 'What Is Ransomware?' available at *https://www.mcafee.com*, accessed on 3 September 2021.
[109] Ibid.
[110] A cybersecurity company founded in 2000.
[111] Fortinet 'The 2021 Ransomware Survey Report' available at *https://www.fortinet.com*, accessed on 15 November 2021.
[112] A South African cybersecurity publisher.
[113] Kirsten Doyle 'BUSINESSES ILL-PREPARED FOR CYBER ATTACKS' available at *http://v2.itweb.co.za*, accessed on 13 November 2021.
[114] A cybersecurity company founded in 1990.

malware as the preferred mode of perpetrating cyberattacks.[115] ITWeb further attributed a 22% increase in cyberattacks targeting South African organisations in 2019 to the use of third-party applications and services containing cybersecurity vulnerabilities.[116]

PricewaterhouseCoopers[117] offer three recurring motives for cyberattacks, namely:[118] financial gain; political or military advantage and; activism of a particular cause to which the cybercriminal supports. Zandi Lesame *et al* concur that cyberattacks involving identity theft are predominantly motivated by financial gain, whereby cybercriminals appropriate the victim's identity to steal funds from the victim's bank account.[119] The email cyberattacks against the Federal Bureau of Investigation[120] in November 2021 are a quintessential example of a politically motivated cyberattack seeking the compromise of confidential information held by that government agency.[121] Similarly, hacking for activism is frequently demonstrated by the hacker group Anonymous, who are known for leaking confidential organisational documents with the purpose of eliciting public scrutiny regarding the contents of those leaked documents.[122]

Accenture[123] asserts that South African organisations remain an attractive target for cyberattacks due to insufficient investment in cybersecurity,[124] as was illustrated in the cyberattacks against the Department of Justice, where it was suggested that the Department of Justice's failure to pay their Information Technology[125] (IT) unit resulted in inadequate cybersecurity to prevent cybercriminals from breaching the department's systems.[126]

---

[115] ITWeb 'Panda Cybersecurity Report 2017: Africa in top 10 targeted regions' available at *https://www.itweb.co.za*, accessed on 13 November 2021.
[116] ITWeb 'Cyber attackers eye SA businesses' available at *https://www.itweb.co.za*, accessed on 14 November 2021.
[117] A professional services company founded in 1998. Commonly referred to as 'PwC'.
[118] ITWeb 'PwC focuses on cyber attacks' available at *https://www.itweb.co.za*, accessed on 14 November 2021.
[119] Zandi Lesame, Blessing Mbatha & Sibongile Sindane (eds) *NEW MEDIA IN THE INFORMATION SOCIETY* 1 ed (2012) 188.
[120] A government agency in the United States of America (USA). Commonly referred to as the 'FBI'.
[121] BBC 'FBI probes cyber-attack emails sent from internal server' available at *https://www.bbc.com*, accessed on 15 November 2021.
[122] Dale Beran 'THE RETURN OF ANONYMOUS' available at *https://www.theatlantic.com*, accessed on 15 November 2021.
[123] A technology services company founded in 1989.
[124] Accenture 'INSIGHT INTO THE CYBERTHREAT LANDSCAPE IN SOUTH AFRICA' available at *https://www.accenture.com*, accessed on 15 November 2021.
[125] Hereafter referred to as 'IT'.
[126] Narissa Subramoney 'Calls for transparency after justice department cyber attack' available at *https://www.citizen.co.z*a, accessed on 15 November 2021.

1.2.10. Cyberattacks targeting health establishments during the coronavirus pandemic

A study by Joel Chigada and Rujeko Madzinga concluded that the number of cyberattacks targeting healthcare organisations increased exponentially during the COVID-19 pandemic, and noted that health establishments were an attractive target for data breaches because of the large amounts of personal information being stored therein.[127] Correspondingly, South Africa's Information Regulator[128] disclosed in September 2021 that more than 38 South African organisations suffered data breaches throughout the year.[129] News company the Independent Online[130] relayed the results of Comparitech's[131] 2020 survey, which indicated an increase in cybercrime in South Africa since the start of the national COVID-19 lockdown.[132] In furtherance, Ademola *et al* note that although EPRs allow for instantaneous access to patients' medical information, a critical shortcoming is the vulnerability of EPRs to hacking and unauthorised access – this is what cybercriminals have been exploiting.[133]

On 4 April 2020, the International Criminal Police Organization[134] issued a purple notice to all its member countries,[135] which warned that cybercriminals were targeting healthcare institutions with ransomware.[136] During the same month, the WHO issued a notice warning its member states[137] to be vigilant of phishing scam emails[138] purporting to be from the WHO.[139] Phishing cyberattacks are characterised by any attempt to steal sensitive information belonging

[127] Joel Chigada & Rujeko Madzinga 'Cyberattacks and threats during COVID-19: A systematic literature review' (2021) 23(1) *SAJIM* 4-5.
[128] The Information Regulator is the juristic person noted in terms of Section 39 of the Protection of Personal Information Act 4 of 2013, who has additional obligations as per the Promotion of Access to Information Act 2 of 2000.
[129] Jan Vermeulen 'Alarming number of security breaches in South Africa' available at *https://mybroadband.co.za*, accessed on 15 November 2021.
[130] Commonly referred to as 'IOL'.
[131] A technology research company founded in 2015.
[132] Shanice Naidoo 'Cybercrime on the rise since start of lockdown' available at *https://www.iol.co.za*, accessed on 22 November 2021.
[133] Ademola P Abidoye *et al* op cit note 58.
[134] Commonly referred to as the 'INTERPOL'.
[135] South Africa is a member country of the INTERPOL.
[136] INTERPOL 'Cybercriminals targeting critical healthcare institutions with ransomware' available at *https://www.interpol.in*, accessed on 17 June 2021.
[137] South Africa is a member country of the WHO.
[138] WHO 'Beware of criminals pretending to be WHO' available at *https://www.who.int*, accessed on 16 November 2021.
[139] WHO 'WHO reports fivefold increase in cyber attacks, urges vigilance' available at *https://www.who.int*, accessed on 3 September 2021.

to the target, such as the target's account password or access code.[140] Cloudflare[141] emphasises that phishing is conducted via spoofing, which is when a cybercriminal attempts to appear as a credible or reputable source to deceive the target into disclosing sensitive information.[142]

On 20 May 2020, Deloitte[143] reported that medical device suppliers worldwide were being targeted by keyloggers developed by cybercriminals.[144] A keylogger is a type of malware that tracks and logs key strokes typed on the keyboard of a computer or smartphone for the purposes of recreating passwords and access codes.[145] According to Deloitte, the objective of this keylogger cyberattack was to obtain access to confidential information regarding pharmaceutical and medical devices being deployed against COVID-19 in each country.[146]

On 9 June 2020, the Life Healthcare Group announced that its hospitals in South Africa fell victim to a cyberattack whereby administrative IT systems and email servers were compromised.[147] Other than a prospective data breach, it was speculated that the Life Healthcare Group was the victim of a ransomware cyberattack.[148] However, the extent of the data breach remained under investigation at that point in time.[149] Under those circumstances, the Life Healthcare Group switched to their back-up systems to continue functioning (although there were delays thereof).[150]

The Life Healthcare Group stated that they contained the cyberattack, and apologised for administrative and payment billing delays.[151] The Life Healthcare Group further advised that cybersecurity experts and forensic investigators were enlisted for assistance regarding this

---

[140] Cloudflare 'What is a phishing attack?' available at *https://www.cloudflare.com*, accessed on 16 November 2021.
[141] A website security company founded in 2009.
[142] Cloudflare op cit note 140.
[143] An accounting and financial services company founded in 1845.
[144] Deloitte 'COVID-19 Global Cyber risks: Attack surfaces expand amid return to work efforts' available at *https://www2.deloitte.com*, accessed on 17 June 2021.
[145] Norton 'What is a keylogger and how do I protect myself against one?' available at *https://us.norton.com*, accessed on 3 September 2021.
[146] Deloitte op cit note 144.
[147] Reuters 'South Africa's Life Healthcare hit by cyber attack' available at *https://www.reuters.com*, accessed on 17 November 2021.
[148] Edward-John Bottomley 'SA hit as hackers target hospitals during Covid-19 crisis – here's what Life may be facing' available at *https://www.businessinsider.co.za*, accessed on 17 November 2021.
[149] TIMESLIVE 'Hackers strike at Life Healthcare, extent of data breach yet to be assessed' available at *https://www.timeslive.co.za*, accessed on 17 November 2021.
[150] Aniruddha Ghosh 'Life Healthcare hit by cyber attack' available at *https://www.iol.co.za*, accessed on 17 November 2021.
[151] Life Healthcare Group 'LIFE HEALTHCARE CYBER INCIDENT Q & A' available at *https://www.lifehealthcare.co.za*, accessed on 17 November 2021.

incident, and that the authorities (including the Information Regulator) were notified of this cyberattack.[152] In their communiqué to the public,[153] the Life Healthcare Group made reference to the warning notice issued by the North Atlantic Treaty Organization[154] in June 2020 declaring that cybercriminals were targeting essential healthcare services amidst the COVID-19 pandemic,[155] and the Life Healthcare Group offered this as a possible motive for the cyberattack. By August 2020, the Life Healthcare Group reported that their affected IT systems had been fully restored.[156] The cyberattack therein was confirmed to have been a data breach that impacted upon the Life Healthcare Group's ability to complete patient billing, medical aid claims submissions, supplier invoice processing and the production of financial results.[157]

At present, there exists a body of journal articles and theses pertaining to EHRs, hospital cybersecurity management and cyberattacks during the COVID-19 pandemic. However, there is still an absence in the contextualisation thereof to South African health establishments during the COVID-19 pandemic, especially with the recent promulgation of the POPIA and the Cybercrimes Act.[158] This study explores such developments and proffers recommendations therein.

1.3. RATIONALE FOR STUDY AND COMMON THEMES

The principal rationale motivating this study is derived from every citizen and permanent resident of South Africa having a right to privacy in terms of Section 14 of the Constitution. Moreover, the POPIA states that it was passed with the purpose of giving greater effect to this constitutional right to privacy.[159] Likewise, the NHA advocates for the confidential treatment of healthcare users' information[160] in support of their right to privacy.

---

[152] Ibid.
[153] Ibid.
[154] Commonly referred to as 'NATO'.
[155] Sarah Coble 'NATO Condemns Cyber-Attacks' available at *https://www.infosecurity-magazine.com*, accessed on 17 November 2021.
[156] Samuel Mungadze 'Life Healthcare reveals damage caused by data breach' available at *https://www.itweb.co.za*, accessed on 17 November 2021.
[157] Ibid.
[158] Act 19 of 2020.
[159] POPIA, s 2(a).
[160] NHA, s 14.

In furtherance, unlawful access to electronic information is criminalised and related offences can be penalised in terms of Section 2(2)(a) of the Cybercrimes Act.[161] It is with the aforementioned legislation and the rights to privacy and confidentiality in mind that this study was conceived in order to suggest methods of protecting patients' electronic personal information in South African private hospitals, particularly amidst the landscape of increased cyberattacks targeting the healthcare sector in exploitation of the COVID-19 pandemic.

Currently, there is a gap in the existing body of research pertaining to data security in the South African health sector after the promulgation of the POPIA and Cybercrimes Act,[162] especially within the context of the COVID-19 pandemic. As such, the research themes for this study include: cybersecurity; healthcare policy; information and data security and; personal rights (to privacy) – there will be a specific focus on these themes during the COVID-19 pandemic in South Africa. This study seeks to address the aforementioned gap in existing research by examining newly promulgated legislation and proposing compliant cybersecurity and information security practices to protect patients' electronic personal information in South African private hospitals.

1.4. OBJECTIVES OF STUDY

The objectives of this study are as follows:

(i) To explore the extent to which the privacy of patients' electronic personal information is protected by South African law against unauthorised access.

(ii) To examine documented policies in South African private hospitals addressing the processing of patients' electronic personal information.

(iii) To suggest further actions South African private hospitals can take to prevent unauthorised access to patients' electronic personal information during the COVID-19 pandemic.

[161] Act 19 of 2020.
[162] Ibid.

1.5. RESEARCH QUESTIONS

The research questions which will be addressed in this study are as follows:

(a) To what extent is the privacy of patients' electronic personal information protected by South African law against unauthorised access?

(b) Which documented policies in South African private hospitals address the processing of patients' electronic personal information?

(c) What further action should South African private hospitals take to prevent unauthorised access to patients' electronic personal information during the COVID-19 pandemic?

1.6. RESEARCH DESIGN AND METHODOLOGY

This was a desktop study by literature review whereby existing information was analysed. The methodology used in this study included both primary and secondary sources as the main forms of data, sourced predominantly online via databases and relevant organisational websites (which included South African private hospitals' official websites).

Primary sources included South African legislation, particularly acts and *Government Gazette* regulations. Secondary sources included books, journal articles, news articles and organisational documents, namely policies and manuals from the Life Healthcare Group, Netcare, the Lenmed Group and Mediclinic. The above-mentioned documents were available electronically via those South African private hospitals' official websites and were an obligation in terms of existing legislation.[163]

This study did not entail the participation of human subjects[164] as it was conducted via desktop research due to the lockdown restrictions imposed by the COVID-19 pandemic and for the purposes of avoiding potential exposure to public health risks. As a result of the physical limitations imposed by the COVID-19 pandemic lockdown, organisational documents from the above-named four largest South African private hospital groups were utilised for this study

[163] Refer to Section 2.3 of Chapter 2 hereinafter for the relevant legislation.
[164] Refer to Appendix 1 annexed hereto.

due their accessibility and availability as online resources amidst the national lockdown restrictions.

1.7. STRUCTURE OF DISSERTATION

Chapter one contextualises the issue of COVID-19 in South Africa. This chapter offers a literature review that explores the concepts of cybersecurity, information security and cyberattacks during the COVID-19 pandemic as well as the relevant definitions elicited from the POPIA, the NHA and the Cybercrimes Act[165] (amongst other legislation). The research questions, objectives, rationale, methodology and design for this study are provided.

Chapter two explores South African legislation governing record-keeping obligations, lawful access to data and unauthorised access to personal information. Particularly, sections of the POPIA are detailed with emphasis placed upon the requirements of responsible parties in ensuring that the privacy of a data subject's personal information is upheld, and an overview of the eight lawful conditions for processing is detailed.

Chapter three examines hospital privacy policy documents and focuses on the terms relating to the protection of patients' electronic personal information records. Wireless network encryption and security vulnerabilities are considered, coupled with the device interconnectivity and local factors affecting device connectivity.

Chapter four suggests cybersecurity and information security interventions and controls to combat identified data security risks, citing existing frameworks in support thereof.

Chapter five is the conclusion, which consists of a summary of this study.

[165] Act 19 of 2020.

CHAPTER TWO

SOUTH AFRICAN LAW AND ACCESS TO PATIENTS' RECORDS

2.1. INTRODUCTION

This chapter commences by outlining lawful access to records in accordance with the legislation that is currently in effect, and there is a specific focus on the rights of patients in relation to accessing to their own medical records. In contrast, unlawful access to data – particularly electronic records – is examined alongside the statutory criminal offences that are the consequences for such actions. Furthermore, the record-keeping obligations of health establishments are detailed in addition to the associated impositions for the collection and retention of patients' records. Thereafter, the necessitation of organisational controls for safeguarding patient records containing personal information is elucidated. Additionally, the mandatory reporting procedures in the case of a data breach is explicated with an emphasis upon informing affected data subjects of the extent and impact of the data breach incident. Lastly, an overview of the POPIA's eight conditions for the lawful processing of personal information will be provided.

2.2. THE REPEAL OF SECTIONS OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

The Electronic Communications and Transactions Act 25 of 2002[166] (ECTA) was the former legislative authority pertaining to the protection of personal information[167] and lawful access to data.[168] On 1 July 2020, the POPIA was signed into effect with the grace period for compliance elapsing on 30 June 2021.[169] Hence, Chapter 8 of the ECTA[170] was replaced, resulting in the POPIA being the current overarching legislation governing the processing and

[166] Hereafter referred to as the 'ECTA'.
[167] ECTA, s 51.
[168] ECTA, s 86.
[169] POPIA 'Protection of Personal Information Act (POPI Act)' available at *https://popia.co.za,* accessed on 29 July 2021.
[170] ECTA, s 50-1.

protection of personal information and records therein.[171] However, Section 3(2)(b) of the POPIA endorses that any other legislation containing more extensive processing conditions than those mentioned in Chapter 3 of the POPIA take precedence. It is further noted that Section 3(2)(a) of the POPIA states that the POPIA applies to the exclusion of other legislation, unless otherwise noted in the aforementioned Section 3(2)(b).[172] Moreover, Chapter 13 of the ECTA[173] was replaced by the Cybercrimes Act[174] in 2021.

2.3. THE PROMOTION OF ACCESS TO INFORMATION ACT AND LAWFUL ACCESS TO RECORDS

As enshrined in Section 32(1) of the Constitution, every person has the right of access to:

(a) any information that is held by the state[175] and;

(b) any information that is held by another person and which is required for the exercise or protection of any rights.[176]

The Promotion of Access to Information Act 2 of 2000[177] (PAIA) was passed in compliance with Section 32(2) of the Constitution, which stipulates that national legislation must be enacted to give effect to the aforementioned rights detailed in Section 32(1) of the Constitution. In the context of the PAIA, a record means any recorded information (regardless of its form or medium) that is in the possession of a public body or a private body.[178] A public body therein refers to any department or institute of the government, and a private body is any organisation that is not government-owned.[179] Therefore, EPRs and EHRs held by hospitals are subject to the provisions of the PAIA,[180] because both private and public hospitals must comply with the PAIA.

[171] POPIA, s 3(1)(a).
[172] POPIA.
[173] ECTA, s 85-9.
[174] Act 19 of 2020.
[175] Constitution, s 32(1)(a).
[176] Constitution, s 32(1)(b).
[177] Hereafter referred to as the 'PAIA'.
[178] PAIA, s 1.
[179] Ibid.
[180] PAIA, s 3.

Accordingly, patients are entitled to have access to their own records that are being held by the hospitals they use. It is of note that the HPCSA requires that health practitioners maintain patient records, which must include personal identifying information of the patient.[181] The HPCSA states that a healthcare practitioner shall provide medical records to any person over the age of twelve who requests their medical records.[182] Healthcare practitioners cannot make medical records available to any other person without the authorisation of the patient concerned, unless ordered by a court or if it is a case where non-disclosure is a risk to public health.[183]

Section 30 of the PAIA provisions for circumstances where a third party may access medical records belonging to another person (usually with the prior written consent of that patient). Private bodies can impose restrictions on access to certain types of organisational information held in their custody (bearing in mind compliance with the POPIA). Hence, the requirement in terms of Section 51 and Section 52 of the PAIA, whereby public bodies and private bodies are compelled to devise a PAIA manual (that is made publicly available) to facilitate the process of requesting access to information held by those public bodies and private bodies – which includes public and private hospitals.

2.4. UNLAWFUL ACCESS TO DATA

Section 2(1) of the Cybercrimes Act[184] declares that any person who unlawfully and intentionally accesses a computer system or computer data storage medium is guilty of an offence. Unlawful access to a computer or system includes an unauthorised person: using the data on a computer or system without appropriate permission;[185] using the programs on a computer or system without appropriate permission;[186] disrupting the functioning of a computer or system without appropriate permission[187] and; copying the data from a computer

[181] HPCSA op cit note 31 at para 4.1.
[182] HPCSA op cit note 31 at para 11.1.
[183] Ibid.
[184] Act 19 of 2020.
[185] Cybercrimes Act 19 of 2020, s 2(2)(b)(i).
[186] Cybercrimes Act 19 of 2020, s 2(2)(c)(i).
[187] Ibid.

or system without appropriate permission.[188] The ensuing Section 3 of the Cybercrimes Act[189] makes provision for the unlawful interception of data, whereby any person who unlawfully intercepts the data contained within a data system is guilty of an offence.

The Cybercrimes Act clarifies the concept of 'interception of data' as the viewing, capturing or copying of data, which is of a non-public nature.[190] Unlawful interference with data or a computer programme is considered an offence in terms of Section 5 of the Cybercrimes Act.[191] Furthermore, unlawful interference with computer systems is criminalised as per Section 6 of the Cybercrimes Act.[192] Expressly, any of the aforementioned acts of unlawful access to stored data (especially data containing EHRs and EPRs) constitutes a cybercrime.

2.5. THE NATIONAL HEALTH ACT AND RECORD-KEEPING

Section 15 and Section 16 of the NHA permit healthcare practitioners and service providers (such as private hospitals) to access a patient's records for the purposes of treating the patient. In terms of the POPIA, a private hospital would be regarded as a responsible party for the processing of a patient's records in these circumstances.[193] Other than the specified purposes to which a patient's records are intended to be used for, Section 17(1) of the NHA explicitly details that a health establishment must implement control measures to prevent unauthorised access to patients' records.[194] The NHA further warns that individuals who commit any of the following offences can be fined, imprisoned or both:[195]

(a) Failing to prevent unauthorised access to health user records[196] as per Section 17(1) of the NHA;

(b) Falsifying records by adding, deleting or changing information contained in the record;[197]

[188] Cybercrimes Act 19 of 2020, s 2(2)(c)(ii).
[189] Act 19 of 2020.
[190] Cybercrimes Act 19 of 2020, s 3(4).
[191] Act 19 of 2020.
[192] Ibid.
[193] POPIA, s 1.
[194] Ibid.
[195] NHA, 17(2).
[196] NHA, s 17(2)(a).
[197] NHA, s 17(2)(b).

(c) Creating, changing or destroying records without the authority to do so;[198]

(d) Failing to create or change a record when required to;[199]

(e) Providing false information for inclusion in a record;[200]

(f) Copying part of a record without the authority to do so;[201]

(g) Connecting personal identification information of a healthcare user with their health condition, history or treatment without the authority to do so;[202]

(h) Gaining unauthorised access to records or record-keeping systems;[203]

(i) Connecting to computers or electronic systems where records are stored without the authority to do so;[204]

(j) Impairing the operation of systems where records are stored.[205]

Thus, the above-mentioned offences impose data security requirements for both health establishments and health practitioners alike with regard to the protection of patients' medical personal information (especially in the form of EHRs and EPRs),[206] which are compliant with the requirements of the POPIA. There is an additional obligation imposed by the HPCSA[207] in relation to patient records that are stored as data on Compact Discs[208] containing Read-Only Memory.[209] The HPCSA states that there must be protective measures to safeguard this data, such as encryption and password protection to prevent unauthorised persons from accessing the data.[210] The HPCSA further requires that a back-up copy of these CD-ROMs must be stored

[198] NHA, s 17(2)(c).
[199] NHA, s 17(2)(d).
[200] NHA, s 17(2)(e).
[201] NHA, s 17(2)(f).
[202] NHA, s 17(2)(g).
[203] NHA, s 17(2)(h).
[204] NHA, s 17(2)(i).
[205] NHA, s 17(2)(j).
[206] Healthcare practitioners are further required to exercise confidentiality.
[207] HPCSA op cit note 31 at para 12.1.5.
[208] Hereafter referred to as a 'CD'.
[209] Hereafter referred to as 'ROM'.
[210] HPCSA op cit note 31 at para 12.1.2.

at a separate site so that if the original CD is tampered with, the back-up CD can be relied upon to retrieve the data.[211]

2.6. THE PROTECTION OF PERSONAL INFORMATION ACT SECTIONS AND REGULATIONS

2.6.1. The security of personal information

In terms of Section 5(a) of the POPIA, data subjects retain the right to be notified when their personal information has been accessed by an unauthorised person. In this circumstance, the onus is upon the responsible party (such as a private hospital) to notify the affected data subject (such as a patient). Hence, in the event of a data breach, an organisation must notify the impacted data subjects whose personal information was compromised. Section 6 of the POPIA notes that the act does not extend to protecting personal information accessed and used by the authorities for prevention of criminal offences such as terrorism.[212]

The POPIA additionally imposes that personal information must be processed both lawfully[213] and in a manner that does not infringe upon the data subject's right to privacy,[214] with an emphasis on personal information being processed only for its designated purpose.[215] Section 11(1)(a) of the POPIA reiterates that personal information must be processed with the consent of the data subject. If a data subject objects to the processing of their personal information, the data subject must submit an objection form to the responsible party as per Regulation 2(1) in GN 1383 *GG* 42110 of 14 December 2018.

Personal information is generally expected to be collected directly from the data subject concerned,[216] unless the personal information: is available[217] as a public record;[218] has a child

[211] HPCSA op cit note 31 at para 12.1.4.
[212] POPIA, s 6(1).
[213] POPIA, s 9(a).
[214] POPIA, s 9(b).
[215] POPIA, s 10.
[216] POPIA, s 12(1).
[217] POPIA, s 12(2)(a).
[218] Public records are records that are made available to the public, which are exempt from the requirements of the POPIA as the information contained therein is public knowledge.

as the data subject[219] or; is not practically obtainable through methods compliant with the POPIA.[220] Section 13 of the POPIA reinforces the need for a specified purpose to which a data subject's personal information must be collected. A further consideration is that the restrictions imposed by Section 26 of the POPIA prohibit the processing of a data subject's special personal information unless permitted in terms of Section 27 and Section 33 of the POPIA.

Thereinafter, Section 14 of the POPIA places a restriction upon the retention of records containing personal information by requiring that such records be disposed of within a reasonable timeframe after they have been used for their intended purpose. Section 16 of the POPIA mandates that responsible parties must take steps to ensure the accuracy of stored personal information, which is in tandem with the three aforementioned principles of information security (confidentiality, integrity and accessibility). There is a further obligation in terms of Section 18 of the POPIA to ensure that data subjects are aware of which personal information items are being collected and for what purpose this collected personal information is to be used.

Markedly, the entirety of Section 19(1) of the POPIA details that a responsible party must maintain the integrity and confidentiality of stored personal information by preventing: damage or unauthorised destruction of personal information[221] and; unlawful access to personal information.[222] Thereupon, Section 19(2) of the POPIA compels responsible parties to:

(a) identify internal and external risks to stored personal information;[223]

(b) establish and maintain safeguards against identified risks;[224]

(c) regularly verify the effective implementation of safeguards in use;[225]

(d) ensure that safeguards are continually updated to accommodate new risks.[226]

Section 19(3) of the POPIA indicates that responsible parties must have due regard for accepted information security practices (such as the ISO/IEC 27002) and procedures used to

[219] POPIA, s 12(2)(b).
[220] POPIA, s 12(2)(f).
[221] POPIA, s 19(1)(a).
[222] POPIA, s 19(1)(b).
[223] POPIA, s 19(2)(a).
[224] POPIA, s 19(2)(b).
[225] POPIA, s 19(2)(c).
[226] POPIA, s 19(2)(d).

protect information, and responsible parties may have to comply with prescribed rules and regulations. It is of note that the POPIA permits a responsible party to utilise an operator, which is a person who processes personal information on behalf of a responsible party.[227] This entitles responsible parties (such as private hospitals) to use third-parties (such as cloud storage companies) to process and store personal information belonging to data subjects (the patients). However, the responsible party is still required to protect the personal information of data subjects by ensuring that the operator is maintaining personal information security safeguards, irrespective of who the responsible party has enlisted to process such information on their behalf.

2.6.2. Data breaches

Section 22 of the POPIA describes the actions that should be taken if a data subject's personal information is being accessed or acquired by an unauthorised person, as is the case when a data breach occurs. Specifically, Section 22(1) of the POPIA states that upon a data breach incident, both the Information Regulator[228] and the affected data subject[229] should be notified as soon as reasonably possible.[230] This notification of data breach must be in writing[231] and can be: sent via email[232] or postal mail;[233] announced on the responsible party's official website[234] or; published via the media.[235]

A notice issued to a data subject advising that their personal information has been compromised must include information regarding:[236]

(a) the potential consequences of the security incident;[237]

(b) the measures that the responsible party is taking to address the security incident;[238]

[227] POPIA, s 1.
[228] POPIA, s 22(1)(a).
[229] POPIA, s 22(1)(b).
[230] POPIA, 22(2).
[231] POPIA, s 22(4).
[232] POPIA, s 22(4)(b).
[233] POPIA, s 22(4)(a).
[234] POPIA, s 22(4)(c).
[235] POPIA, s 22(4)(d).
[236] POPIA, s 22(5).
[237] POPIA, s 22(5)(a).
[238] POPIA, s 22(5)(b).

(c) suggestions for the data subject to mitigate the impact of the security incident[239] and;

(d) the identity of the person or persons who caused the security incident (if known).[240]

Data subjects reserve the right to request access to their own records from any responsible party holding the data subject's personal information.[241] Data subjects may also request corrections or the deletion of their personal information,[242] which the responsible party must attempt to comply with.[243] Data subjects are further entitled to submit a complaint to the Information Regulator in accordance with Section 74 of the POPIA, given that the complaint is made in writing.[244]

Upon receipt of a written complaint, the Information Regulator has the ability to: investigate the complaint;[245] take immediate action on the matter;[246] decide to not take action[247] on the matter[248] or; refer the matter to the Enforcement Committee[249] or another regulatory body.[250] The Information Regulator possesses the ability to assist in a settlement between the parties involved in a complaint.[251] In the event of an unresolved dispute, a data subject can institute civil action for damages against the responsible party as per Section 99 of the POPIA.

2.6.3. 'Accountability' and 'processing limitation' conditions

The POPIA prescribes eight conditions for the lawful processing of personal information. The first condition is accountability in which the responsible party is required to ensure that the subsequent seven conditions for the lawful processing of personal information are complied with.[252]

[239] POPIA, s 22(5)(c).
[240] POPIA, s 22(5)(d).
[241] POPIA, s 23(1).
[242] POPIA, s 24(1).
[243] POPIA, s 24(2).
[244] POPIA, s 75(1).
[245] POPIA, s 76(1)(a).
[246] POPIA, s 76(1)(b).
[247] POPIA, s 76(1)(c).
[248] POPIA, s 77.
[249] POPIA, s 76(1)(e).
[250] POPIA, s 78.
[251] POPIA, s 80.
[252] POPIA, s 8.

The second condition, described as 'processing limitation', stipulates that personal information must be processed lawfully[253] and reasonably in order to not infringe upon the data subject's privacy.[254] This condition advocates for minimal processing of personal information, whereby such information must only be processed for its intended purpose and not excessively therein.[255] There is a further requirement for the responsible party to obtain consent from the data subject[256] and justify that the processing is:

(a) necessary for the performance of a contract wherein the data subject is a party;[257]

(b) an obligation in terms of the law;[258]

(c) to protect a legitimate interest of the data subject;[259]

(d) necessary for the performance of a public law duty;[260]

(e) to protect a legitimate interest of the responsible party.[261]

This condition allows for a data subject to withdraw consent[262] for processing at any time or object to the processing of personal information,[263] given that this objection is done in the prescribed manner and is not incompatible with processing activities that are mandated by the law.[264]

Additionally, Section 12(1) of the POPIA endorses that personal information must be collected directly from the data subject, unless:

(a) the information is already part of a public record;[265]

[253] POPIA, s 9(a).
[254] POPIA, s 9(b).
[255] POPIA, s 10.
[256] POPIA, s 11(1)(a).
[257] POPIA, s 11(1)(b).
[258] POPIA, s 11(1)(c).
[259] POPIA, s 11(1)(d).
[260] POPIA, s 11(1)(e).
[261] POPIA, s 11(1)(f).
[262] POPIA, s 11(2)(b).
[263] POPIA, s 11(3).
[264] POPIA, s 11(3)(a).
[265] POPIA, s 12(2)(a).

(b) the data subject has consented to the collection of such information from another source;[266]

(c) the collection of such information from another source does not prejudice the data subject;[267]

(d) the collection of such information from another source is necessary to comply with a revenue collection obligation[268] or to avoid prejudice in terms of punishment of offences;[269]

(e) the collection of such information from another source is necessary for the conduct of proceedings in a court or tribunal;[270]

(f) it is in the interests of national security;[271]

(g) it is a legitimate interest of the responsible party;[272]

(h) compliance would prejudice a lawful purpose for the collection;[273]

(i) compliance is not practical in the circumstances.[274]

2.6.4. The 'purpose specification' condition

The third condition for lawful processing is the specification of a purpose, which entails that personal information is to be collected for a defined and lawful purpose that is related to a function of the responsible party.[275] Section 14 of the POPIA endorses that records of personal information are not to be retained longer than is necessary for their intended purpose[276] unless:

(a) retention is required by the law;[277]

---

[266] POPIA, s 12(2)(b).
[267] POPIA, s 12(2)(c).
[268] POPIA, s 12(2)(d)(ii).
[269] POPIA, s 12(2)(d)(i).
[270] POPIA, s 12(2)(d)(iii).
[271] POPIA, s 12(2)(d)(iv).
[272] POPIA, s 12(2)(d)(v).
[273] POPIA, s 12(2)(e).
[274] POPIA, s 12(f).
[275] POPIA, s 13(1).
[276] POPIA, s 14(1).
[277] POPIA, s 14(1)(a).

(b) the responsible party reasonably requires the record for a longer period of time;[278]

(c) retention of the record is required by a contract between the parties;[279]

(d) the data subject has consented to the retention of the record.[280]

The POPIA further states that records of personal information can be retained for extended periods for historical, statistical or research purposes if the responsible party has established safeguards for these records.[281] However, the POPIA endorses that a responsible party must destroy records of personal information if the party is not authorised to retrain the record in terms of the aforementioned exceptions.[282] In terms of Section 14(5) of the POPIA, the destruction of a record containing personal information must be done in a manner where the record cannot be reconstructed in an intelligible form. In addition, a responsible party must restrict the processing of personal information if:

(a) the accuracy of the personal information is contested by the data subject;[283]

(b) the responsible party no longer has a purpose to which the personal information is required for;[284]

(c) the processing is unlawful;[285]

(d) the data subject opposes the destruction of the personal information and requests restriction of the record instead;[286]

(e) the data subject requests that data containing personal information be transferred to another system.[287]

[278] POPIA, s 14(1)(b).
[279] POPIA, s 14(1)(c).
[280] POPIA, s 14(1)(d).
[281] POPIA, s 14(2).
[282] POPIA, s 14(4).
[283] POPIA, s 14(6)(a).
[284] POPIA, s 14(6)(b).
[285] POPIA, s 14(6)(c).
[286] Ibid.
[287] POPIA, s 14(6)(d).

2.6.5. 'Further processing limitation', 'information quality' and 'openness' conditions

The fourth condition of lawful processing, listed as the 'further processing limitation', prescribes that collected personal information must be compatible with the purpose for which the information was collected.[288] Moreover, the ensuing fifth condition for lawful processing is information quality, whereby a responsible party must ensure that a data subject's personal information is complete, accurate and updated.[289] The sixth condition, openness, states that the responsible party must ensure that personal information documentation must be accessible to the data subject[290] in terms of Section 14 and Section 51 of the PAIA. This condition further requires that data subjects receive notification of when personal information is being collected and the purpose thereof.[291]

2.6.6. The 'security safeguards' condition

The seventh condition for lawful processing is security safeguards in which responsible parties must ensure the integrity and confidentiality of personal information (as detailed previously).[292] Should there be a security compromise affecting a data subject's personal information, the responsible party is required to notify the data subject as per Section 22 of the POPIA in accordance with the aforementioned procedure. Albeit a responsible party may appoint an operator to process personal information on their behalf, an operator must only process personal information with the knowledge of the responsible party,[293] and the operator must further treat this personal information with confidentiality unless directed otherwise by the law.[294] An operator is obliged to have a contract with the responsible party with relation to processing duties, and the responsible party must ensure that the operator maintains security measures for the protection of personal information.[295] Accordingly, it is the duty of the operator to inform the responsible party of any instance whereby the personal information of a data subject has been accessed or acquired by an unauthorised person.[296]

---

[288] POPIA, s 15(2).
[289] POPIA, s 16(1).
[290] POPIA, s 17.
[291] POPIA, s 18.
[292] POPIA, s 19.
[293] POPIA, s 20(a).
[294] POPIA, s 20(b).
[295] POPIA, s 21(1).
[296] POPIA, s 21(2).

2.6.7. The 'data subject participation' condition

The eighth and final condition for lawful processing is data subject participation. Section 23 of the POPIA states that identified data subjects are entitled to: request confirmation[297] that personal information is being held by a responsible party; request records[298] of this personal information and; correct personal information where applicable.[299] In the instance of a data subject requesting the correction or deletion[300] of a record containing personal information, a responsible party must attempt to comply with such a request.[301] It is further endorsed in Section 25 of the POPIA that provisions of the PAIA that permit access to records are also applicable under the POPIA.

2.7. CONCLUSION

This chapter outlined lawful access to records as per current legislation and focused on the rights of patients in relation to accessing to their own medical records. Unlawful access to data (namely electronic records) was examined alongside the related statutory criminal offences. Additionally, the record-keeping obligations of health establishments were detailed with the associated impositions for the collection and retention of patients' records. Thereafter, the necessitation of organisational controls for safeguarding patient records containing personal information was described. Furthermore, the mandatory reporting procedures in the case of a data breach was explicated with an emphasis upon advising affected data subjects of the extent and impact of the incident. Lastly, an overview of the POPIA's eight conditions for the lawful processing of personal information was provided.

[297] POPIA, s 23(1)(a).
[298] POPIA, s 23(1)(b).
[299] POPIA, s 23(2).
[300] POPIA, s 24(1).
[301] POPIA, s 24(2).

CHAPTER THREE

THE PRIVACY OF PATIENTS' ELECTRONIC PERSONAL INFORMATION IN SOUTH AFRICAN HOSPITALS

3.1. INTRODUCTION

This chapter critically examines the privacy policies belonging to private hospital groups operating in South Africa for legislative compliance, namely: the Life Healthcare Group, Netcare, the Lenmed Group and Mediclinic. Similarly, the record access policies for the above-mentioned private hospital groups are reviewed. Collectively, each private hospital group's documentation regarding patient record information security is to be explored. In addition, factors such as wireless network encryption and connected devices are considered for vulnerabilities that affect patient data, especially in the context of interconnected medical devices.

3.2. PERSONAL INFORMATION POLICIES

3.2.1. The Life Healthcare Group

The Life Healthcare Group owns multiple private hospitals throughout South Africa. The processing of personal information and regulation of access to records at all of the Life Healthcare Group's hospitals is governed by a standardised 'Privacy Notice' document[302] and PAIA manual[303] available on the Life Healthcare Group's official website, wherein their 2021 Privacy Notice[304] replaces their previous 2017 Privacy Notice.[305] The Life Healthcare Group's

[302] Life Healthcare Group 'Privacy Notice' available at *https://www.lifehealthcare.co.za*, accessed on 24 November 2021.
[303] Life Healthcare Group 'ACCESS TO INFORMATION MANUAL' available at *https://www.lifehealthcare.co.za,* accessed on 24 November 2021.
[304] Life Healthcare Group op cit note 302.
[305] Life Healthcare Group 'Privacy Notice' available at *https://www.lifehealthcare.co.za,* accessed on 12 June 2021.

PAIA manual was created in compliance with Section 51 of the PAIA, which mandates that organisations maintain a PAIA manual for regulating access to records. Likewise, the Life Healthcare Group's 2021 Privacy Notice[306] was made in compliance with Section 18 of the POPIA, which necessitates the need for a responsible party's openness for the lawful processing of a data subject's personal information.

The Life Healthcare Group's 2021 Privacy Notice outlines that patients' personal information is only collected in circumstances where it is required by the group's hospitals for healthcare services, or for the payment of rendered healthcare services – strictly with the consent of the patient,[307] which adheres to Section 11 of the POPIA where consent from a data subject (patient) is required for the processing of personal information. It is of note that the collection of personal information in this instance is defined and therefore compliant with Section 13 of the POPIA, whereby personal information must be collected for a specified purpose. Additionally, there is a disclaimer in relation to the disclosure of patients' personal information declaring that a patient's personal information may be disclosed for the execution of health services, if it is ordered by a court, or in the event that non-disclosure is a serious threat to public health.[308] A disclosure of this nature is permitted by Section 14(2) of the NHA. In furtherance, there is a general exemption to the processing of a patient's personal information in terms of Section 32(1)(a) of the POPIA, provided that a healthcare practitioner or establishment (such as a private hospital) can demonstrate that such porcessing is necessary for the proper treatment and care of the patient.

The 2021 Privacy Notice document further states that patients' personal information may be shared with third parties for the purposes of providing health services, processing payment, or if it is required by the law.[309] The use of third parties for the processing of personal information is subject to Section 21 of the POPIA, which states that responsible parties must ensure that third parties (operators) have security measures for the protection of the personal information belonging to data subjects (patients). The Life Healthcare Group has not specified which third parties they use. Consequently, the third parties' policies could not be reviewed. Based on the sixth condition of the POPIA, the Life Healthcare Group has not declared the

[306] Life Healthcare Group op cit note 302.
[307] Ibid.
[308] Ibid.
[309] Ibid.

level of protection afforded to data subjects' personal information by these third-party operators as per Section 18(1)(g) of the POPIA, specifically in the case of the third party being an international organisation or residing in a foreign country. It is of note that in terms of Section 18(1)(h) of the POPIA, only the responsible party is required to inform data subjects of the recipients or categories of recipients of their data. Furthermore, as per Section 23(1)(b) of the POPIA, a responsible party is permitted to provide the names of the recipients or categories of recipients to a data subject.

The 2021 Privacy Notice document by the Life Healthcare Group endorses that there are measures in place to ensure that a patient's personal information will be kept confidential and secure,[310] which addresses the confidentiality obligation in terms of Section 14 of the NHA. The Life Healthcare Group additionally states the following in reference to their security safeguards:[311]

> 'We [the Life Healthcare Group] have appropriate organisational and technical security measures in place to prevent unauthorized access or unlawful processing of Personal Information and to prevent Personal Information [from] being lost, destroyed or damaged. We monitor our information systems in an endeavour to ensure that the ongoing security is robust. All Personal Information you [the patient] provide to us is stored securely…The transmission of information via the internet cannot be guaranteed as completely secure.'

Albeit organisations are entitled to practice information and knowledge management in relation to their internal organisational controls, the Life Healthcare Group's privacy policy would benefit from more details. The Life Healthcare Group has stated their intention to be compliant with Section 19 of the POPIA with regard to security safeguards that protect patients' personal information against unauthorised access. This is demonstrated in the Life Healthcare Group's 2021 Privacy Policy document wherein the Life Healthcare Group specifies when they collect patients' personal information and for what purposes such information is utilised.[312] However, there is no reference to compliance with internationally accepted information security standards such as the ISO/IEC 27002 and whether or not these

[310] Ibid.
[311] Ibid.
[312] Ibid.

data protection standards are considered. There is also no reference to the security measures of the third parties that the Life Healthcare Group utilise for the processing of patients' personal information. Moreover, the Life Healthcare Group's endorsement that the information they transmit via the internet cannot be guaranteed as completely secure should have been supplemented by their existing cybersecurity policies for the prevention of security compromises and cybercrimes such as unlawful access.[313]

The Life Healthcare Group further discloses that they retain Closed-Circuit Television[314] security footage of their premises for a limited period of time as well as Internet Protocol[315] (IP) addresses upon user access to the Life Healthcare Group's websites.[316] However, there is no declaration of the period of retention of these records as well as patients' personal information and data which are included therein.

The Life Healthcare Group informs patients of their right to raise complaints with the hospital in their 'patient rights' document, which includes the prospect of referral to another dispute resolution body (such as the Information Regulator) should the complaint remain unresolved.[317] Annexure C of the corresponding PAIA manual contains an objection to the processing of personal information form, which patients can complete and submit to the Life Healthcare Group should they wish to.[318] This objection is aligned with Sections 11(3) and 11(4) of the POPIA, which permit a data subject to object to the processing of personal information. If there is an ongoing dispute between a patient (data subject) and the Life Healthcare Group relating to the patient's personal information, the patient is entitled to lodge a written complaint with the Information Regulator as per Form 5 of the Life Healthcare Group's PAIA manual.[319]

Paragraph 17 of the Life Healthcare Group's PAIA manual describes the group's grounds for the refusal of access to records, and provides remedies in the subsequent Paragraph 18.[320] The listed grounds for refusal are predominantly centred around retaining the privacy and confidentiality of personal information belonging to other individuals (patients), which may

[313] Cybercrimes Act 19 of 2020, s 2.
[314] Commonly referred to as 'CCTV'.
[315] Hereafter referred to as 'IP'.
[316] Life Healthcare Group op cit note 302.
[317] Life Healthcare Group 'patient rights and responsibilities' available at *https://www.lifehealthcare.co.za*, accessed on 24 November 2021.
[318] Life Healthcare Group op cit note 303.
[319] Ibid.
[320] Life Healthcare Group op cit note 303 at para 17-8.

appear as part of the requested records,[321] and which emphasises that the right to privacy for all data subjects must be considered.

Admittedly, the Life Healthcare Group's 2021 Privacy Notice[322] and the accompanying PAIA manual[323] are more comprehensive when compared to the 2017 Privacy Notice,[324] especially with the advent of the POPIA. Although both the Life Healthcare Group's 2017 Privacy Notice[325] and 2021 Privacy Notice[326] declare that personal information would only be retained for the period that such information is required for, neither of these notices endorse the exact duration for the retention of such records. Furthermore, the information security practices regarding the protection of personal information data on the Life Healthcare Group's 'limited access' servers remains scant and further elaboration regarding the security measures therein would be beneficial for their privacy policy, especially in light of the fact that the Life Healthcare Group's IT servers were targeted for the data breach that occurred in June 2020.

3.2.2. Netcare

Netcare indisputably owns the most private hospitals in South Africa.[327] Netcare's 'Information Manual'[328] and 'Netcare Privacy Policy'[329] documents regulate the processing of personal information in their numerous hospitals throughout the country. In Paragraph 3 of the Netcare Privacy Policy,[330] Netcare shares their principles for the processing of patients' personal information data, which underscore their patients' right to privacy (as per Section 14 of the Constitution). In the following Paragraph 4,[331] Netcare specifies the purposes for which Netcare uses the personal information of their patients, most notably:

(i) for the processing of a patient's hospital admissions or the booking of a patient's online appointments;

[321] Life Healthcare Group op cit note 303 at para 17.1.
[322] Life Healthcare Group op cit note 302.
[323] Life Healthcare Group op cit note 303.
[324] Life Healthcare Group op cit note 305.
[325] Ibid.
[326] Life Healthcare Group op cit note 302.
[327] Netcare 'Group profile' available at *https://www.netcare.co.za*, accessed on 25 November 2021.
[328] Netcare 'Information Manual' available at *https://www.netcare.co.za*, accessed on 25 November 2021.
[329] Netcare 'Netcare Privacy Policy' available at *https://www.netcare.co.za*, accessed on 25 November 2021.
[330] Ibid.
[331] Ibid.

(ii) for the assessment of the psychiatric or psychological condition of a patient;

(iii) for assisting with technical user support queries.

These purposes for the processing of personal information comply with the 'openness' condition prescribed in the POPIA, which mandates a responsible party to ensure that the data subject is aware of the purpose for which personal information is being collected and processed.[332] There is a reference in Paragraph 5[333] to the retention of records being in line with Netcare's 'TERMS AND CONDITIONS OF ADMISSION' document,[334] which states that Netcare's records are retained for a period of five years – this retention period is one year less than the recommended duration prescribed by the HPCSA, which is six years from the date such records are deemed dormant.[335] In the ensuing Paragraph 6,[336] Netcare endorses that:

> 'Netcare recognise[s] the vital role that information technology plays in its daily operations, and the reliance placed on information technology systems in processing personal information. Although absolute security cannot be guaranteed, Netcare will take reasonable technical and organisational measures to protect your [the patient's] personal information against accident, unauthorised or intentional manipulation, loss, misuse, destruction, disclosure or access.'

In the above-mentioned statement, Netcare declares that they are adhering to the seventh condition of lawful processing by implementing security safeguards to protect personal information in terms of Section 19 of the POPIA. There is further mention of Netcare having implemented procedures for responding to data breach incidents,[337] and this relates to Section 22 of the POPIA where a responsible party must notify affect data subjects in the case of a data breach.

[332] POPIA, s 18(1)(c).
[333] Netcare op cit note 329.
[334] Netcare 'TERMS AND CONDITIONS OF ADMISSION' available at *https://www.netcare.co.za*, accessed on 26 November 2021.
[335] HPCSA op cit note 31 at para 9.2.
[336] Netcare op cit note 329.
[337] Ibid.

In Paragraph 7 of the Netcare Privacy Policy, Netcare warrants that they may disclose personal information if: consent is obtained; it is required by the law or; it is required for the treatment of a patient.[338] Such a disclosure is permissible as per Section 14(2) of the NHA. Of interest, Paragraph 8 of Netcare's Information Manual[339] discloses the reasons for the refusal of requests to access records, whereby protection of the personal information of other data subjects is the foremost reason.

At Paragraph 8 of the Netcare Privacy Policy,[340] Netcare admits that patients' data is stored concurrently on Netcare's servers as well as servers belonging to third parties. This raises questions with regard to the security standards adhered to by the third-party servers Netcare utilises for storing their patients' data as this information has not been outlined. Other relevant issues include the geographic location of these third-party servers and the cybersecurity laws applicable to the territories those third-party severs are located within. Section 21 of the POPIA states that responsible parties must ensure that third parties (operators) maintain security measures for the protection of the personal information belonging to data subjects (patients). Netcare has not declared the level of protection afforded to data subjects' personal information by these third-party operators, especially considering the 'openness' condition in Section 18(1)(g) of the POPIA, specifically in relation to the third-party servers being in a foreign country. In this instance, transfers of personal information to a third party in foreign country must comply with Section 72 of the POPIA, which compels the responsible party to have a binding agreement with the foreign third-party operator.

Subsequently, the concluding Paragraph 12 of the Netcare Privacy Policy[341] declares patients' rights relating to their personal information, such as the right: to request the update[342] of personal information, to request the deletion[343] of personal information, and to place an objection[344] to the processing of personal information – these are the rights of data subjects (patients) in accordance with Section 11 and Section 24 of the POPIA.

[338] Ibid.
[339] Netcare op cit note 328.
[340] Netcare op cit note 329.
[341] Ibid.
[342] In compliance with Section 24(1)(a) of the POPIA.
[343] In compliance with Section 24(1)(b) of the POPIA.
[344] In compliance with Section 11(3) of the POPIA.

3.2.3. The Lenmed Group

The Lenmed Group has a number of specialised private hospitals across South Africa,[345] with the 'Lenmed Privacy Policy'[346] and 'Lenmed PAIA Information Manual'[347] documents standardising the processing of patients' personal information and access to records[348] therein. The Lenmed Privacy Policy document advises which types of personal information can be collected from patients, namely:[349] a patient's admission information; a patient's health information (medical history); a patient's medical scheme information and; a patient's bank account information for billing purposes (amongst others).

The Lenmed Group concedes that while they attempt to collect personal information directly from the patient concerned, there may be circumstances where a patient's personal information is collected from a third party instead, as is the case with the interdepartmental transfer of patient records occurring during the course of treating a patient.[350] While collection of personal information directly from the data subject is detailed in Section 12(1) of the POPIA, collection of such information from another source is permissible in terms of 12(2) of the POPIA if it would not prejudice the data subject (such as for the rendering of emergency health services to a patient). The Lenmed Privacy Policy[351] elaborates by sharing that patients' personal information can be collected for:[352]

(a) rendering hospital services to patients;

(b) processing patients' admissions to hospitals;

(c) booking online appointments;

(d) providing interdepartmental treatment;

---

[345] The Lenmed Group 'Lenmed Private Hospitals' available at *https://www.lenmed.co.za*, accessed on 26 November 2021.
[346] The Lenmed Group 'Lenmed Privacy Policy' available at *https://www.lenmed.co.za*, accessed on 26 November 2021.
[347] The Lenmed Group 'Lenmed PAIA Information Manual' available at *https://www.lenmed.co.za*, accessed on 26 November 2021.
[348] The PAIA manual is in compliance with Section 51 of the PAIA.
[349] The Lenmed Group op cit note 346 at p 6.
[350] The Lenmed Group op cit note 346 at p 7.
[351] The Lenmed Group op cit note 346 at p 8-9.
[352] Specifying the purpose for collection of personal information is obligatory in terms of Section 13 of the POPIA.

(e) processing medical aid scheme claims;

(f) conducting research, in which case, a patient's personal information is made to be de-identifying of the patient.

There are specific conditions by which the Lenmed Group permits the disclosure of patients' personal information, which include:[353]

(a) when personal information is requested or approved by the patient;

(b) when personal information is necessary for providing patients with proper treatment;

(c) when personal information is required by the law;

(d) when personal information is required by a patient's medical aid scheme;

(e) when personal information is required for the enforcement of the Lenmed Group's rights.

The Lenmed Group's grounds for refusal of access to records stipulated in Paragraph 16 of the Lenmed PAIA Information Manual[354] endorse that access requests that infringe upon another data subject's right to privacy[355] will be denied. In contrast, both the Lenmed Privacy Policy[356] and the Lenmed PAIA Information Manual[357] are vague in respect of data security measures. In accordance with Section 19 of the POPIA, a responsible party is compelled to maintain security safeguards for the personal information of data subjects. In the incident of a security compromise (such as a data breach), the responsible party must notify the affected data subjects.[358] Moreover, the Lenmed Group does not particularise the period to which they retain personal information.[359]

It is also of note that the Lenmed Group utilises external servers for the storage of electronic personal information records, and the details thereof are not disclosed.[360] The

[353] The Lenmed Group op cit note 346 at p 10.
[354] The Lenmed Group op cit note 347.
[355] In terms of Section 14 of the Constitution.
[356] The Lenmed Group op cit note 346 at p 11.
[357] The Lenmed Group op cit note 347 at para 15.
[358] POPIA, s 22.
[359] The Lenmed Group op cit note 346 at p 11-2.
[360] The Lenmed Group op cit note 346 at p 13.

geographic location of these external servers is not made known, and the provisions of Section 72 of the POPIA relating to the transborder flow of personal information may apply if the third party server is in a foreign country. Any third party is further regarded as an operator and the responsible party must ensure that such operator implements security measures to protect data subjects' personal information.[361]

The Lenmed Group then discloses patients' rights to request the deletion and alteration of personal information, and to issue an objection[362] to the processing of personal information.[363] Patients are additionally encouraged to direct unresolved complaints to the Information Regulator.[364]

3.2.4. Mediclinic

Mediclinic is an international company that owns several private hospitals in South Africa. Mediclinic's 'PRIVACY NOTICE TO PATIENTS' document[365] is the privacy policy applicable to all Mediclinic hospitals throughout South Africa. Mediclinic's privacy notice starts by separating personal information into two categories: general personal information and sensitive personal information.[366] Mediclinic considers general personal information to be uniquely identifying information (such as identity numbers and full names), whereas sensitive personal information is regarded as information relating to a person's race, political opinions, religious belief and health.[367] Mediclinic's category of sensitive personal information aligns with the POPIA's classification of special personal information.[368]

In Paragraph 3, Mediclinic declares that all personal information is to be collected directly from the patient.[369] Patients can make use of the affiliated CareConnect online portal

[361] POPIA, s 21.
[362] As per Section 11 and Section 24 of the POPIA.
[363] The Lenmed Group op cit note 346 at p 14.
[364] The Lenmed Group op cit note 346 at p 15.
[365] Mediclinic 'PRIVACY NOTICE TO PATIENTS' available at *https://www.mediclinic.co.za*, accessed on 26 November 2021.
[366] Mediclinic op cit note 365 at para 2.
[367] Ibid.
[368] POPIA, s 26.
[369] Mediclinic op cit note 365.

to facilitate the process of sharing treatment information across all healthcare services.[370] Collection of personal information directly from the data subject (the patient) is a practice compliant with Section 12(1) of the POPIA. Mediclinic then specifies their purposes[371] for the processing of personal information, which include:[372]

(a) contractual obligations with the patient;

(b) legal obligations;

(c) public interest;

(d) a patient consenting to the processing of their personal information;

(e) a legitimate interest of the patient or a third party.

In Paragraph 6, Mediclinic details that patients' personal information can be disclosed to service providers and suppliers to enhance healthcare service delivery to the patients.[373] These service providers are an operator in terms of Section 20 of the POPIA, because they process personal information on behalf of the responsible party (the hospital). As such, the responsible party is obligated to ensure that the operators maintain security measures for the processing of personal information.[374]

Mediclinic reiterates that consent to process personal information[375] will be obtained in accordance with the legal requirements.[376] Paragraph 10 does not prescribe a timeframe for which patients' personal information is to be kept, and only states that such personal information will be kept for the period it is necessary for.[377] Paragraph 11 then makes known that patients have the right to request the correction and erasure of their personal information records held by Mediclinic,[378] in compliance with Section 11 and Section 24 of the POPIA.

[370] Mediclinic op cit note 301 at para 3.
[371] Specifying the purpose for collection of personal information is mandated by Section 13 of the POPIA.
[372] Mediclinic op cit note 365 at para 4.
[373] Mediclinic op cit note 365.
[374] POPIA, s 21.
[375] This is required in terms of Section 11 of the POPIA, subject the exceptions mentioned previously.
[376] Mediclinic op cit note 365 at para 7.
[377] Mediclinic op cit note 365.
[378] Ibid.

Paragraph 9 endorses that Mediclinic has procedures to notify patients of a data breach, should one occur, which demonstrates adherence to Section 22 of the POPIA. Additionally, Mediclinic specifies that they maintain numerous controls to ensure the privacy and confidentiality of patients' personal information records, noticeably:[379]

(a) identity management;

(b) access management;

(c) infrastructure security;

(d) operational security;

(e) vulnerability management;

(f) disaster recovery planning;

(g) security awareness training.

Although Mediclinic does not provide further details regarding their controls, the fact that their hospitals have such controls is in alignment with Section 19 of the POPIA, whereby security measures for the protection of personal information are necessary. However, Mediclinic has not noted if their controls are in compliance with updated information security practices (such as the ISO/IEC 27002) as per Section 19(3) of the POPIA.

3.3. FURTHER CONSIDERATION: WIRELESS NETWORKS

3.3.1. Network types and usage

Undoubtedly, the usage of the internet is integral to the functioning of modern society, chiefly with the remote communication requirements arising from the COVID-19 pandemic, which caused internet data usage in South Africa to significantly increase between 2020 and 2021.[380] Lesame *et al* describe the internet as 'a global collection of networks' which are

[379] Ibid.
[380] Given Majola 'SA data usage soars' available at *https://www.iol.co.za*, accessed on 27 November 2021.

interconnected.[381] Differing modes of connecting to the internet exist, and this can be achieved through the use of: Local Area Networks[382] (LANs); Wide Area Networks[383] (WANs) and; Wireless Local Area Networks[384] (WLANs).

A LAN is considered a cluster of two or more computers connected within a small geographic area,[385] whereas a WAN can be several computers connected throughout the globe.[386] Much like a LAN, a WLAN is confined to a particular area, however, the key difference is that a WLAN is wireless and does not require the use of cables for connectivity among devices.[387] Wi-Fi networks are classified as the most commonly used type of WLAN.[388] A Wi-Fi network appears on devices through the display of a Secure Set Identifier[389] (SSID), which is colloquially called a Wi-Fi network name.[390] SSIDs can be transmitted from devices that support Wi-Fi, such as internet modems and hotspots on phones and computers. An SSID can easily be modified via the device it is transmitted from, because an SSID is not unique to the device it emanates from.

In South Africa, Internet Service Providers[391] (ISPs) provide internet in the forms of: an Asymmetric Digital Subscriber Line[392] (ADSL); a Fibre connection or; a Long-Term Evolution[393] (LTE) subscription. ADSL is internet provided through obsolete copper-based lines, which have been in the process of being phased out since 2020 in South Africa – ADSL is to be replaced by Fibre cabling.[394] LTE on the other hand uses mobile towers to transmit and relay internet service signals,[395] much like cell towers transmit signals to allow phones to send and receive messages and make phone calls. Fourth Generation[396] (4G) LTE in particular

[381] Zandi Lesame *et al* op cit note 119 at 59.
[382] Hereafter referred to as an 'LAN'.
[383] Hereafter referred to as a 'WAN'.
[384] Hereafter referred to as a 'WLAN'.
[385] Joseph Migga Kizza *Guide to Computer Network Security* 4 ed (2017) 5.
[386] Joseph Migga Kizza op cit note 385 at 6.
[387] Joseph Migga Kizza op cit note 385 at 39.
[388] Lee Badman 'What is the difference between WLAN and Wi-Fi?' available at *https://www.techtarget.com*, accessed on 27 November 2021.
[389] Hereafter referred to as an 'SSID'.
[390] D-Link 'What is SSID?' available at *https://eu.dlink.com*, accessed on 27 November 2021.
[391] Hereafter referred to as an 'ISP'.
[392] Hereafter referred to as 'ADSL'.
[393] Hereafter referred to as 'LTE'.
[394] BusinessTech 'What is ADSL?' available on *https://businesstech.co.za*, accessed on 28 November 2021.
[395] Joseph Migga Kizza op cit note 385 at 414.
[396] Hereafter referred to as '4G'.

boasts faster download and upload speeds than its predecessor.[397] The above-mentioned internet connection services can be accessed via modems or smartphones, a majority of which are capable of transmitting WLANs (Wi-Fi networks). In brief, individuals require an ADSL, Fibre or LTE subscription with an ISP in order to connect to the internet via an LAN or WLAN (Wi-Fi network).

Netcare prescribes strict guidelines for the proper use of their Wi-Fi networks, namely that Wi-Fi users (which can be patients or hospital staff) must not use Netcare hospitals' Wi-Fi networks in a manner that damages or burdens those WLANs.[398] Netcare also states that all persons connected to their Wi-Fi networks are responsible for the cybersecurity on their own devices,[399] which includes any personal information data stored therein.

In 2017, Mediclinic launched free Wi-Fi network access for patients and doctors alike, citing the installation of Fibre cabling at their hospitals as the catalyst for this decision.[400] Patients who want to use these free Wi-Fi networks are requested to provide their email address and mobile phone number for access therein.[401] Mediclinic released a statement wherein they declared that their business Wi-Fi networks are isolated for each medical device to which they are intended to be paired with,[402] with separate frequencies allocated to each of these medical devices.

3.3.2. Wi-Fi network encryption

Wi-Fi networks can either be encrypted (secure) or 'open' (unsecure). The fundamental forms of Wi-Fi encryption are Wi-Fi Protected Access[403] (WPA) and its successor Wi-Fi Protected Access 2[404] (WPA2). The main difference between WPA and WPA2 encryption is that WPA2 is newer and offers enhanced security, whilst WPA is outdated but supports older devices that are incapable of connecting to WPA2 encrypted Wi-Fi networks due to their older

[397] Verizon 'What is 4G LTE and why it matters' available at *https://www.verizon.com*, accessed on 28 November 2021.
[398] Netcare 'Wifi' available at *https://www.netcare.co.za*, accessed on 28 November 2021.
[399] Ibid.
[400] Mediclinic 'Free Wi-Fi at Mediclinic' available at *https://www.thefutureofhealthcare.co.za*, accessed on 28 November 2021.
[401] Ibid.
[402] Mediclinic 'Free in-hospital Wi-Fi – a real patient's perk' available at *https://www.mediclinicinfohub.co.z*a, accessed on 28 November 2021.
[403] Hereafter referred to as 'WPA'.
[404] Hereafter referred to as 'WPA2'.

infrastructure.[405] There is a hybrid WPA/WPA2 encryption intended to accommodate old and new devices alike while offering the benefits of both encryptions – the only drawback with the WPA/WPA2 encryption being the exposure to previous WPA-based security flaws.

In combination with WPA and WPA2, there are various forms of WPA keys (access codes), which include: a Pre-Shared Key[406] (PSK), a Temporal Key Integrity Protocol[407] (TKIP) and an Advanced Encryption Standard[408] (AES). A PSK is a password that permits access to the WPA or WPA2 encrypted Wi-Fi network.[409] A TKIP is a randomised key generated per access to the Wi-Fi network.[410] AES is newer and can work in tandem with a PSK. AES is also exclusive to the WPA2 encryption.[411]

Additional network security can be afforded to individuals who use a Virtual Private Network[412] (VPN), which encrypts an individual's connection to a Wi-Fi network by masking data (such as the individual's IP address) via an encrypted tunnel whereby the individual's data is re-routed to a remote server belonging to the VPN service provider.[413]

3.3.3. Other Wi-Fi network vulnerabilities

Chigada and Madzinga contend that unsecured public Wi-Fi networks pose a serious security threat to the devices connected to those WLANs and the data contained on those connected devices (especially data consisting of personal information).[414] Joseph Kizza asserts that the validation of the identity of a Wi-Fi network name (SSID) remains the most pressing issue with regard to SSID replication.[415] Kizza states that Media Access Control[416] (MAC) addresses have the potential to be unique to the device they are associated with, such as a modem or

[405] Sony 'What Is Wireless Encryption and Why Is It Used?' available at *https://www.sony.com*, accessed on 28 November 2021.
[406] Hereafter referred to as 'PSK'.
[407] Hereafter referred to as 'TKIP'.
[408] Hereafter referred to as 'AES'.
[409] Ibid.
[410] Ibid.
[411] Chris Hoffman 'Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both?' available at *https://www.howtogeek.com*, accessed on 28 November 2021.
[412] Hereafter referred to as a 'VPN'.
[413] Norton 'How does a VPN work?' available at *https://us.norton.com*, accessed on 6 February 2022.
[414] Joel Chigada & Rujeko Madzinga op cit note 127 at 5.
[415] Joseph Migga Kizza op cit note 385 at 419.
[416] Hereafter referred to as 'MAC'.

smartphone (given that such MAC address has not been cloned).[417] However, an SSID can easily be modified to match another Wi-Fi network's SSID in order to deceive unsuspecting individuals into connecting to the impostor network.[418] Once an individual connects to the impostor network, that individual's device can be compromised by way of keyloggers, malware and the like. Similarly, Kizza has noted that intentional frequency jamming is a further concern for WLANs that utilise the 2.4 Gigahertz[419] (GHz) frequency to transmit Wi-Fi networks, as this frequency interference action can disrupt and impair the use of necessary Wi-Fi networks using that frequency.[420]

3.3.4. The Internet of Things

The Internet of Things[421] (IoT) has been explained as a visionary aspiration of seamless device interconnectivity.[422] Fortinet describes the IoT as being characterised by interconnected devices being capable of communicating data to a network in real-time.[423] This interconnected data transmission resulting from the IoT model is beneficial for enhanced communication, information relay and business productivity by ultimately reducing the amount of time required for the sending and receipt of data among devices and their affiliated network.[424]

The IoT concept maintains its fair share of security challenges though, particularly with authentication and encryption-related security issues that occur when data is in the process of being transferred wirelessly between devices of differing infrastructures with limited compatibility.[425] Similarly, Patricia Williams and Andrew Woodward propose that web servers, which connect medical devices in accordance with the IoT model, are susceptible to cybercriminals exploiting the security vulnerabilities of the individual medical devices connected to those web servers in order to compromise these networks as a whole.[426]

---

[417] Joseph Migga Kizza op cit note 385 at 419.
[418] Joseph Migga Kizza op cit note 385 at 419.
[419] Hereafter referred to as 'GHz'.
[420] Joseph Migga Kizza op cit note 385 at 423.
[421] Hereafter referred to as the 'IoT'.
[422] Joseph Migga Kizza op cit note 385 at 519.
[423] Fortinet 'IoT Edge' available at *https://www.fortinet.com*, accessed on 28 November 2021.
[424] Tommy Quek 'The advantages and disadvantages of Internet Of Things (IoT)' available at *https://www.linkedin.com*, accessed on 6 February 2022.
[425] Joseph Migga Kizza op cit note 385 at 527.
[426] Patricia AH Williams & Andrew J Woodward 'Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem' (2015) 8 *Medical Devices: Evidence and Research* 309.

Moshadiqque Al Ameen *et al* found that the most common security vulnerabilities affecting medical devices include: data modification; impersonation attacks; eavesdropping and replaying.[427] Data modification, as mentioned previously, is mostly the result of unauthorised access to stored data (such as personal information) held by bodies such as hospitals. Impersonation attacks, such as SSID replication and spoofing, were noted to have been perpetrated by cybercriminals for the purposes of unlawfully seizing control of devices belonging to others. In contrast, eavesdropping occurs when a cybercriminal intercepts medical devices for the purposes of: acquiring confidential information about a patient[428] or; modifying data being transmitted between two devices.[429] Fortinet warns that eavesdropping attacks are prominently perpetrated by cybercriminals who infiltrate networks and monitor network activity to identify targets for interception and eavesdropping.[430] Al Ameen *et al* elaborate and state that replaying is the act of sending intercepted data (after eavesdropping) to another person purporting to be a credible source (spoofing) in an attempt to conduct phishing and steal account credentials.[431]

As the IoT model of interconnected devices within hospitals normalises as the standard for the provision of healthcare services and treatment of patients, the security risks and impact on EHRs and EPRs is still under review. The introduction of the EVDS and its affiliated QR codes (most of which are presented via mobile devices) are the epitome of the IoT model in effect – healthcare users literally present their QR code via smartphone to an organisation's scanner in order to prove the status of their vaccination, and such information is relayed and verified by a system owned by the DoH.

The viability of the data security within those QR codes, the smartphones they are stored on, and the data scanners utilised by organisations (including hospitals) are pending review. Undoubtedly, patients' vaccination data contained in their allocated QR codes will be read and stored by hospitals on their servers. However, in the process of patients' vaccination data being transmitted to hospital servers, the cybersecurity of the hospitals' scanning and network devices transmitting such data needs to be ensured.

---

[427] Moshaddique Al Ameen, Jingwei Liu & Kyungsup Kwak 'Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications' (2012) 36 *J Med Syst* 97.
[428] Ibid.
[429] Fortinet 'Eavesdropping' available at *https://www.fortinet.com*, accessed on 28 November 2021.
[430] Ibid.
[431] Moshaddique Al Ameen *et al* op cit note 427.

3.4. ADDITIONAL FACTORS

Williams and Woodward indicate that the use of legacy (outdated) operating software and systems are a cause of cybersecurity breaches, particularly software that is more than five years old and has not received recent updates.[432] A lack of software and patch updates on devices that require them is another problematic aspect.[433] In the context of hospitals, medical devices are frequently identified to lack basic security features (such as basic firewalls)[434] due to containing elementary firmware and hardware,[435] which could adversely impact upon the cybersecurity of patients' data that is being stored on those devices or transmitted via such devices.

A lack of employee awareness of cybersecurity issues and practices when operating devices has also been attributed to data breaches,[436] with one study citing a causal nexus between hospital employees working long hours and limited interest and time investment by those overburdened employees in learning more about cybersecurity.[437] In furtherance, South Africa is no stranger to an absence of widespread digital literacy, with the term the 'digital divide' coined to exemplify the lack of Information Communication Technology[438] access and expertise nationally.[439] Internationally, Kaspersky established that employees lacking cybersecurity awareness who use organisational IT resources inappropriately increase the possibility of cybercrime being committed.[440] NordPass[441] concluded that although 2021 has brought technological advancements, multiple regions globally were still deficient in simple cybersecurity practices to mitigate the risk of cyberattacks, such as using strong passwords for online accounts.[442]

---

[432] Patricia AH Williams & Andrew J Woodward op cit note 426 at 311.
[433] Ibid.
[434] Alan Grau 'Securing Medical Devices: What is Really Needed?' available at *https://www.medtechintelligence.com*, accessed on 6 February 2022.
[435] Patricia AH Williams & Andrew J Woodward op cit note 426 at 311.
[436] Ibid.
[437] Joel Chigada & Rujeko Madzinga op cit note 127 at 5.
[438] Commonly referred to as 'ICTs'.
[439] Zandi Lesame *et al* op cit note 119 at 114.
[440] Brendyn Lotz 'Employees using IT resources for the wrong thing could be costly' available at *https://htxt.co.za*, accessed on 28 November 2021.
[441] A company affiliated with NordVPN.
[442] MyBroadband 'It's 2021 and the most common password is still 123456' available at *https://mybroadband.co.z*a, accessed on 28 November 2021.

South Africa additionally has an ongoing issue of load shedding, which impacts upon all electronic devices (including servers storing personal information data) and the connectivity of devices reliant upon WLANs and LANs due to the lack of electricity and signal emission.[443] In addition, there is a national systemic corruption problem resulting in South Africa being perceived as one of the most corrupt countries in Africa.[444] Correspondingly, the phenomenon dubbed the 'Insider Effect' is when an employee of an organisation (an 'insider') wilfully perpetrates cybercrime targeting their employer, through the use of their internal organisational knowledge.[445] This factor cannot be ruled out in the situation of South Africa's healthcare sector, with the South African President admitting that corruption is blatant at the government level (which includes state-owned departments).[446]

3.5. CONCLUSION

This chapter examined the privacy policies of private hospital groups operating in South Africa for legislative compliance, namely: the Life Healthcare Group, Netcare, the Lenmed Group and Mediclinic. The record access policies for the above-mentioned private hospital groups were reviewed as well as each private hospital group's documentation regarding patient record information security. Additionally, factors such as wireless network encryption and connected devices were considered for vulnerabilities that affected patient data, especially in the context of interconnected medical devices sharing a common server.

[443] Luke Daniel 'Cellphone towers are crippled by load shedding – and theft of at least 200 batteries each month' available at *https://www.businessinsider.co.za*, accessed on 28 November 2021.
[444] Ernest Mabuza 'SA remains pegged below 50 points in Corruption Perception Index' available at *https://www.timeslive.co.za*, accessed on 28 November 2021.
[445] Joseph Migga Kizza op cit note 385 at 78.
[446] Mogomotsi Magome & Andrew Meldrum 'South Africa's Ramaphosa says corruption has damaged country' available at *https://apnews.com*, accessed on 28 November 2021.

CHAPTER FOUR

RECOMMENDATIONS

4.1. INTRODUCTION

Based on the identified risks to patients' personal information data, this chapter offers the recommendations hereinafter which comply with local legislation and international standards, namely: the disposal of patient records; the physical security of premises used for storing records and data; the development of an incident response plan; risk management practices; cybersecurity controls and; the education of employees on the risk prevention practices.

4.2. THE DISPOSAL OF USED PATIENT RECORDS

Hospitals should prescribe an appropriate timeframe for the disposal of patient records that are no longer in use, and hospitals should further implement a process to be followed for such disposal. Section 14 of the POPIA stipulates that responsible parties must delete or destroy personal information records after such records have been processed for their intended purpose. Although Buys suggests that patients' medical records should be deleted five years subsequent to their use,[447] the HPCSA proposes that patient records be retained for not less than six years after they were used,[448] with records belonging to children requiring to be held until the child becomes an adult.[449]

The Medical Protection Society (South Africa) emphasises the importance of the proper destruction of discarded EPRs and EHRs via disk shredding or the overwriting of patients' data contained on disks.[450] The Medical Protection Society states that while external contractors may be utilised for the physical disposal of disks containing EPRs and EHRs, the responsible

[447] M Buys 'Protecting personal information: Implications of the Protection of Personal Information (POPI) Act for healthcare professionals' (2017) 107(11) *SAMJ* 956.
[448] HPCSA op cit note 31 at para 9.2.
[449] HPCSA op cit note 31 at para 9.3.
[450] The Medical Protection Society 'Appendix 1: Retention and disposal of records' available at *https://www.medicalprotection.org*, accessed on 29 November 2021.

party (the hospital) must confirm that these records were indeed destroyed properly in order to prevent the recovery of data containing EPRs and EHRs for identity theft motives.[451]

4.3. PHYSICAL SECURITY MEASURES

The physical security of servers, data storage disks and the premises where EPRs and EHRs are being stored must be secured. The four basic principles of physical security are:[452] the deterrence of criminals; the prevention of a security breach; the detection of intrusion (security breach alerts) and; response to the security breach.

The ISO/IEC 27002 standards prescribe access control to defend against unauthorised physical access to areas where information is stored via the use of physical barriers and intrusion detection systems such as alarms.[453] There is a recommendation of restricting access to employees who have obtained prior approval[454] (from a line manager, for instance, who has the authority to grant permission for records access). Further entry guidelines are presented whereby individuals must be identified, authenticated and noted prior to accessing record storage areas.[455] Authentication includes the use of biometrics (like fingerprints) and access cards with appropriate clearance.[456]

Moreover, the ISO/IEC 27002 standards detail that external and environmental threats need to be safeguarded against.[457] There are two categories of disasters: natural disasters (like earthquakes and floods) and human-caused disasters (like theft and terrorism).[458] In South Africa, human-induced issues include theft and malicious damage property, which can be prevented by securing the data storage premises and engaging the services of a private security company to monitor and respond to physical security breaches.[459] In terms of load shedding and electricity outages, hospitals in particular must keep independent direct current power

[451] Ibid.
[452] Joseph Migga Kizza op cit note 385 at 41.
[453] ISO op cit note 85 at para 11.1.1.
[454] Ibid.
[455] ISO op cit note 85 at para 11.1.2.
[456] Joseph Migga Kizza op cit note 317 at 46.
[457] ISO op cit note 85 at para 11.1.4.
[458] Joseph Migga Kizza op cit note 385 at 176.
[459] Joseph Migga Kizza op cit note 385 at 178.

generation supplies on hand, such as generators, inverters or batteries in order to keep devices, networks and servers functional for the continuous rendering of health services to patients.[460]

Maintaining external back-ups of patients' EHR and EPR data is advisable in case such data is deleted or held ransom (via ransomware cyberattack), so that this data can be restored[461] and retrieved in compliance with the information security principle of accessibility. A further proposition is to enclose storage disks containing EPRs and EHRS in units with electromagnetic shielding to prevent electromagnetic pulse interference and damage to the data contained on those disks.[462]

4.4. DEVELOP AN INCIDENT RESPONSE PLAN

The National Institute of Standards and Technology[463] (NIST) describes an incident response plan as a 'predetermined set of instructions' to which individuals within an organisation are expected to adhere to in the circumstance of a cyberattack against the organisation's IT systems.[464] The key elements of an incident response plan include: an appointed first responder, delegated roles and responsibilities, the availability of offline resources for use, instructions for the containment of the threat, and the process for recovery from the incident.[465]

In the occurrence of a cybersecurity incident implicating a data subject's personal information, responsible parties are compelled to notify the Information Regulator[466] and the affected data subject[467] in accordance with the POPIA. Therefore, responsible parties (such as hospitals) must have a notification system to fulfil the aforementioned legislative duties owed to data subjects (such as patients) in the event of a data breach.

---

[460] Ibid.
[461] Joseph Migga Kizza op cit note 385 at 184.
[462] ISO op cit note 85 at para 11.1.3.
[463] A government agency in the USA. Hereafter referred to as the 'NIST'.
[464] NIST 'incident response plan' available at *https://csrc.nist.gov,* accessed on 6 February 2022.
[465] ISA Cybersecurity 'Elements of an Incident Response Plan' available at *https://isacybersecurity*, accessed on 6 February 2022.
[466] POPIA, s 22(1)(a).
[467] POPIA, s 22(1)(b).

An incident response protocol needs to be in effect within hospitals for communicating with the Information Regulator[468] and for reporting any data breach incidents that have occurred. Furthermore, a process whereby the hospital discloses data breach information to affected patients is necessary – this can be achieved through a hospital issuing communication via the media in accordance with Section 22(4) of the POPIA. Therefore, the hospital would have to make appropriate arrangements for liaising with local media to publicise information relating to a hospital data breach incident in order to notify patients whose personal information may have been compromised.[469] Alternatively, hospitals can utilise their own website or verified social media accounts for providing announcements to patients regarding data breaches,[470] given these notices provide adequate details regarding the incident so that patients can exercise appropriate countermeasures in terms of Section 22 of the POPIA.

In the implementation of a cyber incident response plan in the healthcare sector, Jill McKeon notes that maintaining a communications strategy is vital to reducing miscommunication between hospitals and their patients.[471] McKeon further advocates for healthcare organisations practicing their chosen incident response plans to ensure employee preparedness in the event that an incident occurs.[472]

The NIST further prescribes a comprehensive organisational cybersecurity framework consisting of five core elements,[473] principally:

(i) the identification of cybersecurity risks at an organisational level;[474]

(ii) the ongoing protection against identified cybersecurity risks through the use of appropriate safeguards;[475]

(iii) the ongoing detection of cybersecurity risks and incidents;[476]

---

[468] Information Regulator (South Africa) 'Contact Us' available at *https://justice.gov.za*, accessed on 29 November 2021.
[469] POPIA, s 22(4)(d).
[470] POPIA, s 22(4)(c).
[471] Jill McKeon 'How to Implement a Cyber Incident Response Plan for Healthcare' available at *https://healthitsecurity.com*, accessed on 29 November 2021.
[472] Ibid.
[473] NIST *Framework for Improving Critical Infrastructure Cybersecurity* (2018) para 2.1.
[474] NIST *Framework for Improving Critical Infrastructure Cybersecurity* (2018) p 7.
[475] Ibid.
[476] Ibid.

(iv) the establishment of a response plan regarding the occurrence of cybersecurity incidents;[477]

(v) the establishment of a recovery plan in the event of a cybersecurity incident, and a system for the timely restoration of organisational resources and services.[478]

If hospitals can regulate their detection of cybersecurity risks and their response to data breaches, then there is a possibility that cyberattacks can be contained and EPRs and EHRs can be spared of being compromised by unauthorised access, which would ultimately uphold the information security principles of data integrity and confidentiality.

In the case of the South African private hospital data breaches from June 2020,[479] the Life Healthcare Group took until August 2020 to fully restore their IT systems.[480] However, the Life Healthcare Group did state that they relied upon back-up systems following their containment of the data breach.[481] A defined and well-practiced incident response plan would expedite the restoration period in this circumstance to ensure business continuity.

4.5. EMPLOYEE AWARENESS TRAINING

Hospital employee awareness training with regard to cybersecurity and data security practices is critical in the prevention of data breaches that jeopardise EHRs and EPRs. Mandatory professional development initiatives, such as conferences and workshops, are encouraged for increasing employee cybersecurity awareness and training. The enrolment of employees in lengthy technology training programmes can enhance the efficacy of hospital employee IT education in relation to cybersecurity. Programmes like the International Computer Driving Licence[482] offer basic cybersecurity and data security modules tailored for members of the

[477] NIST *Framework for Improving Critical Infrastructure Cybersecurity* (2018) p 8.
[478] Ibid.
[479] Life Healthcare Group op cit note 139.
[480] Samuel Mungadze op cit note 156.
[481] Life Healthcare Group op cit note 139.
[482] Commonly referred to as the 'ICDL'.

workforce,[483] by which employees can be motivated to enrol in with incentives and financial support provided by their employer (the hospital) as a form of focused education.[484]

Supplementary education of employees pertaining to the use of their online organisational accounts is recommended, such as advisory with regard to the restriction of use of personal email and social media while on hospital LANs and WLANs (Wi-Fi networks) – this can prevent the infiltration of malware on hospital servers via employee personal accounts, which tend to lack the level of security found on organisational accounts.[485] Deloitte suggests that the mitigation of phishing attacks perpetrated via email can be achieved by employees refraining from opening attachments and links appearing in emails filtered as spam, and by employees verifying the sender of suspicious emails.[486]

Comparatively, Google[487] offers two-step verification for access to Google accounts, including custom domain organisational Gmail[488] email accounts. Two-step verification entails the use of both a password and a security key on a mobile device to access a Gmail account.[489] Thereafter, a notification is sent to the Gmail account and affiliated mobile device noting an account sign-in. Two-step verification can be used to detect unauthorised access to accounts (especially keylogger password replication attempts)[490] due to the associated security key mobile device receiving alerts regarding attempted sign-ins. The Microsoft Outlook email service provider also offers two-step verification services to its clients.[491]

Two-step verification can prove useful in a hospital setting, granted that hospital employees are provided with business mobile devices for work use. Ideally, hospitals should issue employees with devices for business use only. These devices supplied by the hospital should maintain standardised security protocols that optimise data encryption and prevent data

[483] ICDL Africa 'ICDL Programmes' available at *https://icdlafrica.org*, accessed on 29 November 2021.
[484] Joseph Migga Kizza op cit note 385 at 449.
[485] Lisa Gentes-Hunt 'How Health Facilities Can Prevent, Mitigate Ransomware in 2021' available at *https://healthitsecurity.com*, accessed on 29 November 2021.
[486] Deloitte op cit note 144.
[487] A technology company founded in 1998.
[488] Google's email service provider.
[489] Google 'Google 2-Step Verification' available at https://www.google.com, accessed on 29 November 2021.
[490] Fortinet 'How To Detect the Presence of a Keylogger on Your Phone' available at https://www.fortinet.com, accessed on 29 November 2021.
[491] Microsoft 'How to use two-step verification with your Microsoft account' available at https://support.microsoft.com, accessed on 29 November 2021.

interception. In furtherance, initiatives such as the 'Bring Your Own Device'[492] policy where employees are permitted to use personal devices to access business networks containing sensitive information is not advisable due the prospect of these personal devices containing security flaws.[493] If hospital employees can maintain encrypted access to their business devices and accounts, then patient personal information contained in those hospital employees' business devices and accounts would remain secured and confidential in compliance with Section 14 of the NHA, the HPCSA guidelines[494] and the information security principle of confidentiality.

4.6. RISK MANAGEMENT

Enterprise Risk Management[495] (ERM) is the management and mitigation of risk in an organisation.[496] ERM places an emphasis on the implementation of a risk management framework to attain legislative compliance and more effective operational processes within an organisation (such as a hospital).[497] Deloitte comments that due to the demands of the COVID-19 pandemic, organisations' IT strategies are one of the most important elements of an ERM plan.[498] Ernst & Young[499] indicate that the external economic impact of the COVID-19 pandemic on organisations must be considered in the evaluation and institution of operational changes.[500]

The NIST proposes a seven-part risk management framework which consists of:[501]

(i) the organisation's preparation in managing risks;

[492] Commonly referred to as 'BYOD'.
[493] Forcepoint 'What is Bring Your Own Device (BYOD)?' available at *https://www.forcepoint.com*, accessed on 6 February 2022.
[494] HPCSA op cit note 31.
[495] Hereafter referred to as 'ERM'.
[496] The Open University *Risk management* (2019) 37.
[497] The Open University *Risk management* (2019) 41.
[498] Deloitte 'The Impact of COVID-19 on enterprise-level risk management' available at *https://www2.deloitte.com*, accessed on 29 November 2021.
[499] A professional services company founded in 1989. Commonly referred to as 'EY'.
[500] Ernst & Young 'Enterprise risk management (ERM) in the COVID-19 world' available at *https://assets.ey.com*, accessed on 29 November 2021.
[501] NIST 'NIST Risk Management Framework' available at *https://csrc.nist.gov*, accessed on 29 November 2021.

(ii) the categorisation of organisational information based on sensitivity;

(iii) the selection of organisational controls based on a risk assessment;

(iv) the implementation of organisational controls;

(v) the assessment of existing organisational controls;

(vi) the authorisation of organisational risk-management mitigation decisions and;

(vii) the ongoing monitoring of risks.

The NIST risk management framework should be considered by hospitals in South Africa owing to the requirements listed in Section 19(2) of the POPIA that compel responsible parties to maintain controls against risks to a data subject's personal information. The adoption of both a risk management framework in tandem with a cybersecurity framework is beneficial in maintaining controls that prevent unlawful interference with a data subject's personal information as per the requirements of the POPIA.[502]

Williams and Woodward further suggest the establishment of reporting and feedback loops between hospitals and medical device manufacturers for identified flaws in medical devices that pose risks to the hospital's cybersecurity as well as patients' data therein.[503] Kizza endorses that the separation of duties within an organisation (like a hospital) is the most effective method of mitigating risk through the limiting of IT access privileges for employees who do not require those rights in the discharge of their duties.[504] Kizza asserts that an employee with less access privileges is a lesser risk to an organisation on the basis that they lack total autonomy over sensitive and critical data.[505]

The ISO 31000 risk management guidelines propose 'risk treatment' as a method of addressing risk.[506] The risk treatment options include:[507] the avoidance of the risk through curbing risk-inviting activities; the removal of the source of the risk; the altering of the

[502] POPIA, s 19(2).
[503] Patricia AH Williams & Andrew J Woodward op cit note 426 at 311.
[504] Joseph Migga Kizza op cit note 385 at 203.
[505] Ibid.
[506] ISO *ISO/IEC 31000* (2018) at para 6.5.
[507] ISO *ISO/IEC 31000* (2018) at para 6.5.2.

consequences of the risk or; the sharing of the risk with other organisations and parties. CIO[508] proffers business continuity planning as an appropriate means of responding to cyberattacks and severe risks.[509] Business continuity is described as the ability of an organisation to resume functioning following a major disruption (such as a natural disaster or a human-made disaster).[510] Business continuity is the synthesis of risk management and response planning. In the circumstance of hospitals in South Africa, such hospitals are classified as an essential service[511] and therefore must have a plan for continuing business even during the COVID-19 pandemic. The continuation of business therein requires the ongoing processing of EPRs and EHRs in order to render healthcare services to patients, and such processing is subject to the POPIA.

4.7. CYBERSECURITY CONTROLS

A vulnerability assessment is a proactive and productive method of identifying an organisation's cybersecurity risks through the use of network scans.[512] Any identified vulnerabilities in connected applications, software, servers and networks are elicited via this scan and can be rectified in order to prevent cyberattacks.[513] Vulnerabilities can include: device setting misconfigurations, outdated security and absent critical update patches.[514] Another form of vulnerability assessment is penetration testing, which is when an individual is hired to purposefully hack into an organisation's IT systems to simulate a real-life cyberattack scenario.[515] The value of this exercise is that the cybersecurity of the organisation's IT systems are tested, in addition to the organisation's incident response plan.[516] Certified Ethical Hackers[517] can be enlisted to conduct these penetration tests.[518] Organisations can also have a

[508] An IT magazine founded in 1987.
[509] Kim Lindros and Ed Tittel 'How to create an effective business continuity plan' available at *https://www.cio.com*, accessed on 29 November 2021.
[510] Ibid.
[511] South African Government 'Essential services – Coronavirus COVID-19' available at *https://www.gov.za*, accessed on 29 November 2021.
[512] Fortinet 'Vulnerability Assessment' available at *https://www.fortinet.com*, accessed on 29 November 2021.
[513] Ibid.
[514] Ibid.
[515] Joseph Migga Kizza op cit note 385 at 101.
[516] Ibid.
[517] Commonly referred to as 'CEHs'.
[518] EC Council 'CEH' available at *https://www.eccouncil.org*, accessed on 29 November 2021.

vulnerability assessment conducted via a contracted IT security firm, who can provide a report on the results of a cyber health check relating to the organisation's cybersecurity controls.[519] In the report following the penetration test, the incident should be logged and noted for future cybersecurity enhancements, preventative measures and the education of the organisation's employees.

Due to the COVID-19 pandemic, numerous healthcare organisations have placed reliance upon third-party servers for the storage of patients' data (containing their personal information).[520] If hospitals choose to utilise third-party servers to host patients' data, it is suggested that those third-party service providers be audited via a cybersecurity risk assessment before a hospital signs into a data storage agreement with them.[521] This is especially applicable to the Lenmed Group and Netcare, who declared in their privacy policy documents that their hospitals use third-party servers for the storage of their patients' data.

With regard to the use of WLANs in hospitals, it would be good practice to ensure that those Wi-Fi networks are WPA2 encrypted and use a PSK access code. An isolated set of Wi-Fi networks should be designated for guest or patient use at the hospital, and these allocated networks must contain WPA2 encryption and an accompanying PSK code that is changed daily. For hospital employees, separate Wi-Fi networks with WPA2 encryption and PSKs can be used.

To safeguard against unauthorised access on employee Wi-Fi networks, the WLANs administrator can restrict access to the Wi-Fi network based on the MAC addresses of the devices being used to access the Wi-Fi network so that only approved hospital devices may access that WLANs.[522] Additional security to hospital networks can be supplied through the use of a firewall,[523] which is capable of filtering traffic to and from a network.[524] Similarly,

---

[519] Shih Ming Pan, Chii-Wen Wu & Pei-Te Chen *et al* 'CYBERSECURITY HEALTH CHECK' in Kim Andreasson (ed) *Cybersecurity: Public Sector Threats and Responses* (2012) chap 11.
[520] Jill McKeon 'Top Healthcare Cybersecurity Challenges, How to Overcome Them' available at *https://healthitsecurity.com*, accessed on 29 November 2021.
[521] Jill McKeon 'The Importance of Third-Party Risk Assessments in Healthcare' available at *https://healthitsecurity.com*, accessed on 29 November 2021.
[522] Joseph Migga Kizza op cit note 385 at 424.
[523] Joseph Migga Kizza op cit note 385 at 251.
[524] Fortinet 'What Is a Firewall?' available at *https://www.fortinet.com*, accessed on 29 November 2021.

hospitals can consider employing Cisco certified network experts to manage hospital WLANs and serve as the administrators therein.[525]

Netcare[526] and the Lenmed Group[527] both offer online booking systems for patient admissions and have advised in their privacy policy documents that patients' personal information will be processed via these online portals. To ensure the confidentiality of patients' personal information submitted to these online booking systems, hospitals must have a Secure Sockets Layer[528] (SSL) certificate to identify and validate the web server host to determine that it is not a spoofed website, and that any data submitted therein will be encrypted for viewing by the SSL certificate web server host only.[529] SSL certificates expire within two years of issuance,[530] therefore the onus is upon the web server host (the hospital) to renew their SSL certificate. A further method of web-based encryption is through the use of Hypertext Transfer Protocol Secure[531] to authenticate the hospital's web server host and reassure patients who are using the online booking system that the integrity and confidentiality of submitted personal information will be upheld.[532]

With regard to the protection of email systems against the increase in international phishing cyberattacks healthcare service providers as noted by Deloitte,[533] the United States Department of Health and Human Services propose the implementation of email system filters to detect malicious content and intercept these problematic emails before they appear in an employee's inbox.[534] In a hospital setting, this can prevent the compromise of hospital employees' email accounts, and safeguard the confidentiality of messages containing patients' personal information. Similarly, content filtering[535] is an effective tool for hospitals to use to scan, detect and filter out harmful content such as viruses and malware from the hospital's IT

[525] Cisco 'Cisco Certifications' available at *https://www.cisco.com*, accessed on 29 November 2021.
[526] Netcare 'Welcome to your personal Health Centre' available at *https://www.netcare.co.za*, accessed on 29 November 2021.
[527] Lenmed 'Admission Procedures' available at *https://www.lenmed.co.za*, accessed on 29 November 2021.
[528] Hereafter referred to as an 'SSL'.
[529] Fortinet 'What Is an SSL Certificate?' available at *https://www.fortinet.com*, accessed on 29 November 2021.
[530] Ibid.
[531] Commonly referred to as 'HTTPS'.
[532] Google Search Central 'Secure your site with HTTPS' available at *https://developers.google.com*, accessed on 29 November 2021.
[533] Deloitte op cit note 144.
[534] United States Department of Health and Human Services 'Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients' available at *https://www.phe.gov*, accessed on 29 November 2021.
[535] Joseph Migga Kizza op cit note 385 at 331.

systems as well as phishing attempts via the hospital's email systems. The ISO/IEC 27002 standards further suggest the implementation of software installation restrictions on organisational devices[536] to prevent employees from wilfully or negligently installing malware onto hospital devices that could harm the hospital's devices and networks.

4.8. INFORMATION OFFICERS

All public and private bodies are required to have an Information Officer in accordance with the PAIA and the POPIA. Public bodies are obligated to have an Information Officer in terms of Section 17 of the PAIA to manage requests for access to records. Private bodies (such as private hospitals) are obligated to provide access to records in terms of Section 50 of the PAIA. An 'Information Officer' for a private body is defined as the head of a private body as per Section 1 of the POPIA.[537] The duty of an Information Officer is to encourage compliance with the conditions for lawful processing as detailed in the POPIA.[538] The Information Regulator Guidance Note for Information Officers further delegates the task of devising policies for lawful processing of personal information to an Information Officer.[539] As per the Information Regulator Guidance Note, some other duties of an Information Officer include:[540]

(i) ensuring that a POPIA compliance framework is implemented, monitored and maintained;[541]

(ii) ensuring that a personal information impact assessment is performed to ascertain if there is compliance with the lawful conditions for processing;[542]

(iii) ensuring that a PAIA manual is developed[543] and maintained;[544]

---

[536] ISO *ISO/IEC 27002* (2013) at para 12.6.2.
[537] Information Regulator 'GUIDANCE NOTE ON INFORMATION OFFICERS AND DEPUTY INFORMATION OFFICERS' available at *http://www.presscouncil.org.za/,* accessed on 2 August 20212, para 1.4.
[538] POPIA, s 55(1).
[539] Information Regulator op cit note 537, para 6.1.1.1.
[540] Information Regulator op cit note 537, para 6.2.
[541] Information Regulator op cit note 537, para 6.2.1.
[542] Information Regulator op cit note 537, para 6.2.2.
[543] This manual must be in compliance with Section 51 of the PAIA.
[544] Information Regulator op cit note 537, para 6.2.3.

(iv) ensuring there are internal measures for the processing of requests for access to information;[545]

(v) ensuring that awareness training sessions are conducted, which focus on the requirements of the POPIA.[546]

Therefore the aforementioned duties are applicable to Information Officers employed at private hospitals and can enhance the privacy of patients' personal information if complied with, namely the POPIA awareness training and the monitoring of the efficacy of personal information processing practices. Information Officers who regularly attend awareness training and monitor the measures for the processing of patients' personal information contribute towards the security safeguards[547] of the personal information. The Information Officer can further assume the task of liaising with the Information Regulator and the public with regard to security incidents in accordance with Section 22 of the POPIA.

4.9. CONCLUSION

This chapter offered recommendations that comply with local legislation and international standards, such as: the disposal of patient records; the physical security of premises used for storing records and data; the development of an incident response plan; risk management practices; cybersecurity controls and; the education of employees on the risk prevention practices. The aforementioned recommendations were based on the identified risks and vulnerabilities with regard to patients' data.

[545] Information Regulator op cit note 537, para 6.2.4.
[546] Information Regulator op cit note 537, para 6.2.5.
[547] POPIA, s 19.

CHAPTER FIVE

CONCLUSION

5.1. RESEARCH SUMMARY

Firstly, this research consisted of a brief overview of the COVID-19 situation in South Africa. This was followed by a literature review containing the pertinent definitions in the POPIA, the NHA, the Cybercrimes Act,[548] the HPCSA guidelines (and other relevant legislation), cybersecurity, information security and the cyberattacks targeting the healthcare sector during the COVID-19 pandemic.

Subsequently, South African legislation relating to record-keeping and personal information were examined, which included: the PAIA, the POPIA, the NHA and the Cybercrimes Act.[549] The privacy of data subjects and legislative obligations placed upon responsible parties was provided in detail, in addition to the eight conditions for the lawful processing of personal information as per the POPIA.

The ensuing chapter investigated the privacy policy documents of private hospital groups with a focus on the protection of patients' personal information records (EPRs and EHRs) and any issues therein. WLANs and Wi-Fi networks were described, along with the IoT, and shortcomings in device connectivity.

Risk management, cybersecurity controls and employee awareness practices were proposed in relation to the prevention of data compromise incidents and with regard to hospital privacy policies.

[548] Act 19 of 2020.
[549] Ibid.

BIBLIOGRAPHY

I STATUTES

Children's Act 38 of 2005

s 1

s 13

Constitution of the Republic of South Africa, 1996

s 14

s 27

s 28

s 32

Cybercrimes Act 19 of 2020

s 1

s 2

s 3

s 5

s 6

Disaster Management Act 57 of 2002

Eastern Cape Provincial Health Act 10 of 1999

s 1

s 12

s 14

s 17

Electronic Communications and Transactions Act 25 of 2002

s 1

s 50

s 51

s 85

s 86

s 87

s 88

s 89

KwaZulu-Natal Health Act 1 of 2009

s 1

s 7

Mental Health Care Act 17 of 2002

s 13

National Health Act 61 of 2003

s 1

s 14

s 15

s 16

s 17

Promotion of Access to Information Act 2 of 2000

s 1

s 3

s 14

s 17

s 50

s 51

s 52

Protection of Personal Information Act 4 of 2013

s 1

s 2

s 3

s 5

s 6

s 8

s 9

s 10

s 11

s 12

s 13

s 14

s 15

s 16

s 17

s 18

s 19

s 20

s 21

s 22

s 23

s 24

s 25

s 26

s 27

s 28

s 29

s 30

s 31

s 32

s 33

s 35

s 39

s 55

s 72

s 74

s 75

s 76

s 77

s 78

s 80

s 99

II SECONDARY SOURCES

(a) Books

Dhai, A, McQuoid-Mason, D *Bioethics, Human Rights and Health Law* 2 ed Cape Town: Juta, (2020).

Kizza, JM *Guide to Computer Network Security* 4 ed London: Springer, (2017).

Lesame, Z, Mbatha, B, Sindane, S *NEW MEDIA IN THE INFORMATION SOCIETY* 1 ed Pretoria: Van Schaik, (2012).

Ming Pan, S, Te Chen, P, Ting Lo, Y, Wen Liu, P, Wen Wu, C 'CYBERSECURITY HEALTH CHECK' in K Andreasson (ed) *Cybersecurity: Public Sector Threats and Responses* Boca Raton: Taylor & Francis, (2012) 275-292.

Singh, JA 'LAW AND THE HEALTH PROFESSIONAL IN SOUTH AFRICA' in K Moodley (ed) *Medical ethics, law and human rights: A South African perspective* Pretoria: Van Schaik, (2017) 129-165.

Sue, D, Sue, D, Sue, DW, Sue, S *Understanding Abnormal Behavior* 11 ed Stamford: Cengage Learning, (2016).

The Open University *Introduction to cybersecurity* London: The Open University, (2016).

(b) Journal articles

Abidoye, AP, Adesina, AO, Agbele, KK, Februarie, R, Nyongesa, HO 'Ensuring the security and privacy of information in mobile health-care communication systems' (2011) 107(9/10) *South African Journal of Science* 1-7.

Adesina, AO, Agbele, K, Nyongesa, H 'ICT and Information Security Perspectives in E-Health Systems' (2010) 4(1) *Journal of Mobile Communication* 17-22.

Ameen, M, Kwak, K, Liu, J 'Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications' (2012) 36(93) *Journal of Medical Systems* 93-101.

Botha, A, Herselman, M, Thulare, T 'Data Integrity: Challenges in Health Information Systems in South Africa' (2020) 14(11) *International Journal of Computer and Information Engineering* 423-429.

Buys, M 'Protection of personal information: Implications of the Protection of Personal Information (POPI) Act for healthcare professionals' (2017) 107(11) *South African Medical Journal* 954-956.

Chigada, J, Madzinga, R 'Cyberattacks and threats during COVID-19: A systematic literature review' (2021) 23(1) *South African Journal of Information Management* 1-11.

Williams, PAH, Woodward, AJ 'Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem' (2015) 8 *Medical Devices: Evidence and Research* 305-316.

(c) Websites

'About COVID-19 (Coronavirus)', *Department of Health* available at https://sacoronavirus.co.za/information-about-the-virus-2/, accessed on 16 June 2021.

‘ACCESS TO INFORMATION MANUAL’ (October 2021), *Life Healthcare Group* available at https://www.lifehealthcare.co.za/media/3472/life-sept2021-final-paia-manual-updated-oct-4-2021.pdf, accessed on 24 November 2021.

‘Admission Procedures’, *Lenmed* available at https://www.lenmed.co.za/patient-information-lenmed/hospital-admissions-lenmed/, accessed on 29 November 2021.

‘Appendix 1: Retention and disposal of records’, *The Medical Protection Society* available at https://www.medicalprotection.org/southafrica/advice-booklets/medical-records-in-south-africa-an-mps-guide/appendix-1-retention-and-disposal-of-records, accessed on 29 November 2021.

‘APPLICATION FORM FOR AUTHORISATION TO PROCESS PERSONAL INFORMATION OF CHILDREN’, *Information Regulator (South Africa)* available at https://www.justice.gov.za/inforeg/docs/forms/InfoRegSA-Form-Application%20form%20for%20authorisation%20to%20process%20Personal%20Information%20of%20Children-eForm-2021.pdf, accessed on 03 November 2021.

Badman, L ‘What is the difference between WLAN and Wi-Fi?’ (June 2021), *TechTarget* available at https://www.techtarget.com/searchnetworking/answer/Wireless-vs-Wi-Fi-What-is-the-difference-between-Wi-Fi-and-WLAN, accessed on 28 November 2021.

Beran, D ‘THE RETURN OF ANONYMOUS’ (11 August 2020), *The Atlantic* available at https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/, accessed on 15 November 2021.

‘Beware of criminals pretending to be WHO’, *World Health Organization* available at https://www.who.int/about/cyber-security, accessed on 16 November 2021.

Bottomley, EJ ‘SA hit as hackers target hospitals during Covid-19 crisis – here’s what Life may be facing’ (10 June 2020), *Business Insider* available at https://www.businessinsider.co.za/life-hospitals-hit-by-cyberattack-2020-6, accessed on 17 November 2021.

‘CEH’, *EC Council* available at https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/, accessed on 29 November 2021.

‘Cisco Certifications’, *Cisco* available at https://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html, accessed on 29 November 2021.

Coble, S ‘NATO Condemns Cyber-Attacks’ (4 June 2020), *infosecurity* available at https://www.infosecurity-magazine.com/news/nato-condemns-cyberattacks/, accessed on 17 November 2021.

‘Contact Us’, *Information Regulator (South Africa)* available at https://justice.gov.za/inforeg/contact.html, accessed on 29 November 2021.

‘Coronavirus’, *World Health Organization* available at https://www.who.int/health-topics/coronavirus#tab=tab_1, accessed on 25 July 2021.

‘Coronavirus and COVID-19: What You Should Know’, *WebMD* available at https://www.webmd.com/lung/coronavirus#1-2, accessed on 31 October 2021.

‘COVID-19 Coronavirus vaccine’, *South African Government* available at https://www.gov.za/covid-19/vaccine/vaccine, accessed on 02 November 2021.

‘COVID-19 Coronavirus vaccine strategy’, *South African Government* available at https://www.gov.za/covid-19/vaccine/strategy, accessed on 02 November 2021.

‘COVID-19 Global Cyber risks: Attack surfaces expand amid return to work efforts’ (20 May 2020), *Deloitte* available at https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/COVID-19/gx-cyber-COVID-19-executive-briefing-issue-7-release-date-5.20.2020.pdf, accessed on 17 June 2021.

‘Cyber attackers eye SA businesses’ (28 June 2020), *ITWeb* available at https://www.itweb.co.za/content/PmxVEMKXY8xqQY85, accessed on 14 November 2021.

‘Cybercriminals targeting critical healthcare institutions with ransomware’ (04 April 2020), *INTERPOL* available at https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware, accessed on 06 June 2021.

‘Cybersecurity Basics’, *AVG* available at https://www.avg.com/en/signal/cyber-security-terms, accessed on 03 September 2021.

Daniel, L ‘Cellphone towers are crippled by load shedding – and theft of at least 200 batteries each month’ (10 November 2021), *Business Insider* available at https://www.businessinsider.co.za/no-cell-phone-signal-during-load-shedding-due-to-battery-theft-2021-11, accessed on 28 November 2021.

Department of Health *Patients’ Rights Charter* available at www.kznhealth.gov.za, accessed on 10 August 2021.

Doyle, K ‘BUSINESSES ILL-PREPARED FOR FOR CYBERATTACKS’ (06 December 2016), *ITWeb* available at http://v2.itweb.co.za/event/itweb/security-summit-2017/?page=news&itwid=158119, accessed on 13 November 2021.

Dyk, JV, Karim, AA ‘Phase 2 of SA’s Covid-19 vaccine rollout starts: This is how it works’ (17 May 2021), *news24* available at https://www.news24.com/news24/SouthAfrica/News/phase-2-of-sas-covid-19-vaccine-rollout-starts-this-is-how-it-works-20210517, accessed on 02 November 2021.

‘Eavesdropping’, *Fortinet* available at https://www.fortinet.com/resources/cyberglossary/eavesdropping, accessed on 28 November 2021.

‘Electronic Vaccination Data System (EVDS) Self Registration Portal’, *South African Government* available at https://www.gov.za/covid-19/vaccine/evds, accessed on 02 November 2021.

‘Elements of an Incident Response Plan’, *ISA Cybersecurity* available at https://isacybersecurity.com/elements-of-an-incident-response-plan/, accessed on 06 February 2022.

‘Enterprise risk management (ERM) in the COVID-19 world’, *Ernst & Young* available at https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/government-and-public-sector/ey-enterprise-risk-management-in-the-covid-19-world.pdf, accessed on 29 November 2021.

‘Essential services – Coronavirus COVID-19’, *South African Government* available at https://www.gov.za/covid-19/companies-and-employees/essential-services-coronavirus-covid-19, accessed on 29 November 2021.

‘EU Digital COVID Certificate’, *European Commission* available at https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en, accessed on 02 November 2021.

‘FBI probes cyber-attack emails sent from internal sever’ (14 November 2021), *BBC* available at https://www.bbc.com/news/world-us-canada-59278277, accessed on 15 November 2021.

‘Free Wi-Fi at Mediclinic’ (07 February 2017), *Mediclinic* available at https://www.thefutureofhealthcare.co.za/free-wi-fi-mediclinic/, accessed on 28 November 2021.

‘Free in-hospital Wi-Fi – a real patients perk’ (07 February 2017), *Mediclinic* available at https://www.mediclinicinfohub.co.za/free-hospital-wi-fi-real-patients-perk/, accessed on 28 November 2021.

Gentes-Hunt, L ‘How Health Facilities Can Prevent, Mitigate Ransomware in 2021’ (13 August 2021), *HealthITSecurity* available at https://healthitsecurity.com/news/how-health-facilities-can-prevent-mitigate-ransomware-in-2021, accessed on 29 November 2021

Ghosh, A 'Life Healthcare hit by cyber attack' (09 June 2020), *IOL* available at https://www.iol.co.za/business-report/companies/life-healthcare-hit-by-cyber-attack-49149807, accessed on 17 November 2021.

'Google 2-Step Verification', *Google* available at https://www.google.com/landing/2step/, accessed on 29 November 2021.

Grau, A 'Securing Medical Devices: What is Really Needed?' (09 January 2020), *MedTech Intelligence* available at https://www.medtechintelligence.com/feature_article/securing-medical-devices-what-is-really-needed/, accessed on 06 February 2022.

'Group profile', *Netcare* available at https://www.netcare.co.za/Who-We-Are/Group-at-a-glance/Group-profile/, accessed on 25 November 2021.

'Hackers strike at Life Healthcare, extent of data breach yet to assessed' (09 June 2020), *TIMESLIVE* available at https://www.timeslive.co.za/news/south-africa/2020-06-09-hackers-strike-at-life-healthcare-extent-of-data-breach-yet-to-be-assessed/, accessed on 17 November 2021.

'Hacking definition: What is hacking?', *Malwarebytes* available at https://www.malwarebytes.com/hacker, accessed on 03 September 2021.

'Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients', *United States Department of Health and Human Services* available at https://www.phe.gov/preparedness/planning/405d/documents/hicp-main-508.pdf, accessed on 29 November 2021.

Health Professions Council of South Africa *CONFIDENTIALITY: PROTECTING AND PROVIDING INFORMATION BOOKLET 5* available at www.hpcsa.co.za, accessed on 02 September 2021.

Health Professions Council of South Africa *GUIDELINES ON THE KEEPING OF PATIENT RECORDS BOOKLET 9* available at www.hpcsa.co.za, accessed on 26 August 2021.

Hoffman, C 'Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both?' (20 July 2017), *How-To Geek* available at https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/, accessed on 28 November 2021.

'How does a VPN work?', *Norton* available at https://us.norton.com/internetsecurity-wifi-how-does-a-vpn-work.html, accessed on 06 February 2022.

'How To Detect the Presence of a Keylogger on Your Phone', *Fortinet* available at https://www.fortinet.com/resources/cyberglossary/how-to-detect-keylogger-on-phone, accessed on 29 November 2021.

'How to use two-step verification with your Microsoft account', *Microsoft* available at https://support.microsoft.com/en-us/account-billing/how-to-use-two-step-verification-with-your-microsoft-account-c7910146-672f-01e9-50a0-93b4585e7eb4, accessed on 29 November 2021.

'IATA Travel Pass Initiative', *International Air Transport Association* available at https://www.iata.org/en/programs/passenger/travel-pass/, accessed on 02 November 2021.

'ICDL Programmes', *ICDL Africa* available at https://icdlafrica.org/icdl-programmes/, accessed on 29 November 2021.

'incident response plan', *National Institute of Standards and Technology* available at https://csrc.nist.gov/glossary/term/incident_response_plan#:~:text=Definition(s)%3A,organization's%20information%20systems(s)., accessed on 06 February 2022.

'Information Manual' (June 2021), *Netcare* available at https://www.netcare.co.za/Portals/_default/GlobalDocuments/Information-Manual-June-2021-v7.1.pdf, accessed on 26 November 2021.

Information Regulator *GUIDANCE NOTE ON INFORMATION OFFICERS AND DEPUTY INFORMATION OFFICERS* available at www.presscouncil.org.za, accessed on 02 August 2022.

‘INSIGHT INTO THE CYBERTHREAT LANDSCAPE IN SOUTH AFRICA’, *Accenture* available at https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf, accessed on 15 November 2021.

International Organization for Standardization *ISO 31000* available at https://www.iso.org, accessed on 29 November 2021.

International Organization for Standardization *ISO/IEC 27002* available at https://www.iso.org, accessed on 17 November 2021.

‘IoT Edge’, *Fortinet* available at https://www.fortinet.com/resources/cyberglossary/iot-edge, accessed on 28 November 2021.

‘It’s 2021 and the most common password is still 123456’ (21 November 2021), *MyBroadband* available at https://mybroadband.co.za/news/security/423790-its-2021-and-the-most-common-password-is-still-123456.html, accessed on 28 November 2021.

Labuschagne, H ‘This is how many vaccine certificates were issued last week’ (11 October 2021), *MyBroadband* available at https://mybroadband.co.za/news/government/417752-this-is-how-many-vaccine-certificates-were-issued-last-week.html, accessed on 02 November 2021.

‘Lenmed PAIA Information Manual’ (June 2021), *The Lenmed Group* available at https://www.lenmed.co.za/wp-content/uploads/lenmed-health-group-paia-manual-2021.pdf, accessed on 26 November 2021.

‘Lenmed Privacy Policy’ (June 2021), *The Lenmed Group* available at https://www.lenmed.co.za/wp-content/uploads/Lenmed-Privacy-Policy-2021-1.pdf, accessed on 26 November 2021.

‘Lenmed Private Hospitals’, *The Lenmed Group* available at https://www.lenmed.co.za/about-lenmed/, accessed on 26 November 2021.

‘LIFE HEALTHCARE CYBER INCIDENT Q & A’ (09 June 2020), *Life Healthcare Group* available at https://www.lifehealthcare.co.za/media/3177/20200609_life-healthcare-cyber-incident_web-q-and-a-final.pdf, accessed on 19 April 2021.

Lindros, K, Tittel, E ‘How to create an effective business continuity plan’ (18 July 2017), *CIO* available at https://www.cio.com/article/2381021/best-practices-how-to-create-an-effective-business-continuity-plan.html, accessed on 29 November 2021.

Lotz, B ‘Employees using IT resources for the wrong thing could be costly’ (18 October 2021), *Hypertext* available at https://htxt.co.za/2021/10/employees-using-it-resources-for-the-wrong-thing-could-be-costly/, accessed on 28 November 2021.

Mabuza, E ‘SA remains pegged below 50 points in Corruption Perception Index’ (28 January 2021), *TIMESLIVE* available at https://www.timeslive.co.za/news/south-africa/2021-01-28-sa-remains-pegged-below-50-points-in-corruption-perception-index/, accessed on 28 November 2021.

Majola, G ‘SA data usage soars’ (11 May 2021), *IOL* available at https://www.iol.co.za/business-report/companies/sa-data-usage-soars-26679d38-1f69-4768-baad-349115770091, accessed on 27 November 2021.

McKeon, J ‘How to Implement a Cyber Incident Response Plan for Healthcare’, *HealthITSecurity* available at https://healthitsecurity.com/features/how-to-implement-a-cyber-incident-response-plan-for-healthcare, accessed on 29 November 2021.

McKeon, J ‘The Importance of Third-Party Risk Assessments in Healthcare’, *HealthITSecurity* available at https://healthitsecurity.com/features/the-importance-of-third-party-risk-assessments-in-healthcare, accessed on 29 November 2021.

McKeon, J ‘Top Healthcare Cybersecurity Challenges, How to Overcome Them’, *HealthITSecurity* available at https://healthitsecurity.com/features/top-healthcare-cybersecurity-challenges-how-to-overcome-them, accessed on 29 November 2021.

Meldrum, A, Mogomotsi, M 'South Africa's Ramaphosa says corruption has damaged country' (28 April 2021), *Associated Press News* available at https://apnews.com/article/africa-south-africa-business-government-and-politics-e806adebeaef73acd6326316eb0f72af, accessed on 28 November 2021.

Mungadze, S 'Life Healthcare reveals damage caused by data breach' (31 August 2020), *ITWeb* available at https://www.itweb.co.za/content/rW1xLv59YPGvRk6m, accessed on 06 June 2021.

Naidoo, S 'Cybercrime on the rise since start of lockdown' (05 December 2020), *IOL* available at https://www.iol.co.za/weekend-argus/news/cybercrime-on-the-rise-since-start-of-lockdown-a0e3739c-b026-43e3-8b25-cc85596ad6e1, accessed on 22 November 2021.

National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* available at https://nvlpubs.nist.gov/, accessed on 29 November 2021.

'Netcare Privacy Policy' (September 2021), *Netcare* available at https://www.netcare.co.za/Portals/_default/GlobalDocuments/NETCARE-GROUP-PRIVACY-POLICY-WEBSITE-SEPTEMBER-2021.pdf, accessed on 26 November 2021.

'NIST Risk Management Framework' (01 November 2021), *NIST* available at https://csrc.nist.gov/projects/risk-management/about-rmf, accessed on 29 November 2021.

'Panda Cybersecurity Report 2017: Africa in top 10 targeted regions' (08 June 2018), *ITWeb* available athttps://www.itweb.co.za/content/zKWEBbvy4ZNqmRjO, accessed on 14 November 2021.

'patient rights and responsibilities' (December 2015), *Life Healthcare Group* available at https://www.lifehealthcare.co.za/media/1056/patient-rights-and-responsibilities-leaflet.pdf, accessed on 24 November 2021.

‘Privacy Notice’ (14 September 2017), *Life Healthcare Group* available at https://www.lifehealthcare.co.za/media/2412/h-lhc-website-privacy-notice.pdf, accessed on 12 June 2021.

‘Privacy Notice’ (28 January 2021), *Life Healthcare Group* available at https://www.lifehealthcare.co.za/media/3276/website-privacy-notice-updated-15-03-2021.pdf, accessed on 24 November 2021.

‘PRIVACY NOTICE TO PATIENTS’ (01 July 2021), *Mediclinic* available at https://www.mediclinic.co.za/content/dam/mc-sa-corporate/downloads/privacy/POPIA_Data_Privacy_Notice-Patients-MCSA_V1.0.pdf, accessed on 27 November 2021.

‘Protection of Personal Information Act (POPI Act)’, *POPIA* available at https://popia.co.za/, accessed on 29 July 2021.

‘PwC focuses on cyber attacks’ (28 May 2019), *ITWeb* available at https://www.itweb.co.za/content/JBwErvn5wg2q6Db2, accessed on 14 November 2021.

‘QR Code Security: What are QR codes and are they safe?’, *Kaspersky* available at https://www.kaspersky.co.za/resource-center/definitions/what-is-a-qr-code-how-to-scan, accessed on 02 November 2021.

Quek, T ‘The advantages and disadvantages of Internet Of Things (IoT)’ (14 February 2017), *LinkedIn* available at https://www.linkedin.com/pulse/advantages-disadvantages-internet-things-iot-tommy-quek, accessed on 06 February 2022.

‘Secure your site with HTTPS’, *Google Search Central* available at https://developers.google.com/search/docs/advanced/security/https, accessed on 29 November 2021.

‘South African COVID-19 Vaccine Certificate System’, *Department of Health* available at https://vaccine.certificate.health.gov.za/, accessed on 02 November 2021.

‘South African is getting an updated vaccine certificate at the end of October – here are 9 other things to know’, *BusinessTech* available at https://businesstech.co.za/news/lifestyle/528962/south-africa-is-getting-an-updated-vaccine-certificate-at-the-end-of-october-here-are-9-other-things-to-know/, accessed on 02 November 2021.

‘South Africa’s Life Healthcare hit by cyber attack’ (09 June 2020), *Reuters* available at https://www.reuters.com/article/us-life-healthcare-cyber-idUSKBN23G0MY, accessed on 17 November 2021.

‘Statement by President Cyril Ramaphosa on measures to combat COVID-19 epidemic’ (15 March 2020), *Department of Health* available at https://sacoronavirus.co.za/2020/03/15/statement-by-president-cyril-ramaphosa-on-measures-to-combat-covid-19-epidemic/, accessed on 16 June 2021.

Subramoney, N ‘Calls for transparency after justice department cyber attack’ (13 September 2021), *The Citizen* available at https://www.citizen.co.za/lifestyle/technology/2623360/calls-for-transparency-after-justice-department-cyber-attack/, accessed on 15 November 2021.

‘TERMS AND CONDITIONS OF ADMISSION’ (October 2021), *Netcare* available at https://www.netcare.co.za/Portals/4/Documents/Netcare%20Admission%20Terms%20and%20Conditions.pdf, accessed on 26 November 2021.

‘The 2021 Ransomware Survey Report’, *Fortinet* available at https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-ransomware-survery.pdf, accessed on 15 November 2021.

‘The impact of COVID-19 on enterprise-level risk management’ (19 April 2021), *Deloitte* available at https://www2.deloitte.com/hu/en/pages/technology/articles/the-impact-of-COVID-19-on-enterprise-level-risk-management.html, accessed on 29 November 2021.

‘Tips on how to protect yourself against cybercrime’, *Kaspersky* available at https://www.kaspersky.co.za/resource-center/threats/what-is-cybercrime, accessed on 03 September 2021.

‘Understanding malware & other threats’ (29 June 2021), *Microsoft* available at https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/understanding-malware, accessed on 03 September 2021.

‘Update on Covid-19 (Saturday 30 October 2021)’ (30 October 2021), *Department of Health* available at https://sacoronavirus.co.za/2021/10/30/update-on-covid-19-saturday-30-october-2021/, accessed on 01 November 2021.

Vermeulen, J ‘Alarming number of security breaches in South Africa’ (19 September 2021), *MyBroadband* available at https://mybroadband.co.za/news/security/414724-alarming-number-of-security-breaches-in-south-africa.html, accessed on 16 November 2021.

Vermeulen, J ‘South Africa’s Covid-19 vaccine certificate goes live’ (08 October 2021), *MyBroadband* available at https://mybroadband.co.za/news/government/417580-south-africas-covid-19-vaccine-certificate-goes-live.html, accessed on 02 November 2021.

Vermeulen, J ‘Warning over vaccine certificate personal information’ (12 October 2021), *MyBroadband* available at https://mybroadband.co.za/news/government/418012-warning-over-vaccine-certificate-personal-information.html, accessed on 02 November 2021.

‘Vulnerability Assessment’, *Fortinet* available at https://www.fortinet.com/resources/cyberglossary/vulnerability-assessment, accessed on 29 November 2021.

‘Welcome to your personal Health Centre’, *Netcare* available at https://www.netcare.co.za/mynetcare-online/, accessed on 29 November 2021.

‘What is 4G LTE and why it matters’, *Verizon* available at https://www.verizon.com/about/news/what-4g-lte-and-why-it-matters, accessed on 28 November 2021.

‘What is a Cyber Attack?’, *Fortinet* available at https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks, accessed on 15 November 2021.

‘What is a cyber attack?’ (17 July 2020), *NordVPN* available at https://nordvpn.com/blog/what-is-a-cyber-attack/, accessed on 03 September 2021.

‘What is ADSL?’ (23 June 2021), *BusinessTech* available at https://businesstech.co.za/news/industry-news/500289/what-is-adsl/, accessed on 28 November 2021.

‘What Is a Firewall?’, *Fortinet* available at https://www.fortinet.com/resources/cyberglossary/firewall-defined, accessed on 29 November 2021.

‘What is a keylogger and how do I protect myself against one?’ (01 June 2020), *Norton* available at https://us.norton.com/internetsecurity-malware-what-is-a-keylogger.html, accessed on 17 June 2021.

‘What Is an SSL Certificate?’, *Fortinet* available at https://www.fortinet.com/resources/cyberglossary/ssl-certificate, accessed on 29 November 2021.

‘What is a phishing attack?’, *Cloudflare* available at https://www.cloudflare.com/learning/access-management/phishing-attack/, accessed on 16 November 2021.

‘What is a Threat Actor and Why Should You Care?’ (26 March 2021), *Sophos* available at https://home.sophos.com/en-us/security-news/2021/what-is-a-threat-actor.aspx, accessed on 03 September 2021.

‘What is Bring Your Own Device (BYOD)?’, *Forcepoint* available at https://www.forcepoint.com/cyber-edu/bring-your-own-device-byod, accessed on 06 February 2022.

‘What Is Cybersecurity?’, *Avast* available at https://www.avast.com/c-b-what-is-cybersecurity#topic-1, accessed on 14 August 2021.

‘What is data security?’, *IBM* available at https://www.ibm.com/topics/data-security, accessed on 03 November 2021.

‘What is Information Security?’, *Cisco* available at https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html, accessed on 17 June 2021.

‘What Is Ransomware?’, *McAfee* available at https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware.html, accessed on 17 June 2021.

‘What is SSID?’, *D-Link* available at https://eu.dlink.com/uk/en/support/faq/access-points-and-range-extenders/what-is-ssid, accessed on 28 November 2021.

‘What is the COVID Passport for travelling?’, *COVID Passport* available at https://www.covidpasscertificate.com/, accessed on 02 November 2021.

‘What Is Wireless Encryption and Why Is It Used?’ (14 April 2021), *Sony* available at https://www.sony.com/electronics/support/articles/00009475, accessed on 28 November 2021.

‘WHO Coronavirus (COVID-19) Dashboard’, *World Health Organization* available at https://covid19.who.int/, accessed on 31 October 2021.

‘WHO reports fivefold increase in cyber attacks, urges vigilance’ (23 April 2020), *World Health Organization* available at https://www.who.int/news/item/23-04-2020-who-

reports-fivefold-increase-in-cyber-attacks-urges-vigilance, accessed on 03 September 2021.

'Wifi', *Netcare* available at https://www.netcare.co.za/Wifi, accessed on 28 November 2021.

World Health Organization *Definitions of Key Concepts from the WHO Patient Safety Curriculum Guide (2011)* available at www.who.int, accessed on 26 August 2021.

APPENDIX 1: ETHICAL CLEARANCE

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

Ms Ashwini Singh (219052945)
School Of Law
Howard College

Dear Ms Ashwini Singh,

Protocol reference number: 00013002
Project title: Securing the privacy of patients electronic personal information in South African hospitals during COVID-19

Exemption from Ethics Review

In response to your application received on 23 June 2021 , your school has indicated that the protocol has been granted **EXEMPTION FROM ETHICS REVIEW.**

Any alteration/s to the exempted research protocol, e.g., Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through an amendment/modification prior to its implementation. The original exemption number must be cited.

For any changes that could result in potential risk, an ethics application including the proposed amendments must be submitted to the relevant UKZN Research Ethics Committee. The original exemption number must be cited.

In case you have further queries, please quote the above reference number.

PLEASE NOTE:
Research data should be securely stored in the discipline/department for a period of 5 years.

I take this opportunity of wishing you everything of the best with your study.

Yours sincerely

[redacted]

Mr Simphiwe Peaceful Phungula
obo Academic Leader Research
School Of Law