The evolution of privacy governance in healthcare in post-apartheid South Africa

Introduction

Professor Lenka Bula, Vice Chancellor and Principal UNISA, Professor Motsa Madikane, Vice Principal teaching and learning, community engagement, and student support, Professor Kole Acting Executive Dean College of Law, Professor Dube, Acting Director, School of Law, Dr Morodi, Director, School of Criminal Justice. My respondent, Professor Labuschaigne, Department of Jurisprudence UNISA, colleagues, family, friends…

Prior to the advent of South Africa's democratic dispensation, the right to privacy was largely recognised at common law and not the subject of significant codification. This position has significantly changed with the right to privacy being progressively developed with specific regard to clinical practice and health research. With the advent of the Constitution, and increasing awareness of research participant protections, a concept that was predominantly interpreted by the common law, is now governed by various pieces of legislation, ethical guidelines and influenced by international instruments.

Failure to observe patient privacy strikes at the heart of the fiduciary relationship between a health professional and patient. Trust between the patient and the health care professional is critical to the optimal utilisation of health services by patients for their ultimate well-being. The same principles regarding protecting privacy to encourage trust, applies when one considers the relationship between researcher and research participant. This lecture explores the post-transition evolution of privacy in the healthcare context in South Africa. It showcases the legislative and ethical strides that South Africa has taken over the past 29 years in protecting patients and research participants' fundamental right to privacy from, its inception within the Bill of Rights, to its emphasis on protecting personal information/ data under the Protection of Personal Information Act. It further outlines some of the challenges to privacy as a result of recent statutory developments and considers how these challenges could be managed practically in an open data driven society.

The development of privacy governance in healthcare in South Africa cannot be discussed without reflecting on the past to truly understand why a fundamental rights focus is critical to our context. The historical exploitation of African populations regarding health research transgressions and health services delivery is a reality. However, the gravity of some of these atrocities were only highlighted post-democracy during the Truth and Reconciliation Commission (TRC) Hearings. This includes the gross medical ethics and human rights abuses conducted under the guise of scientific experimentation and at the hands of the man ominously dubbed as South Africa's "Dr Death", Wouter Basson, a cardiologist and personal physician to then State President PW Botha. Ultimately, the TRC found that with the support of an extensive international network, scientists, doctors, dentists, and laboratories, amongst others, supported the apartheid Chemical and Biological Warfare program, more commonly known as Project Coast. It further held that Project Coast was "evidence of science being subverted to cause disease and undermine the health of communities". With such disregard to the victims' human rights, it is highly unlikely that there was any consideration towards their privacy.

Perhaps the most prominent example of medical professionalism being undermined by corrupting and morally reprehensive attitudes and actions, is that of the murder of Steve Biko, anti-apartheid activist and leader of the Black Consciousness movement, who died in 1977 while in police detention and as a result of the grossly inadequate treatment received from two doctors responsible for his care. Over 5 days in which they supposedly attended to Biko's care, his doctors failed to take his condition seriously. They failed to examine Biko under proper conditions despite obvious signs of possible brain damage; no history was taken; simple tests regarding Biko's mental state were also not carried out, his personal medical data was shared with the state without consent and; they allowed the police to be present during the examination, which despite influencing their diagnosis and management, clearly violated Biko's right to privacy and confidentiality. Apart from the obvious human rights atrocities meted out against Biko at the hands of the doctors responsible for his care, who have been described as "moral monsters," there was a flagrant disregard of doctor-patient confidentiality and a violation of Biko's privacy.

The fact that there have only been a handful of prosecutions for the gross human rights abuses committed under the apartheid regime, speaks to the need to ensure tighter regulatory measures where the dignity of the people of South Africa are at stake to foster trust amongst the population. This is even more relevant in the healthcare setting where patients are in a vulnerable position with complete trust being placed in medical professionals responsible for their care. It is with this background in mind, that I turn to discuss the ethico-legal evolution of privacy governance regarding healthcare in post-apartheid South Africa.

The main difference between the rights to privacy and confidentiality is that while the right to privacy may be invoked to prevent anyone from accessing an individual's personal information, confidentiality rests on a trust relationship and therefore binds specific individuals only. While confidentiality is often described as an ethical obligation, it is very much a legal requirement in the medical sector.

The protection and recognition of the right to privacy as a fundamental human right, provides an indication of its importance. In terms of section 14 of the Constitution, the right to privacy includes the right not to have one's person searched. The physical examination of a person in the health care/ health research context can then be interpreted to be an invasion of privacy. Such examination may only occur if the person waives their right to privacy. Further, information related to the health status of a person is inextricably bound to issues of privacy. However, the constitutional right to privacy is not absolute and may be limited. In addition to protections developed under the Constitution, the right to privacy in the healthcare context is further safeguarded in various laws and policy documents beginning with the National Heath Act 61 of 2003 (NHA).

The NHA provides a framework for a structured uniform health system considering the obligations imposed by the Constitution and other laws on national, provincial and local government with regard to health services. Section 14 (1) of the NHA stipulates that all information of a person receiving treatment, including information relating to his/her health status, treatment or stay in a health establishment, is confidential. This is a significant guarantee under the NHA, as without an assurance of confidentiality, patients may be hesitant to use health facilities and disclose necessary information for a diagnosis and

treatment. However, confidential information may be disclosed where consent is provided in writing; a court order or law requires disclosure; or where non-disclosure will represent a serious threat to public health. For example, during the Covid-19 pandemic, regulations were developed for the disclosure of patients' Covid-19 statuses to effect quarantine, isolation and hence not infect others. The NHA creates a further exception with regard to the access of health records by allowing for a health worker or health care provider to disclose personal information of the person receiving treatment, if it is necessary for any legitimate purpose within the ordinary course and scope of their duties, where such disclosure is in the best interests of the person receiving treatment. In addition, the NHA contains provisions for the access to and protection of health records. While the NHA provides for the broad protection of patient privacy and confidentiality, perhaps the most significant piece of legislation that came into effect in July 2021, and which has had an impact on privacy in the healthcare sector and challenged existing practices within the health research sector, is the Protection of Personal Information Act 4 of 2013 (POPIA).

Based on the European Union's General Data Protection Regulation, POPIA defines personal information broadly and covers all information related to an identifiable, living person and an identifiable, existing juristic person. It is aligned with international data protection standards and aims to regulate the processing of personal information and safeguards individuals' rights to privacy. This extends to protecting against the unlawful collection, retention, dissemination, and use of personal information. The essence of data protection is to provide a person control over their personal information subject to certain prescribed limitations outlined in law. With more stringent measures in place regarding the use and transfers of personal information, one immediate tension evident from POPIA, is the strain between the right to individual privacy on the one hand and data sharing in the context of open science on the other, which needs to be balanced to ensure progress on economic, social, health care and educational fronts. To this end, and to clarify the application of POPIA to research, including health research, the Academy of Science of South Africa (ASSAf) developed a Code of Conduct for Research which, is at the time of recording this lecture, being considered by the Information Regulator.

It is the responsibility of the responsible party (in the health care context either the practitioner or researcher) to ensure the lawful processing of personal information in a manner that does not infringe on the constitutional rights of individuals to privacy. Essentially, when personal information is collected for research purposes, a participant should know what type of information is being collected, why it is being collected, what will happen to the information, how long it will be retained, whether it will identify the participant, if and why it will be shared and whether it will be transferred outside SA and why. In addition, in the health research context where transfers of personal information across international borders are common-place, POPIA provides an added layer of regulation. Specific health research challenges brought about by the enactment of POPIA and the responses to these challenges, will be discussed later in this lecture. Another piece of legislation which has a bearing on personal information is the Promotion of Access to Information Act 2 of 2000 (PAIA) which like POPIA, is currently under the ambit of the Information Regulator. PAIA attempts to balance the right to information with the right to privacy and impacts how information should be accessed. More relevant to this lecture is the processing of personal information under POPIA. Now that the privacy protections under the Constitution, the NHA and POPIA have

been briefly examined, it is prudent to canvass how the right to privacy developed regarding healthcare under the common-law.

A breakthrough regarding the duty of a healthcare provider to keep a patient's medical information confidential was achieved in *Jansen van Vuuren NNO v Kruger*, decided before the adoption of the Bill of Rights. In this case, the HIV status of a patient was unlawfully disclosed over a game of golf, by the patient's doctor to a dentist who knew the patient. Unsuccessful in the High Court, the patient's right to medical confidentiality was upheld on appeal. Sadly, the patient succumbed to an AIDS -related illness by the time the judgement was finalised. The Appellate Division of the Supreme Court (now the Supreme Court of Appeals) held that a healthcare provider has both an ethical and legal duty to respect a patient's confidentiality. In *NM V Smith,* the court found that a biography about Patricia De Lille invaded the right to privacy of three female participants involved in a clinical trial, whose HIV-positive status and names were disclosed in it. In addition, at least two inter-related reasons for the constitutional protection of privacy were identified, the first stemming from the constitutional idea of what it means to be a human being, implicit in which is the right to choose what personal information is released into the public arena. The more intimate the information, the more important it becomes to safeguard privacy, dignity and autonomy in that an individual makes the primary decision whether to release the information. The second reason for protecting privacy is the democratic need to reduce the power of the state and to prevent it from denying liberty and dignity by interfering with personal private space. O'Regan J further highlighted in this case the inter-relationship between privacy, liberty and dignity as the key constitutional rights which construct our understanding of what it means to be a human being. Therefore, all these rights are interdependent and mutually reinforcing.

Additional to developments under the common law, the confidentiality requirements set out in the NHA, and provisions which regulate the protection of personal information under POPIA, healthcare providers have ethical duties to protect patient privacy and confidentiality. The fact that the concept of privacy is no longer limited to safeguarding discussions between a doctor and patient in clinical practice settings, and now extends to "big data" generated in the care of patients in modern medicine, makes it prudent to establish how our ethical guidelines, which have quasi-legal standing, have been reformed to incorporate these changes. I will begin this discussion by outlining the Health Professions Council Guideline on Confidentiality, as, revised in 2021.

The HPCSA was established by the Health Professions Act, replacing the old South African and Medical Dental Council as the supreme statutory body regulating the medical profession. Apart from setting out requirements to maintain and retain patient confidentiality, the importance of protecting personal information against improper disclosure is emphasised within the HPCSA Guideline on Confidentiality. The Guideline is aligned with the aforementioned provisions of the NHA. The Guidelines place a duty on a healthcare practitioner to ensure appropriate arrangements for the security of personal information when it is stored, sent or received by electronic means. They also caution practitioners that information sent through the internet may be intercepted and that this should be a deciding factor whether, and in what form to transmit personal information. Another ethical guideline which recognises the privacy risks that come with the advent of new technologies which have driven a cultural transformation in the delivery of healthcare and more particularly for health research, is the

revision of the national Ethics in Health Research Guidelines, Principles, Structures and Processes, which at the time of recording this lecture is still in draft form.

The National Health Research Ethics Council (NHREC) was established in accordance with section 69(1) of the NHA. One of the responsibilities of the NHREC is to determine guidelines for the functioning of health research ethics committees, to facilitate best practice. Accordingly, the first edition of the Department of Health, National Ethics Guidelines was published in 2004, the second edition, in 2015 and it is currently under revision towards a third edition. The draft Revision broadly recognises research participants rights to privacy and confidentiality and that researchers have a duty to protect these rights through the course of the research process, including when disseminating research results or findings. They also rely heavily on POPIA and reiterate the newly legislated stipulations in place for the processing of personal information, including cross-border transfers of information.

Importantly, the draft Revision recognises that data sharing raises specific ethical concerns in relation to privacy and that data sharing decisions involve trade-offs between protecting privacy and advancing research and attempt to guide researchers and RECs when the use and transfer of data is contemplated. There is conflict between serving individual autonomy by keeping data confidential and advancing the possibility of public beneficence by sharing data. A key consideration for researchers, is how to find a balance between these competing interests. In South Africa, the regulation of the transfer of human biological materials should be set out in a Material Transfer Agreement (MTA). The draft Revision of the Guidelines acknowledge that although some MTA's may include clauses regulating the transfers of data, it is advisable to enter into separate Data Transfer Agreements (DTAs) for one or more data sets from the provider to a third party. Further guidance to RECs is outlined for consideration during the protocol review process when data transfers are envisaged.

With regard to re-identifiability the draft Revision acknowledges the possibility of re-identification, with specific reference to groups rather than individuals, through genetic markers. It is the responsibility of researchers to pay attention to eliminating or at least minimize privacy and autonomy risks resulting from re-identification. Therefore, the Draft Revision attempts to address some of the challenges that have developed through the enactment of new legislation regarding the protection of personal information and includes added guidance for RECs on how to manage these challenges.

At this juncture I would like to pause and appreciate that privacy governance in South Africa has developed at a rapid pace and in line with international best practice, over the past 29 years regarding protecting patients and research participants. However, the development of new privacy laws, particularly data protection laws have come at a time when open science and the wide sharing of data for research purposes is gaining momentum. South Africa has aligned itself with the open science trend. To this end, the Draft National Open Science policy which encourages open science, open data and open access, was approved for stakeholder consultation in 2022. In addition, in 2021 the Draft National Data and Cloud policy was published with a vision to transform South Africa into a data driven digital economy. Both these policies encourage open data sharing. On the face of it, POPIA may appear to create underlying challenges between achieving an open science framework for research, against its strict privacy protections geared towards the processing of personal information. However,

POPIA is not a research framework *per se*, therefore these challenges need to be balanced with the progress of research in the era of open science. The first challenge I will address is managing cross-border information flows.

In accordance with section 72 of POPIA, international transfers may take place under five circumstances, three of which appear relevant for research purposes, however only one ground appears to be practical:

Which is when the recipient in the foreign country is subject to a law, binding corporate rules or binding agreement that provides for an adequate level of protection that upholds principles that are substantially similar for the processing of personal information.

A binding contractual agreement, for example a DTA that uphold the principles for the processing of personal information as set out in POPIA, seems to provide a realistic solution for the transfers of personal information outside our borders. Currently, the South African Material Transfer Agreement template, gazetted into law in July 2018, provides some guidance for researchers regarding the transfers of materials and data outside South Africa. However, as the template was published prior to POPIA coming into effect, it is limited regarding the transfers of personal information. The NHREC is also currently revising the national MTA template. Therefore, the fact that a binding DTA appears to be the most practical solution for international transfers of personal information, together with the fact that the current MTA template is limited in its application and currently under revision, has prompted a call for the development of a national DTA template to facilitate and safeguard the transfers of personal information outside South African borders. This then prompts a second challenge regarding how much is too much when personal information is processed.

POPIA appears to be focused on a minimalistic approach – the less personal information processed, the better. This seems to be contrary to the Draft National policy on Open Science which encourages scientists to ensure "optimal use and reuse of research data" and the Draft Data and Cloud policy which aims to transform SA into a data intensive and data driven digital economy with data sharing being encouraged between multiple users. The Draft policy on open science follows the principle of 'as open as possible, as closed as necessary' to ensure that 'maximum benefit is derived from all publicly funded research.' It applies to research generated from public funds, however, indicates that it will be applied on a best-effort basis when research is funded by the private sector or by philanthropic funders and is made subject to contractual conditions requiring open science. The Draft Data and Cloud policy applies to everyone including public and private institutions and (controversially) states that any data generated in the country will be owned by South Africa regardless of where the technology used to generate it is situated, or where the technology company is domiciled. In addition, the Draft Data and Cloud policy concedes under its background and context that "the digital economy is a sharing economy" with the integrity of any digital economy depending on the extent to which sharing advantages are delivered amongst its ecosystem partners. It also proposes the development of a national open data strategy which incorporates principles that data should be open by default, accessible, usable and reusable, comparable and interoperable and trusted. Wide accessibility and re-usability of data are core objectives of both draft policies. While both draft policies respect privacy protections, the language used appears to be much broader than the minimalist approach taken by POPIA where personal

information is subject to limitations depending on the purpose for which it is processed. To provide guidance to researchers, the ASSAf COC developed a minimality assessment to assess whether the processing of identifiable personal information is necessary and proportional.

Although POPIA takes a more cautious approach to the processing of personal information, it does include exceptions from its strict provisions when processing is for research purposes. However, with the Draft National Policy on Open Science and the Draft Data and Cloud policy recognising the significance of South Africa being part of a globally inclusive digital economy, with the latter appreciating data as the "new oil," questions around practically managing the sharing of personal information in an open access space, arise. Furthermore, POPIA is specific to protecting personal information while the Draft Policy on Open Science does not distinguish between personal and non-personal information/data. Yet, the Draft Data and Cloud policy appears to extend the application of POPIA to data and international data transfers that are currently not under its scope.

De-personalised information / data, for example, data that was once personal information but manipulated into anonymous data where the data subject is no longer identifiable, is theoretically not considered personal information under POPIA. However, questions remain around how to treat data that can potentially be re-identified and no specific guidance is provided by POPIA on how de-identification can be achieved. The ASSAf COC attempts to provide clarity to this issue and defines de-identification to mean the deletion of personal information that identifies research participants; can be manipulated to identify research participants; or that can be linked by a reasonably foreseeable method to other information that identifies research participants. However, it acknowledges that complete de-identification is difficult, if not impossible to achieve, considering technological advancements and the fact that increasing volumes of personal information are in the public domain. Categorising information as personal or non-personal depends on the context and has practical ramifications beyond theoretical debate.

Clearly, there are challenges which have been brought about by POPIA which have implications for the practical management of data in the era of open science. A careful balance needs to be established when drawing the line between overstepping privacy of the participant on the one hand and promoting health research for the common good of mankind, on the other. It is difficult to provide exact boundaries as the nature of technologies are always developing and changing rapidly. These boundaries have blurred even further with the advent of artificial intelligence. As such, a discussion regarding the underlying challenges to the right to privacy would not be complete without touching on the role and risks associated with artificial intelligence in healthcare.

According to the World Health Organisation (WHO) guidelines on the Ethics and Governance for Artificial Intelligence (AI) in health, the use of AI in health and medicine are continually expanding. Usable data has flourished specifically in the healthcare sector, being collected from numerous sources, including wearable technologies, genetic information generated by genome sequencing, electronic health-care records, radiological images and hospital rooms. Although the application of AI in Lower to middle income countries (LMICs) may be limited, due to varying factors, including a lack of infrastructure, digital health technologies are already widely used in LMICs for data collection, dissemination of health information by

mobile phones and extended use of electronic medical records on open-software platforms and cloud computing (amongst others). An important area of health research utilising AI is centred around the use of data generated from electronic health records. However, using such data can prove challenging if the underlying information technology system and database do not discourage the production of heterogeneous or low-quality data. Nevertheless, AI can be effectively applied to electronic health records for biomedical research, quality improvement, and the optimization of clinical care. Additionally, AI can assist in analysing clinical practice patterns derived from electronic health records to develop new clinical practice models. The collection, analysis, and use of health data, including from clinical trials, laboratory results, and medical records, are the foundation of medical research and the practice of medicine. However, over the past two decades, what qualifies as health data has expanded dramatically, now including massive quantities of personal data from various sources. Collectively known as "biomedical big data," these various types of data form a health data ecosystem that includes data from standard sources (e.g., health services, public health and research) and further sources (e.g. environmental, lifestyle, socioeconomic, behavioral, and social). Consequently, there are now many more sources of health data, entities that wish to make use of such data, and commercial and non-commercial applications for the data.

In Dinerstein v Google, a case which illustrates litigious challenges related to data-sharing, Dinerstein brought several claims, including breach of contract against the University of Chicago and Google who collaborated to develop software capable of anticipating patients' future healthcare needs. Dinerstein accused the defendants of inadequate anonymisation of health records and placing patient privacy at risk. He alleged that patients could easily be re-identified by Google by combining the records with other available data sets, such as geolocation data from Google Maps (by so-called "data triangulation"). Furthermore, Dinerstein proclaimed that the University had not obtained express consent from each patient to share their medical records with Google, despite the technology giant's commercial interest in the data. The issue of re-identification was largely avoided by the district judge, who dismissed Dinerstein's lawsuit in September 2020. Another recent privacy concern over the misuse of data and data leaks relates to the chatbot, ChatGPT with certain bodies including Samsung initiating bans on its use and others calling for a pause in AI development.

With the encouragement of wide data sharing including through the use of electronic health records, comes the risk of data breaches. As a result, protections and safeguards must be available to prevent (in as far as possible) any threats to data security which could have devastating effects for participants, researchers, institutions and the scientific research space in general. I now turn to discuss data breaches in health care.

The healthcare sector accounts for the highest number of security breaches compared to other industries. Healthcare data is more valuable than any other type of data on the black market because it usually takes longer for healthcare fraud to be discovered. Thus, the data may be used for longer periods compared to data extracted from a stolen credit card for example, which can be stopped immediately when the breach is discovered. Healthcare databases are usually large, making them perfect targets for hackers. The risks associated with data breaches and subsequent informational harms, amplified during the Covid-19 pandemic, where increased hospital visits exposed more patients to security threats. The

pandemic further provided cybercriminals with the opportunity to exploit cybersecurity vulnerabilities and launch cyber-attacks within the healthcare sector. According to IBM Security's annual Cost of Data Breach Report, the average data breach cost for South African organisations reached a record breaking R49.5-million in 2023. In addition, it was found that South African companies had the highest percentage of organisations that had not used security automation that allowed security technologies to enhance or replace human intervention. Furthermore, there are several issues that hospitals face regarding storing, sharing and distributing health records and the most common issues in hospital information systems include: human errors, hackers, missing or stolen paper records, and software errors. A few examples of data breaches in South Africa include those reported by the Life Healthcare Group in 2020, the second largest private hospital operator in South Africa which was hit by a malicious cyber-attack in the midst of the pandemic; and Experian, a consumer, business and credit information services agency which exposed the personal information of as many as 24 million South Africans and over 700 000 business entities.

The Cybercrimes Act 19 of 2020 offers comprehensive regulation in dealing exclusively with cybercrimes and related issues and was signed into law in June 2021. While data protection and cybercrimes are two distinct areas of information communications technology, there is a correlation between these two areas in that the law now has an opportunity to remedy situations of vulnerability. Considering that data has been described as the "new oil" and noting that the commission of crimes across physical borders has become easier, further emphasises the relationship between laws relating to cybercrimes and data protection.

It is imperative that responsible parties have the requisite technical and organizational measures in place to safeguard personal information. The duty to safeguard personal information or data entails cybersecurity measures aimed at identifying internal and external security threats and vulnerabilities.

The regulation of data breaches and penalties associated thereto are contained within POPIA, and further safeguarded under the Cybercrimes Act and in the Electronic Communications and Transactions Act 25 of 2002. The ASSAF COC provides the practicalities on safeguarding personal information in the event of a security compromise. However, the risks associated with breaches in privacy of data are very real and although safeguards and reporting procedures may assist with preventing and managing these risks, the impact of informational harms as a result of data breaches can be severe. Regarding research that involves the extensive networking of samples and data, privacy infringements of personal information may only take place years after the initial research is carried out. Therefore, a robust mechanism which translates the theoretical legal privacy framework into practice, and which aims to safeguard the integrity of participants' data is paramount.

In conclusion, South Africa has made significant strides towards the development of a comprehensive ethico-regulatory framework that aims to protect the privacy and confidentiality of patients and research participants in the healthcare setting. Both the Draft National Open Science Policy and the Draft National Policy on Data and Cloud are data driven, while the protection of personal information under POPIA appears to be suffused with individual autonomy and self-determination, an issue which the ASSAF COC attempts to address. Notably, South Africa is one of the very first countries to have developed a COC for

Research for the protection of personal information. Nevertheless, AI and its advances pose significant challenges that South Africa will need to consider as its privacy protections further evolve. Any tool developed to regulate data flows should be adapted in line with appropriate safeguards that respect the dignity of people considering the pre-democratic South African context.

I would like to thank UNISA for the research opportunities that it provides academics, Professor Motsa Madikane for the welcome, Professor Kole for the introduction, the organising committee, in specific, Mr Ngcobo for handling the logistics and making this lecture possible, the Acting Chair of the Department of Jurisprudence, Dr Siphuma for his support, my dear colleagues from the Department of Jurisprudence, my respondent Professor Labuschaigne, who is not only a colleague but also my mentor, one of the supervisor's to my LLM and PhD and collaborator on various research projects. My husband, for his encouragement, my parents for their unwavering support and for instilling confidence in me to continue my research and handle criticism in a positive manner. My daughter, who shines a light on my path and the Almighty for guiding me forward.

Here are the references I used to prepare my presentation. Thank you, colleagues.