Preserving the Integrity of Medical-Related Information – How "Informed" is Consent?

MN Njotini*

P·E·R

Pioneer in peer-reviewed, open access online law publications

Author

Mzukisi Niven Njotini

Affiliation

University of Johannesburg
South Africa

Email mnjotini@gmail.com

Date of submission

23 October 2017

Date published

3 September 2018

Editor Prof Howard Chitimira

How to cite this article

Njotini MN "Preserving the Integrity of Medical-Related Information – How 'Informed' is Consent?"*PER / PELJ* 2018(21) - DOI http://dx.doi.org/10.17159/1727-3781/2018/v21i0a3400

DOI
http://dx.doi.org/10.17159/1727-3781/2018/v21i0a3400

Abstract

Health care services are recognised as a right. These services are available to "everyone" who needs them. This availability ensures that users, that is, persons who receive treatment in a health establishment or who are in need of health services, are able to have access to these services. Generally, health care services should be available without undue financial burden to users. This then means that the government is saddled with an added financial and administrative burden to ensure their availability to users. However, the availability of the services depends on the availability of resources. In cases where resources are diminished, users who may be in need of health care services may be excluded. Furthermore, the availability of access to health care services does not sufficiently guarantee the securing of users' personal information. Thus, it is enquired what levels of safeguards do health establishments have to secure the personal information of users? Do these security mechanisms allow for the disclosure of personal information to third parties, and how?

Keywords

Personal information; processing; autonomy; security; critical databases.

.....

1 Introduction

South Africa has come a long a way in recognising the need to preserve the integrity of medical-related information.[1] This recognition necessitates a study of the existing information security mechanisms that health establishments adopt.[2] It demands a scrutiny of the extent to which this information can be used and depended upon in a manner that still maintains its quality and purpose. Before the *Constitution*[3] came into effect, South African courts applied the "reasonable doctor test" in order to establish whether or not a reasonable attempt had been made to ensure the security of the medical-related information.[4] This is evident *inter alia* in the case of *Van Wyk v Lewis*.[5] In terms of the reasonable doctor test, the inquiry was made whether or not a reasonable doctor would have divulged a particular piece of information relating to a user.[6] However, the reasonable doctor test was rejected by the court in the case of *Castell v De Greef*[7] and subsequently in the case of *Oldwage v Louwrens*.[8] The aforementioned cases promoted a shift from the doctor-centred approach to a patient-centred approach in preserving the quality of medical-related information.[9] Specifically, the Castell case developed the doctrine of "informed consent". This doctrine accords with the South African human rights culture insofar as

* Mzukisi Niven Njotini. LLB LLM LLD Cert Labour Dispute Resolution Practice. Professor, Department of Private Law, University of Johannesburg, South Africa. Email: mnjotini@gmail.com.

1 IoDSA 2009 https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/king_iii/King_Report_on_Governance_fo.pdf defines the term "information" as the "raw data that has been verified to be accurate and timely, is specific and organised for a purpose, is presented within a context that gives it meaning and relevance and which leads to increase in understanding and decrease in uncertainty".

2 In terms of s 1 of the *National Health Act* 61 of 2003, a health establishment refers to the "whole or part of a public or private institution, facility, building or place, whether for profit or not, that is operated or designed to provide inpatient or outpatient treatment, diagnostic or therapeutic interventions, nursing, rehabilitative, palliative, convalescent, preventative or other health services".

3 *Constitution of the Republic of South Africa*, 1996 (hereinafter referred to the *Constitution*).

4 See *Richter v Estate Hamman* 1976 3 SA 408 (C).

5 In *Van Wyk v Lewis* 1924 AD 438 (hereinafter referred to as the *Van Wyk* case) the court stated that "in deciding what is reasonable the Court will have regard to the general level of skill and diligence possessed and exercised at the time by the members of the branch of the profession to which the practitioner belongs".

6 Claassen and Verschoor *Medical Negligence* 15; Van Oosten 1995 *De Jure* 170. In terms of s 1 of the *National Health Act* 61 of 2003 a user means refers to the "person receiving treatment in a health establishment, including receiving blood or blood products, or using a health service".

7 *Castell v De Greef* 1994 4 SA 408 (C) (hereinafter referred to as the *Castell* case).

8 *Oldwage v Louwrens* 2004 1 All SA 532 (C).

9 Thomas 2007 *SALJ* 190.

it enjoins a strict adherence to specific consumer prescripts that are commonly observed in contemporary societies.[10]

As elaborate as the law relating to informed consent is, it still fails to cover the nature and extent of the security needed to safeguard medical-related information. Simply, the question is: how informed is consent?[11] In examining this question, this paper is divided into four sections. Section 1 scrutinises the meaning and essence of informed consent. It uses as the basis of its enquiry some of the provisions of the *National Health Act*. However, the discussion of informed consent does not seek to re-invent the wheel. Furthermore, it does not imply that a new description of informed consent is necessary. Simply, it aims to localise the nature and ambit of informed consent in an attempt to establish or re-establish the integrity or credibility of medical records in South Africa. The second section investigates issues relating to the manner of handling and safeguarding the information of users. The approaches to guaranteeing the inviolability of information followed *inter alia* in the *Protection of Personal Information Act* are scrutinised. The third section delves into the way forward for South Africa in preserving the security of information kept or stored by health establishments. This section discusses the idea of establishing critical information infrastructures. The fourth section of this paper is the conclusion. In this section, the facts presented in this paper are summarised and a legal framework to preserve the credibility of sensitive information stored by health establishments is presented.

2 Informed consent

2.1 Background

In general, the term "informed consent" is based on the common law doctrine: *volenti non fit iniuria*.[12] Simply, this doctrine denotes that "to a willing person, injury is not done".[13] Within the context of South Africa, informed consent is a right. Initially, this right was accepted by the court in the case of *Stoffberg v Elliot* as an absolute right which the law protects.[14] Because of this, certain requirements must be met before the right to

10 *Castell* case 423H-I. Within the context of South Africa, these consumer prescripts are dealt with in terms of the *Consumer Protection Act* 68 of 2008. These have to do *inter alia* with a duty to inform patients of any indemnity clause in circumstances where such a clause excludes liability for a conduct that is likely to cause harm or injury. See s 49(2)(c) of the *Consumer Protection Act*.

11 For an interesting reading on what other legal questions researchers could explore see Slabbert 2009 *Obiter*.

12 See *Christian Lawyers Association v Minister of Health (Reproductive Health Alliance as Amicus Curiae)* 2005 1 SA 509 (T).

13 Jackson *Medical Law* 134-135.

14 *Stoffberg v Elliot* 1923 CPD 148 148.

informed consent can be said to exist. Firstly, the user must have knowledge or must be aware of the harm or risk.[15] Secondly, he or she must appreciate and understand the nature and extent of the harm or risk.[16] Thirdly, he or she must consent to the harm or risk. That is, the user must assume the harm or risk.[17] Fourthly, the consent given must be intelligible. In other words, it must cover every aspect of the harm or risk.[18]

In South Africa the right to informed consent is recognised in section 12(2) of the *Constitution*. This sub-section states that:

> Everyone has the right to bodily and psychological integrity, which includes the right to make decisions concerning reproduction; to security in and control over their body; and not to be subjected to medical or scientific experiments without their informed consent.

"Security in" and "control over" have a particular meaning for the purposes of section 12(2) of the *Constitution*. The former relates to the "protection of bodily integrity against intrusions by the state and others"[19] and the latter has to do with the "protection of what could be called bodily autonomy or self-determination against interference".[20]

Therefore, the meaning of the right to informed consent in terms of section 12(2) of the *Constitution* extends beyond what is normally referred to as consent. Specifically, it has to do with the practices that describe what is right and wrong,[21] which can be established by examining the degree of skill and care that is reasonably applied in a particular circumstance.[22] Furthermore, it guarantees the patient's autonomous right to decide. It does this by promoting the notion that a peculiar ideal of the person is the substance of his or her ethical or moral edifice.[23]

It is worth mentioning that the foundation of an autonomous decision is *inter alia* that:

> …. moral debate about a particular course of action or controversy is often rooted not only in disagreement about the proper interpretation of applicable moral principles, but also in the interpretation of factual information and in

15 *Castell* case 425H-I.
16 *Castell* case 425H-I.
17 *Castell* case 425H-I.
18 *Castell* case 425H-I.
19 Currie and De Waal *Bill of Rights Handbook* 287.
20 Currie and De Waal *Bill of Rights Handbook* 287.
21 Faden, Beauchamp and King *Informed Consent* 4-5.
22 *Van Wyk* case 444; *Mitchell v Dixon* 1914 AD 519 525.
23 See in general, Rawls 1980 *Journal of Philosophy*. Also see Downie and Telfer 1971 *Journal of Philosophy* 301; Chima 2013 *BMC Medical Ethics* 1.

> divergent assessments of the proper scientific, metaphysical, or religious description of a situation.[24]

In this context manner, autonomy implies a responsibility to accept the consequences of one's decision. Consequently, a decision to consent is autonomous if it is given or furnished independently and voluntarily. In other words, it must exist consequent to information being given that influenced a user to make such a decision.[25] This voluntariness accords with the principle that an autonomous user is generally self-governing.[26] In other words, telling a user to act in a particular way or take a particular decision does not prevent a person from exercising autonomy in granting or refusing consent. However, if a decision is taken after the person has been told or commanded to act in a particular way or take a particular decision, this negates informed consent. An example of this is to be found in the case of *Moore v Regents of the University of California*.[27] Moore, who was a patient at the time, had his spleen taken out or removed from his body with the aim of treating leukaemia. Samples of blood, bone marrow and other tissues were subsequently extracted from his body. He was then told by the hospital to amend his admission form to read that he consented to research being undertaken using the parts removed from his body. He duly amended the form as commanded. It was established later that Moore's physician and his assistant had created the Mo-cell line using the samples taken from Moore. Thereafter, they patented the line and made profit in a sum estimated at 3 billion US Dollars. It could be asked if Moore had also given his informed consent to the creation of the Mo-cell line. In other words, is it legally justified to extend the informed consent given for the removal of a spleen to then create a profitable business? In South Africa, the issue relating to a change or altering of a statement of informed consent is dealt with in the *Consumer Protection Act*.[28] In terms of this Act, the change must relate only to the indemnity clause in the admission form that intends to exclude liability resulting from an activity that could lead to the serious injury or death of a

---

24 See Faden, Beauchamp and King *Informed Consent* 4.

25 *Castell* case 426-427. For example, in the case of *Rogers v Whitaker* 1993 67 ALJR 47 52, the court stated that: "The law should recognise that a doctor has a duty to warn a patient of a material risk inherent in the proposed treatment; a risk is material if, in the circumstances of the particular case, a reasonable person in the patient's position, if warned of the risk, would be likely to attach significance to it or if the medical practitioner is or should reasonably be aware that the particular patient, if warned of the risk, would be likely to attach significance to it. This duty is subject to the therapeutic privilege".

26 Badhwar *Worthwhile Life* 83.

27 See *Moore v Regents of the University of California* 51 Cal 3d 120 (1990). Also see Snyman *Criminal Law* 126-127.

28 *Consumer Protection Act* 68 of 2008.

user.[29] Specifically, section 49(2)(c) of the *Consumer Protection Act* places a duty on health establishments to inform users of an indemnity clause that purports to exclude such liability. Accordingly, the provisions of section 49(2)(c) of the *Consumer Protection Act* remedy the position of the law which existed since the case of *Afrox Healthcare Bpk v Strydom,*[30] which was that there was no duty to inform users of an indemnity clause.

Nevertheless, the cardinal view is that the fact that the command to act in a particular manner comes from the government or is based on a "promise to abide by the will of the majority" does not really matter.[31] The principle that "I am autonomous if I rule myself and no one else rules me" applies.[32] This implies that the carrying out of the command must be justified in terms of section 36 of the *Constitution*. In other words, there must be a law of general application authorising the infringement of the rights in terms of section 12(2) of the *Constitution*.[33] An example of this relates to cases of non-trivial intrusions on bodily integrity with the aim of investigating and preventing wrongdoing.

In practice, there are various ways in which the requirement of informed consent is typically circumvented. The so-called *Havasupai case*[34] is but one such circumstance. In this case the plaintiff was the Havasupai tribe of the Havasupai Indian Reservation. The tribe consists of members who live in the Supai Village on the outskirts of the Grand Canyon. In 1989 an anthropology professor of Arizona State University conducted research on the tribe. The research examined the epidemic of diabetes among the tribal members. A diabetes-focussed project was then established in order to facilitate the intended research. This culminated in blood samples being drawn from more than 200 members of the tribe, who individually and independently furnished Arizona State University with their informed consent. Following this, the blood samples were stored and kept in laboratories held at Arizona State University. However, it transpired that the aforesaid University had carried out research or allowed others to carry out research unrelated[35] to diabetes using the blood samples drawn from the Havasupai tribe. Specifically, the unrelated research was in relation to schizophrenia, migration and inbreeding.

---

29 It is important to note that this exclusion does not include cases of "gross negligence" by health establishments. See s 51(c)(i) of the *Consumer Protection Act*.

30 See *Afrox Healthcare Bpk v Strydom* 2002 4 All SA 125 (SCA).

31 Wolff *Anarchism* 41; Dworkin "Liberalism" 127.

32 Feinberg *Social Philosophy* 21.

33 See *Minister of Safety and Security v Xaba* 2004 1 SACR 149 (D); Tribe *American Constitutional Law* 1330.

34 *Havasupai Tribe of the Havasupai Reservation v. Arizona Board of Regents* Nos 1 CA-CV 07-0454, 1 CA-CV 07-0801 2008.

35 Hereinafter referred to as the "unrelated research".

Therefore, the question to be asked is whether the informed consent of the members of the Havasupai tribe was necessary in these circumstances. Put differently, should Arizona State University have obtained the informed consent of the members of the Havasupai tribe before it conducted the unrelated research using the blood samples? Having failed to do so, what impact does the carrying out of this unrelated research have on the credibility of the research findings by Arizona State University? A spontaneous reader of ordinary prudence may find it possible to respond adequately to these questions. However, there is still legal uncertainty and indecision in relation to the processing[36] and the manner of the handling and processing of the information arising from this unauthorised research.

The section below investigates the essence of informed consent in the context of the *National Health Act.* It is argued that informed consent is pivotal in ensuring that medical-related information is handled and dealt with in terms of the law.

2.2 The National Health Act

Informed consent, as a notion, is not defined in the *National Health Act*. Simply, this Act provides that the informed consent of a user is required in cases where *inter alia* certain information is provided and a user makes or participates in taking particular decisions. On the one hand, section 6 of the *National Health Act* enjoins health establishments to inform a user, in a language which he or she understands,[37] about his or her health status, the diagnosis procedures, the treatment options that are available to him or her, and the benefits, risks, costs and consequences connected with each of the options.[38] Thereafter, a user must be informed of the right to refuse the services and the implications, risks and obligations of this refusal.[39] Consequently, health establishments should have due and special regard to the level of literacy of a user when communicating this information.[40] On

---

36 In this paper, the definition of the word "processing" contained in s 1 of the *Protection of Personal Information Act* 4 of 2013 (hereinafter referred to as the *POPI Act*) is preferred. In terms of this section processing means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

(a) the collection, receipt, recording, organisation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

37 Section 6(2) of the *National Health Act*.

38 Section 6(1)(a)-(d) of the *National Health Act*.

39 Section 6(1)(a)-(d) of the *National Health Act*.

40 Section 6(2) of the *National Health Act*. Also see *Issacs v Pandie* 2012 ZAWCHC 47 (16 May 2012).

the other hand, section 8 of the *National Health Act* regulates situations where informed consent is mandatory in order for a user to make or participate in taking certain decisions. These include circumstances in which the decision relates to the personal health or treatment of a user.[41]

Given the inability of the *National Health Act* to provide meaning to the term informed consent, it is then imperative to examine sources external to the latter Act. One such source is the Health Professions Council of South Africa's (HPCSA) Guidelines for Good Practice in the Health Care Professions, 2008.[42] The HPCSA Guidelines, 2008 states the following:

> Successful relationships between health care practitioners and patients depend upon mutual trust. To establish that trust practitioners must respect patients' autonomy – their right to decide whether or not to undergo any medical intervention, even where a refusal may result in harm to themselves or in their own death. Patients must be given sufficient information in a way that they can understand, to enable them to exercise their right to make informed decisions about their care. This is what is meant by an informed consent.[43]

This states that informed consent is not only a casual arrangement between health establishments and their clients. Importantly, it is a *sine qua non* for the existence of a relationship of trust between health establishments their clients. In this respect, the provisions of section 1 of the *POPI Act* apply. This section enumerates factors to determine whether informed consent is required in a particular case. Firstly, it states that consent is informed if it is made voluntarily by a user.[44] Secondly, it provides that the requisite consent must be specific or must have been made in unambiguous terms.[45] In other words, it must amount to an informed expression of the will of a user.[46] Therefore, before consent can be said to be informed, it has to illustrate the ability of a user to deliberate on a particular decision affecting his or her personal health. This view seems to be followed by Andanda, amongst others.[47] Andanda explains the essence of informed consent by stating that the required consent must amount to a collective declaration by both the health establishments and their users.[48]

---

41 Section 8(1) of the *National Health Act*.
42 Hereinafter referred to as the HPCSA *Guidelines, 2008*.
43 The HPCSA *Guidelines, 2008* 1.
44 Section 1 of the *POPI Act*. It is important to note that circumstances may arise wherein a user may not be able to give the necessary consent. In such cases, any person who is mandated by a user in writing to grant consent on his or her behalf or is authorised to give such consent in terms of any law or court order may be allowed to give the consent. See s 7(1)(a) and (b) of the Act.
45 Section 1 of the *POPI Act*.
46 Section 1 of the *POPI Act*.
47 Andanda 2005 *Dev World Bioeth* 16.
48 Andanda 2005 *Dev World Bioeth* 14.

As simple as the narrative explained above may be, it still does not elucidate situations where consent is required in relation to the processing of clients' information. Let us suppose that in the Havasupai case the issue related to the research project was based on the information, and not the actual blood samples, of the Havasupai tribe. In other words, Arizona State University drew blood samples from the members of the Havasupai tribe, stored the blood samples and on its online computers recorded the information relating to the fact, for example, that some members of the tribe are prone to diabetes and others are not. Some of the questions to ask would be:

- What legal limits exist or should exist to regulate the proper handling and processing of this information?
- Specifically, is the informed consent of the Havasupai tribe necessary before the information relating to the blood samples is handled and dealt with?
- Does this handling and processing become immaterial given that the information is stored online?

It has been stated already that informed consent depends on the presence of certain requirements. These have to do with the fact that a user must be aware of, appreciate, understand and consent to a particular harm or risk.[49] In terms of the *Consumer Protection Act*, this informed consent is absent in cases where there is gross negligence on the part of a health establishment. In view of this, the section below delves into the manner of handling and processing users' medical-related information.[50] It also examines certain

49 See the *Castell* case 425H-I.

50 See s 1 of the *POPI Act*. In terms of the latter section, personal information means information about an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to – "(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; € the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would the contents of the original correspondence; (g) the view or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person." See also s 1 of the *Promotion of Access to Information Act* 2 of 2000.

related provisions for processing personal information in terms of the *POPI Act*.

3 The POPI Act

3.1 General overview

The *POPI Act* came about because of the need to respond to advances in information and communication technology.[51] The developments have expanded the extent to which personal information can be accessed and used. With these advances it became evident that personal information requires protection.[52] Weisbrot elucidates the impact that these ICTs have by stating that:

> Recent advances in information, communication and surveillance technologies have created and intensified a range of privacy issues. The internet, biometrics, digital phones and cameras, powerful computers and radio-frequency identification have all contributed to making it easier, cheaper and faster for government agencies and business organizations to collect, store and aggregate large amounts of personal and sensitive information.[53]

Given the emergence of these technologies, South Africa promulgated the *POPI Act* in order to give effect to section 14 of the *Constitution*. The Act provides measures to protect the processing of personal information.[54] It does this by creating conditions under which personal information may be processed lawfully.[55] Furthermore, it saddles responsible parties with a duty to process personal information belonging to "data subjects".[56] Responsible parties can be public or private bodies which or any person who determines the purpose of or means for processing personal information.[57] Within the context of this paper, these responsible parties have the same powers of handling and processing personal information as have health establishments.

Understandably, the collection of personal information precedes the actual processing thereof. In other words, the first step is to collect personal

---

51 Hereinafter referred to as "ICTs".

52 Article 8(1) of the *Charter of Fundamental Rights of the European Union* (2000).

53 Weisbrot 2008 https://www.alrc.gov.au/news-media/2008/media-briefing-technology-neutral-privacy-principles-should-govern-rapidly-developin. Also see Holtzman *Privacy Lost* 5-14.

54 Section 2(a) of the *POPI Act*.

55 Section 2(b) of the *POPI Act*.

56 Data subject is the term used in s 1 of the *POPI Act* to describe the person to whom personal information relates. It is argued that the term shares particular characteristics with the word "user" described above. For the sake of completeness, the word "user" is preferred in this paper. Thus, reference to a user shall, within the context of this paper, also refer to a data subject, or *vice versa*.

57 Section 1 of the *POPI Act*.

information from users, and whereafter it is possible to commence with the processing.[58] Specifically, the Organisation for Economic Co-operation and Development (OECD) states that the reason for collecting personal information should be specified not later than at the time of collection.[59] Because personal information is collected for a particular purpose,[60] such a purpose must be specific, defined explicitly and be made by lawful and fair means.[61] This means that a user must be informed of the purposes for which the collection is made.[62] This communication can be in the form envisaged in section 18(1) of the *POPI Act*. However, the requirement of collecting personal information by these means can be waived by adhering to the conditions set out in section 18(4) of the *POPI Act*. These conditions are dealt with the section (Processing Procedure) below.

3.2 Processing procedure

Chapter 3 of the *POPI Act* deals with the conditions under which personal information may be processed. These conditions are not discretionary as such. Instead, responsible parties have a duty to ensure that the conditions and the measures that give effect to these conditions are complied with.[63] Condition 2 of Chapter 3 of the *POPI Act* covers issues relating to the lawful processing of personal information. The aforesaid Condition states that personal information must be processed lawfully and in a reasonable manner.[64] The OECD seems to accept this manner of processing personal information.[65] However, the OECD prefers the term "fair means" of processing.[66] The preference for the fair processing of personal information does not necessarily render the approach that South Africa adopts to processing personal information insignificant. This is so, because the notion of fairness is said to be "part and parcel of the concept of lawfulness".[67] Therefore, lawfulness, reasonableness and fairness require that grounds should exist that justify the processing. In South Africa, the accepted grounds of justification are private defence, necessity and consent.[68]

---

58 See s 14(1)(a) of the *POPI Act*.

59 See OECD 2013 https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (hereinafter referred to as the OECD Guidelines".

60 See Condition 3 (Purpose Specification) of Chapter 3 of the *POPI Act*.

61 Section 13(1) of the *POPI Act*; Recommendation 7 of the OECD Guidelines.

62 Section 13(2) of the *POPI Act*.

63 Section 8 of the *POPI Act*.

64 Section 9(a) and (b) of the *POPI Act*.

65 See OECD 2013 https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

66 Recommendation 7 of the OECD Guidelines. Also see art 8(2) of the *Charter of Fundamental Rights of the European Union* (2000).

67 Roos 2006 *CILSA* 105-111.

68 Snyman *Criminal Law* 103-129.

A lawful, reasonable or fair means of processing personal information should foster a processing framework that safeguards the privacy of a user.[69] Specifically, the framework has to have measures to preserve the integrity, confidentiality and authenticity of personal information.[70] Simply, the measures must prevent any loss of, damage to or unauthorised destruction of personal information.[71] Furthermore, they must deter the unlawful accessing or processing of personal information.[72] In doing so, responsible parties must identify all reasonably foreseeable internal and external risks - such as risks to privacy and identity[73] - to personal information in their possession or under their control.[74] They must also establish and maintain appropriate safeguards against the risks identified.[75] Furthermore, they must regularly verify that the safeguards are effectively implemented.[76] Lastly, they must guarantee that the safeguards are continually updated in response to the new risks or deficiencies in previously implemented safeguards.[77]

Lastly, the fundamental principle of our law seems to be that personal information must be processed with the requisite consent.[78] Specifically, a user, or his or her guardian, must provide the necessary consent to the processing.[79] The consent to the processing of information follows the collection process. However, there are circumstances wherein the informed consent of a user may not be mandatory. For example, the consent is not necessarily required in cases where the processing is desirable in order to carry out, conclude or perform actions in terms of an agreement to which the data subject is a party.[80] Secondly, the consent is not necessary in situations where the processing is done in compliance with an obligation imposed by law.[81] Thirdly, it is not mandatory to obtain consent in circumstances where the processing is designed to protect the legitimate interests of a user.[82] Fourthly, consent may not be sought if the processing

69 Section 9(b) of the *POPI Act*; Bennett *Regulating Privacy* 23; Da Veiga and Martins 2015 *CLSR* 246.

70 ISO 2013 http://mahdi.hashemitabar.com/cms/images/Download/ISO/iso-iec-27002-2013-english.pdf.

71 Section 19(1)(a) of the *POPI Act*. Also see Recommendation 11 of OECD Guidelines.

72 Section 19(1)(b) of the *POPI Act*.

73 Roos 2006 *CILSA* 105-107.

74 Section 19(2)(a) of the *POPI Act*.

75 Section 19(2)(b) of the *POPI Act*.

76 Section 19(2)(c) of the *POPI Act*.

77 Section 19(2)(d) of the *POPI Act*.

78 Section 11(1)(a) of the *POPI Act*.

79 Section 11(1)(a) of the *POPI Act*.

80 Section 11(1)(b) of the *POPI Act*.

81 Section 11(1)(c) of the *POPI Act*. For further reading see Recommendation 10 of the OECD Guidelines.

82 Section 11(1)(d) of the *POPI Act*.

is needed for the proper performance of a public law duty by a public body.[83] Fifthly, consent is not needed where the processing is essential for following the legitimate interests of the responsible party or of a third party to whom the personal information is supplied.[84]

In summary, informed consent presupposes a formal knowledge or awareness of the harm or risk to a user. Specifically, the consent must be such that it enables a user to make an informed decision about the harm or risk that could result *inter alia* in serious bodily injury or death. Accordingly, health establishments have a duty to inform and users have a corresponding responsibility to take informed decisions. The duty to inform and to be informed does not relate only to the actual harm or injury as such. It also pertains to the manner of collecting and processing medical-related information that is crucial to the responsibility to take informed decisions. This collection and processing of information is regulated by the *POPI Act*, which deals with the fair, reasonable, justifiable and lawful manner of processing medical-related information. It also regulates situations where the informed consent of a user may not be required.

The section below covers the way forward for South Africa in preserving the integrity of medical-related information. It is argued that information infrastructures are the possible solutions for keeping records of users and monitoring the processing of information online. These infrastructures could be in the form of online databases and could be kept and monitored by heath establishments.

4 Way forward to preserve the integrity of medical-related information

Generally, health establishments are required to process the personal information of users in a lawful and reasonable manner. In other words, they should adopt fair means of processing personal information. Fair means could include those mechanisms or grounds that provide reasonable justifications for the processing. Within the context of this paper, these grounds of justification include cases where specific information is provided and a user takes or participates in taking certain decisions.[85] In this respect, the informed consent of users should validate the processing.[86] The consent must be made voluntarily by users. Conversely, it must constitute an

83 Section 11(1)(e) of the *POPI Act*; *S v Bailey* 1981 4 SA 187 (N).
84 Section 11(1)(f) of the *POPI Act*.
85 See s 6 read with s 8 of the *National Health Act*.
86 For the exceptions to the requirement of informed consent in processing personal information, see s 11(a)-(f) of the *POPI Act*.

autonomous choice to accept the processing of his or her personal information.

Because personal information is fundamental to a user, processes associated with preserving the integrity, confidentiality and authenticity of such information are essential. These processes relate not only to the information *per se*, but they also have an impact on the security of the place where and the manner in which the information is stored. Thus, is it still necessary to disregard recent developments in ICTs by having records containing personal information of users in physical files kept in offline storerooms? Answering this question will require one to undertake a complete study of the information security mechanisms available to South Africa. One example of such measures relates to the establishment of critical databases. A critical database is a collection of critical data in electronic form from which it may be accessed, reproduced or extracted.[87] In turn, critical data is data[88] that is declared by the Minister[89] in terms of section 53 to be essential to the protection of the national security of the Republic or the economic and social well-being of its citizens.[90]

Chapter IX of the *Electronic Communications and Transactions Act* provides a framework for the establishment of critical databases. Basically, the Minister identifies critical data and databases.[91] The Minister does this by deciding which information should be identified as fundamental to the protection of the national security of South Africa.[92] Consequently, he or she has extensive powers to categorise information according to the importance that it has to the security and protection of the economic and social wellbeing of South African citizens.[93] As soon as it is identified, the Minister creates provisions for the registration of critical databases.[94] This could be in the form of rules that provide for the registration of the full names, addresses and contact details of the critical database administrator;[95] the location of the critical data and database or their component parts, and a

87 Section 1 of the *Electronic Communications and Transactions Act* 25 of 2002 (hereinafter referred to as the *ECT Act*).

88 In terms of s 1 of the *ECT Act* the term data refers to the electronic representation of information in any form.

89 Within the context of the *ECT Act*, Minister refers to the Minister of Communications. See s 1 of the *ECT Act*.

90 Section 1 of the *ECT Act*.

91 Section 53 of the *ECT Act*.

92 Section 53(a) of the *ECT Act*.

93 Section 53(a) of the *ECT Act*.

94 Section 54 of the *ECT Act*.

95 A critical database administrator is the person who is responsible for the management and control of a critical databases. See s 1 of the *ECT Act*.

general description of the information stored in the critical database.[96] Subsequently, a critical database administrator may be appointed in order to manage, control and administer the operation of a critical database.[97]

The rationale for establishing critical databases is to guarantee that medical-related information is protected from the risk of loss, damage and unauthorised destruction. Because of this, specific rules should be established that stipulate the manner of accessing, transferring and controlling critical databases; the infrastructural and procedural rules and requirements for securing the reliability of critical databases, and the measures and technological methods to be used in storing and archiving critical databases.[98] In addition, the rules ought to set out specific disaster recovery plans in cases where the loss, damage or destruction of medical-related information occurs.[99]

5 Conclusion

South Africa recognises the need to preserve the confidentiality of medical-related information. Initially, a doctor-centred approach was preferred, which referenced what a reasonable doctor would do when in possession of the information. Nowadays, a patient-centred approach is followed. This approach promotes the idea that the ability to make an informed decision regarding a potential harm depends on the strength of the information given by health establishments. In other words, the more users are informed, the more likely they are to make informed decisions. However, it is evidenced that the extent of the informed consent has not yet been examined. In other words, the pre-occupation has always been on the fact that users must furnish health establishments with their informed consent, but the question relating to the nature and degree of the informed has been left unanswered.

Generally, it is argued that a certain amount of due diligence has to be applied to guarantee that the integrity of medical-related information is maintained. Simply, users must be assured that their medical-related information will be used for the purpose for which it was collected. This can be achieved by ensuring that health establishments process this information in a lawful and reasonable manner. Fair means ought generally to be used in order to effect the processing. These relate to preventing the loss of, damage to or unauthorised destruction of information. Specifically, the means used in processing information must be aimed at promoting its

96 Section 54(2)(a)-(c) of the *ECT Act*. The recording of these particulars may, however, be waived at the Minister's discretion in terms of s 55(2)(a) and (b) of the *ECT Act*.

97 Section 1 of the *ECT Act.*

98 Section 55(1) of the *ECT Act*.

99 Section 55(1)(e)) of the *ECT Act*. For further reading on the powers of the Minister, see generally s 55(2) of the *ECT Act*.

integrity, confidentiality and authenticity. For the processing to be carried out, the informed consent of users is essential. This consent must be given voluntarily by users. Specifically, it must be the autonomous expression of the users' will or decision. Furthermore, the consent has to be given in a language that users understand and are able to speak. Generally, the degree of the informed consent should not be limited only to the likelihood of harm or risk. It ought to be extended to the medical-related information that brings about the need to give the necessary consent. This then enjoins health establishment to have regard to the manner in which this information is collected and processed.

In this paper, establishing critical databases is said to be pivotal in preserving the integrity of medical-related information. Such databases would ensure that the information is processed only by those who have the necessary authority to do so. This authority will be determined by factors regarding, amongst others, whether users consented to the processing, if the processing is necessary in terms of the law, or if the processing is required in order to abide by an order made by the court. To ensure their functionality, critical databases have to be controlled and managed by administrators situated in health establishments. Therefore, health establishment will have to generate rules regulating how to access and control critical databases, how to preserve the credibility of critical databases, and how to record, store and archive medical-related information that is stored in these databases. Furthermore, the rules should illustrate the disaster recovery plans in cases where there is the risk of the loss of, damage to or the destruction of this information.

Bibliography

Literature

Andanda 2005 *Dev World Bioeth*
Andanda P "Module Two – Informed Consent" 2005 *Dev World Bioeth* 14-29

Badhwar *Worthwhile Life*
Badhwar NK *Well-Being: Happiness in a Worthwhile Life* (Oxford University Press Oxford 2014)

Bennett *Regulating Privacy*
Bennett CJ *Regulating Privacy: Data Protection and Policy in Europe and the United States* (Cornell University Press New York 1992)

Chima 2013 *BMC Medical Ethics*
Chima SC "Evaluating the Quality of Informed Consent and Contemporary Clinical Practices by Medical Doctors in South Africa: An Empirical Study" 2013 BMC *Medical Ethics* 1-17

Claassen and Verschoor *Medical Negligence*
Claassen NJB and Verschoor T *Medical Negligence in South Africa* (Digma Pretoria 1992)

Currie and De Waal *Bill of Rights Handbook*
Currie I and De Waal J *The Bill of Rights Handbook* (Juta Cape Town 2016)

Da Veiga and Martins 2015 *CLSR*
Da Veiga A and Martins N "Information Security Culture and Information Protection Culture: A Validated Assessment Instrument" 2015 *CLSR* 243-256

Downie and Telfer 1971 *Journal of Philosophy*
Downie RS and Telfer E "Autonomy" 1971 *Journal of Philosophy* 293-301

Dworkin "Liberalism"
Dworkin R "Liberalism" in Hampshire S (ed) *Public and Private Morality* (Cambridge University Press Cambridge 1978) 113-130

Faden, Beauchamp and King *Informed Consent*
Faden RR, Beauchamp TL and King NM *A History and Theory of Informed Consent* (Oxford University Press Oxford 1986)

Feinberg *Social Philosophy*
Feinberg J *Rights, Justice, and the Bounds of Liberty: Essays in Social Philosophy* (Princeton University Press New Jersey 1980)

Holtzman *Privacy Lost*
Holtzman DH *Privacy Lost: How Technology is Endangering Your Privacy* (Jossey-Bass San Francisco 2006)

HPCSA *Guidelines, 2008*
Health Professions Council of South Africa *Guidelines for Good Practice in the Health Care Professions, 2008* (HPCSA Pretoria 2008)

Jackson *Medical Law*
Jackson E *Medical Law: Texts, Cases and Materials* (Oxford University Press Oxford 2013)

Rawls 1980 *Journal of Philosophy*
Rawls J "Construction and Objectivity" 1980 *Journal of Philosophy* 554-572

Roos 2006 *CILSA*
Roos A "Core Principles of Data Protection Law" 2006 CILSA 103-130

Slabbert 2009 *Obiter*
Slabbert M "This is My Kidney, I Can Do what I Want With it – Property Rights and Ownership of Human Organs" 2009 *Obiter* 499-517

Snyman *Criminal Law*
Snyman CR *Criminal Law* (LexisNexis Durban 2008)

Thomas 2007 *SALJ*
Thomas R "Where to from Castell v De Greef? Lessons from Recent Developments in South Africa and Abroad regarding Consent to Treatment and the Standard of Disclosure" 2007 *SALJ* 188-215

Tribe *American Constitutional Law*
Tribe LH *American Constitutional Law* (Foundation Press New York 2000)

Van Oosten 1995 *De Jure*
Van Oosten FFW "*Castell v De Greef* and the Doctrine of Informed Consent: Medical Paternalism Ousted in Favour of Patient Autonomy" 1995 *De Jure* 164-179

Wolff *Anarchism*
Wolff RP *In Defence of Anarchism* (University of California Press Berkeley 1970)

Case law

Afrox Healthcare Bpk v Strydom 2002 4 All SA 125 (SCA)

Castell v De Greef 1994 4 SA 408 (C)

Christian Lawyers Association v Minister of Health (Reproductive Health Alliance as Amicus Curiae) 2005 1 SA 509 (T)

Havasupai Tribe of the Havasupai Reservation v. Arizona Board of Regents Nos 1 CA-CV 07-0454, 1 CA-CV 07-0801 2008

Issacs v Pandie 2012 ZAWCHC 47 (16 May 2012)

Minister of Safety and Security v Xaba 2004 1 SACR 149 (D)

Mitchell v Dixon 1914 AD 519

Moore v Regents of the University of California 51 Cal 3d 120 (1990)

Oldwage v Louwrens 2004 1 All SA 532 (C)

Richter v Estate Hamman 1976 3 SA 408 (C)

Rogers v Whitaker 1993 67 ALJR 47

S v Bailey 1981 4 SA 187 (N)

Stoffberg v Elliot 1923 CPD 148

Van Wyk v Lewis 1924 AD 438

Legislation

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Electronic Communications and Transactions Act 25 of 2002

National Health Act 61 of 2003

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

International instruments

Charter of Fundamental Rights of the European Union (2000)

Internet sources

IoDSA 2009 https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/king_iii/King_Report_on_Governance_fo.pdf
Institute of Directors Southern Africa 2009 *King III Report* https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/king_iii/King_Report_on_Governance_fo.pdf accessed 3 June 2018

ISO 2013 http://mahdi.hashemitabar.com/cms/images/Download/ISO/iso-iec-27002-2013-english.pdf
International Standards Organisation 2013 *ISO/IEC 27002* http://mahdi.hashemitabar.com/cms/images/Download/ISO/iso-iec-27002-2013-english.pdf accessed 3 June 2018

OECD 2013 https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Organisation for Economic Co-Operation and Development 2013 *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf accessed 3 June 2018

Weisbrot 2008 https://www.alrc.gov.au/news-media/2008/media-briefing-technology-neutral-privacy-principles-should-govern-rapidly-developin
Weisbrot D 2008 *Technology-Neutral Privacy Principles Should Govern Rapidly Developing ICT* https://www.alrc.gov.au/news-media/2008/media-briefing-technology-neutral-privacy-principles-should-govern-rapidly-developin accessed 3 June 2018

List of Abbreviations

CILSA	Comparative and International Law Journal of Southern Africa
CLSR	Computer Law and Security Review
Dev World Bioeth	Developing World Bioethics
HPCSA	Health Professions Council of South Africa
IoDSA	Institute of Directors Southern Africa
ISO	International Standards Organisation
OECD	Organisation for Economic Co-Operation and Development
SALJ	South African Law Journal