National Health Insurance and the Regulation of Electronic Health Records in South Africa: A Primer and Call for Clarification

L Prinsen*

Online ISSN
1727-3781

P·E·R
Pioneer in peer-reviewed, open access online law publications

Author

Larisse Prinsen

Affiliation

University of the Free State, South Africa

Email

prinsenl@ufs.ac.za

Date Submitted

03 February 2025

Date Revised

13 November 2025

Date Accepted

13 November 2025

Date Published

20 March 2026

Editor

Prof Anél Gildenhuys

Journal Editor

Prof Wian Erlank

How to cite this contribution

Prinsen L "National Health Insurance and the Regulation of Electronic Health Records in South Africa: A Primer and Call for Clarification" *PER / PELJ* 2026(29) - DOI http://dx.doi.org/10.17159/1727-3781/2026/v29i0a21166

Copyright

DOI
http://dx.doi.org/10.17159/1727-3781/2026/v29i0a21166

Abstract

Electronic health records (EHRs) are digital records containing health information spanning a patient's lifetime. While the South African public health sector still largely uses hardcopy records, this is bound to change as the government plans to implement a new National Health Insurance (NHI) system. For this system to be efficient, patients must be registered and tracked and this may be achieved by the use of EHRs. While the use of EHRs is beneficial, it creates security and privacy risks to patient information – the most sensitive type of personal information. In order to protect this information as well as possible, EHRs must be adapted to regulatory frameworks and healthcare practitioners must practice in accordance with relevant South African legislation and regulations. These include the *Constitution of the Republic of South Africa*, 1996, the *National Health Act* 61 of 2003, the *Protection of Personal Information Act* 4 of 2013, the *Promotion of Access to Information Act* 2 of 2000, the *Electronic Communication Transaction Act* 25 of 2002, the *Cybercrimes Act* 19 of 2020 and the *Health Professions Act* 56 of 1974, as well as policy documents and guidelines by relevant authorities. This article serves as a primer on these regulatory instruments aimed at healthcare practitioners in preparation for the implementation of the NHI system. It further identifies issues in need of clarification.

Keywords

Electronic health records; ethical guidelines; National Health Insurance; legal regulatory framework.

.....

1 Introduction

Patient medical records, or health records, used to be a collection of paper documents. With the arrival of electronic health records (EHRs), however, and the increasing importance of the right to access, hardcopy records have been and are being replaced by EHRs. A health record may be defined as a "longitudinal collection of an individual's personal and health information, recorded by a healthcare practitioner or at the directive of the healthcare practitioner, regardless of the form or medium used to make such a record"[1] and "where the provider and patient must authorise access to the record".[2] Simply stated, EHRs are digital records containing health information spanning the patient's lifetime.[3]

In South Africa, a developing nation, the use of EHRs is considered a relatively new development in the private sector while paper records are still predominantly used in the public health sector.[4] This is bound to change as the South African government braces to roll out the new National Health Insurance (NHI) system. For the NHI system to be implemented, patients will need to register with the NHI, whereafter their use of healthcare services will be tracked. The registration and tracking of patients across South Africa will necessitate the adoption of a new approach to keeping patient records and this will most likely be achieved by making use of EHRs and national EHR systems.

EHRs have revolutionised healthcare delivery by providing healthcare practitioners (HCPs) with electronic access to a patient's medical history and facilitating the sharing of patient information across a continuum of care.[5] While the use of EHRs has many benefits, it also creates security and privacy risks to patient information, which has been identified as the most sensitive type of personal information.[6] The reason for this is that it contains

* Larisse Prinsen. LLB LLM LLD. Senior Lecturer, Department of Public Law, University of the Free State, South Africa. E-mail: prinsenl@ufs.ac.za. ORCiD: https://orcid.org/0000-0003-0931-4586.

1 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 1.

2 Malcolm, Lyons and Brivik Inc 2019 https://www.lyonsbriviklaw.com/who-owns-patient-records-in-south-africa/.

3 Tsegaye and Flowerday "POPI Compliance" 1.

4 Malcolm, Lyons and Brivik Inc 2019 https://www.lyonsbriviklaw.com/who-owns-patient-records-in-south-africa/.

5 Tsegaye and Flowerday "POPI Compliance" 1.

6 The complexity of EHR use lies not only in the technological aspects of implementation but also in the human and cultural dimensions of change management. Studies have noted that resistance from HCPs and entrenched paper-based practices remains a significant barrier to adoption. See Weeks 2013 *Journal of Contemporary Management* 136-143; Zharima, Griffiths and Goudge 2023 *Frontiers in Digital Health* 5.

confidential information that cannot be changed such as the medical history of the patient.[7]

EHRs, which fall under the greater umbrella of digital health, should be adapted and contextualised to local, national and international regulatory frameworks, and HCPs should practice digital health only in accordance with the relevant legislation and regulations. In South Africa these include the *Constitution of the Republic of South Africa,* 1996 (*Constitution*), the *National Health Act* (*NHA*),[8] the *Protection of Personal Information Act* (*POPIA*),[9] the *Promotion of Access to Information Act* (*PAIA*),[10] the *Electronic Communication Transaction Act* (*ECTA*),[11] the *Cybercrimes Act*[12] and the *Health Professions Act* (*HPA*).[13] The regulatory framework also includes policy documents and guidelines by relevant authorities such as the Health Professions Council of South Africa (HPCSA) and the South African Medical Association (SAMA). This article aims to act as a primer and is intended to educate HCPs on the various instruments at play in the EHR regulatory framework. As such, it will explore some of the most pertinent provisions regarding EHRs as provided for by these instruments with the aim of elucidating and contextualising these provisions for HCPs. Certain issues in need of clarification are also identified.

2 The NHI and EHRS

South Africa is in the process of actively attempting to achieve universal access to healthcare and progressively to realise socio-economic rights, such as the right to access to healthcare provided by section 27 of the *Constitution*. One of the strategies employed in doing so is the implementation of the NHI system. This system is empowered by the *National Health Insurance Act* (*NHI Act*),[14] which was signed into law on 15 May 2024. The *NHI Act* aims to achieve universal health coverage and to ensure that all South Africans gain access to quality healthcare services. It further aims to provide for the establishment of the National Health

7 Tsegaye and Flowerday "POPI Compliance" 1. The Constitutional Court has explained that the right to privacy encompasses informational privacy, but this expectation diminishes as individuals interact more widely with society. See *Bernstein v Bester* 1996 2 SA 751 (CC) para 67. An EHR system could therefore greatly risk the right to privacy as it entails an "interaction" of health information with wider "society", in a sense.

8 *National Health Act* 61 of 2003 (*NHA*).

9 *Protection of Personal Information Act* 4 of 2013 (*POPIA*).

10 *Promotion of Access to Information Act* 2 of 2000 (*PAIA*).

11 *Electronic Communication Transaction Act* 25 of 2002 (*ECTA*).

12 *Cybercrimes Act* 19 of 2020.

13 *Health Professions Act* 56 of 1974 (*HPA*).

14 *National Health Insurance Act* 20 of 2023 (*NHI Act*).

Insurance Fund, which will be used to cover the cost of almost all medical treatments from accredited providers.[15]

The efficacy of the NHI system will partly depend on its ability to register and track patients. South Africa is therefore developing and implementing a national EHR system.[16] The National Department of Health (NDoH), the Department of Science and Technology and the Council for Scientific and Industrial Research have developed a patient registration system that could be used along with EHRs.[17] This system aims to allow patient tracking when and where patients present themselves for treatment in South Africa.[18] Making use of EHRs could facilitate the registration and tracking of patients, which could then improve the continuity and quality of their care. EHRs also enable the sharing of a patient's data across points of care while allowing the added advantage of making current patient information available, on which treatment decisions may be based.[19] EHR systems allow the personal and health information of a patient to be captured, stored and shared.[20] In the context of the NHI, this is needed to allow quality access to healthcare and to allow for such access anywhere in South Africa.

The factors which may negatively impact on the use of EHRs may be social, technical or environmental, and it has been suggested that the connection of disparate systems, data combination, data accessibility, cyber security and a disaster recovery plan will be key enablers of a functioning national EHR system.[21] A discussion of these factors falls outside the scope of this article. Rather, this article focusses on the legal context, or more specifically the regulatory framework surrounding EHRs. Health records are mentioned only a few times in the *NHI Act* itself, and this lack of regulatory guidance further emphasises why knowledge of the greater legislative and ethical framework surrounding these records is necessary. These provisions state

15 Prinsen 2024 https://theconversation.com/south-africas-national-health-insurance-bill-has-noble-aims-but-leaves-too-much-uncertain-it-needs-more-work-208604.

16 Tsegaye and Flowerday "POPI Compliance" 1.

17 Katurura and Cilliers 2018 *African Journal of Primary Health Care and Family Medicine* 1.

18 Katurura and Cilliers 2018 *African Journal of Primary Health Care and Family Medicine* 1.

19 Katurura and Cilliers 2018 *African Journal of Primary Health Care and Family Medicine* 1.

20 Katurura and Cilliers 2018 *African Journal of Primary Health Care and Family Medicine* 1.

21 Moonsamy 2025 https://www.itweb.co.za/article/working-towards-a-single-electronic-health-record-for-sa/Pero37Z38KyMQb6m. Research further shows that South Africa's efforts at a national roll-out of EHRs have often faded due to weak leadership, insufficient technical skills in government and infrastructure challenges (connectivity and hardware shortages), with only the Western Cape having achieved a reasonably integrated provincial system. See Zharima, Griffiths and Goudge 2023 *Frontiers in Digital Health* 6-7; Katurura and Cilliers 2018 *African Journal of Primary Health Care and Family Medicine* 4.

that users of healthcare services or patients paid for by the NHI are entitled to access any records or information relating to their health which are kept by the NHI Fund in order to exercise or protect their rights in terms of section 6(c); and that, in regard to the National Health Information System, health workers, healthcare service providers and those in charge of health establishments must adhere to the provisions of the *NHA* relating to access to health records as well as the protection of those records in accordance with section 34(3). Regarding the information platform of the Fund, the platform must facilitate (a) "the implementation of the objects and the effective management of the Fund", and (b) the "portability and continuity of healthcare services available to users", in order to fulfil the requirements related to information dissemination and recordkeeping.

These provisions offer very little detail as to how EHRs should be created, retained, stored and protected. As such, attention must be given to the instruments discussed below to ensure the lawful handling of patient records and the ultimate efficacy of the NHI system.

3 The regulatory framework

3.1 The Constitution

As the *Constitution* is the supreme law of South Africa, any law or conduct inconsistent with it is invalid, while the obligations imposed thereby must be fulfilled. This is important to keep in mind as the conduct of HCPs regarding the provision of healthcare services and the handling of health records will have to withstand any constitutional scrutiny. This also means that any regulatory instrument, legal or ethical, must be in line with the *Constitution*. These instruments are also often founded on constitutional mandates, as will be noted.

Four provisions found in the *Constitution* must be always kept in mind in the context of this article. First, section 12 of the *Constitution* provides for the freedom and security of the person. It states in subsection (2)(c) that everyone has the right to bodily and psychological integrity. This includes the right not to be subjected to medical or scientific experiments without the informed consent of the relevant person. This confirms the inviolability of consent and underscores the importance of the consent provisions in the Acts, which are to be discussed below. Second is the right to privacy as provided for in section 14. This section is reflected in the privacy protection mechanisms found in *POPIA* and, in the context of medical treatment, is further elaborated on by the *NHA*. Third, the *Constitution*, in section 27(1)(a), also provides that everyone has the right to access to healthcare. The existence of this section partly motivated the enactment of the NHI system, as subsection (2) requires that the state must take reasonable legislative (and other) measures to achieve the progressive realisation of

the right to access to healthcare.[22] Last is the right to access to information, as found in section 32 of the *Constitution*. In terms of this section everyone has the right to access to (a) "any information held by the state", and (b) "any information held by another person" and which is needed for the exercise or protection of any of the rights enshrined in the *Constitution.* A relevant example of this may be a HCP requiring access to a health record to mount a defence against pending litigation. Further, subsection (2) requires that national legislation must be enacted to give effect to this provision, and it is this same provision which prompted the creation of *PAIA,* as discussed below.

Other notable rights guaranteed by the *Constitution* include right to equality (section 9), human dignity (section 10) and life (section 11). These rights are, however, not absolute and may be justifiably limited in terms of the limitation clause (section 36). A full discussion of these rights and non-derogability falls outside the scope of this article, however.

3.2 The National Health Act

The *NHA* provides for access to and the protection of health records. It should be noted that no distinction is made between paper records and EHRs in the Act, and as such, all provisions apply equally. In terms of section 15 of the *NHA* a HCP who has access to health records may disclose personal information, the meaning of which is discussed below, contained in the record to another HCP, a health establishment or any other person as is needed for any legitimate purpose in the ordinary scope and course of the HCP's duties where such disclosure is in the patient's best interests.[23] Although the *NHA* provides no clarification of what this means, it is suggested that emergency medical treatment may constitute such an instance. It may be noted that here the *NHA* specifically refers to "personal

---

22 Subsection (2) of s 27 of the *Constitution* therefore places a mandate on the state to attempt to realise the rights provided for in s 27, a mandate which has been repeatedly reaffirmed and emphasised in South African constitutional case law, which includes *Soobramoney v Minister of Health (KwaZulu-Natal)* 1998 1 SA 765 (CC) and *Minister of Health v Treatment Action Campaign (TAC) (No 2)* 2002 5 SA 721 (CC). As the *NHI Act* is aimed at providing better and quality healthcare to all South Africans, it may be seen as the state's real-world attempt at providing access to healthcare services to everyone as envisioned in the Bill of Rights.

23 This may raise questions of confidentiality. As was explained in *WB v RB* 2024 4 SA 316 (KZD) (*WB v RB*), it is not difficult to understand why health-related information should be treated as confidential as this information invariably includes sensitive personal information. S 14 of the *NHA* also imposes a duty of confidence in regard to information contained in a health record. However, the *WB v RB* case also held that "the confidential relationship between doctor and patient must yield to the requirement of public policy". The NHI is a matter of public policy and as such its necessary components, including EHRs, might also qualify as such. This might mean that the implementation of the NHI-related EHR system could justifiably limit confidentiality rights and expectations. See *WB v RB* paras 22-23.

information" as defined by *PAIA*. At the time that the *NHA* was drafted and promulgated, *POPIA* had not yet come into existence. It is submitted that the definition of "personal information" provided for by *POPIA* should now be followed, as will be explained in further detail below. Further, an HCP may, with the consent of the patient, examine a patient's records for treatment or where the purpose of accessing the record is study-, teaching- or research-related, with the authorisation of the head of the relevant health establishment and that of the appropriate health research ethics committee, according to section 16(1)(a) and (b). However, in terms of section 16(2), where these actions do not reflect or obtain information on the patient's identity, neither the consent of the patient nor the head of the establishment, is required.

Regarding the protection of records, section 17(1) provides that the person in charge of a health establishment must establish control measures to prevent unauthorised access to any records, the storage facility where these are kept, or the systems on which these records are housed or kept. Health records must be protected not only from unauthorised access but also from misuse by those who are authorised to access the records. In this regard section 17(2) criminalises various activities, which include *inter alia* the falsification; creation, alteration or destruction of records; the copying of records; failing to protect records; and connecting any personal identification elements of a record with any element of that record that concerns a patient's condition, treatment or history. It also criminalises various offences related to accessing or intercepting the electronic device or storage system, operating system or programme on which the records are kept.

3.3 The Protection of Personal Information Act

The use of EHRs and a national EHR system as envisioned under the NHI increases the risk to security and privacy, as information which was previously accessible only at a local health facility will be available anywhere in South Africa.[24] As mentioned previously, EHRs need to be protected from both unauthorised entities and misuse by authorised HCPs.[25] *POPIA* is the most important regulatory instrument in South Africa in terms of providing for privacy,[26] and the most relevant to the lawful processing of patient information within a national EHR system. Certain provisions are of importance in this regard. Before discussing these, however, a clarification

24 Tsegaye and Flowerday "POPI Compliance" 1.

25 Tsegaye and Flowerday "POPI Compliance" 1.

26 In the very recent case of *De Jager v Netcare Limited* (42041/16) [2025] ZAGPPHC 141 (17 February 2025) para 6 the court reaffirmed the principle of subsidiarity, confirming that for the right to privacy, *POPIA* is the primary instrument, meaning that challenges to the collection or use of personal information must be framed under POPIA's provisions.

of the relevant terminology is required, especially the meaning of "personal information", "special personal information" and "record" per section 1 of *POPIA*.

> "Personal information" means information relating to an identifiable, living, natural person and, where applicable, an identifiable, existing juristic person. This includes, but is 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 a 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;
>
> (e) 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 reveal the contents of the original correspondence;
>
> (g) The views 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.

"Special personal information" is described in section 1 and section 26 of *POPIA* and means:

> personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a person; or the criminal behaviour of the person.

A "record" is any recorded information:

> (a) Regardless of form or medium, including any of the following: writing on any material; information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; book, map, plan, graph or drawing; or photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
>
> (b) In the possession or under the control of a responsible party;
>
> (c) Whether or not a responsible party created it; and
>
> (d) Regardless of when it came into existence.

For the processing of personal information to be legitimate, it must meet several conditions.[27] These correspond to certain sections of *POPIA*[28] and are as follows:

1. "Accountability" (section 8) means that any person in control of another person's personal information must appoint an Information Officer (IO). The IO must ensure compliance with *POPIA* and its principles. This means that HCPs and health establishments must appoint a person within their practice or facility to act as such;
2. "Processing limitation" (sections 9 to 14) allows for the lawful processing, the minimisation of collected information,[29] consent, justification and objection, and for the collection of personal information directly from the "data subject" (DS). These provisions establish boundaries around the lawful processing of data and emphasise that the least amount of information needed to enable healthcare services should be collected. This also means that consent should be sought not only for the performance of the healthcare service but also for the collection of personal information in the process of delivering such a service;
3. "Purpose specification" (sections 13 and 14) means that personal information should be collected only for a specific purpose and that the relevant person (the person whose information is collected) must be made aware of this purpose. In the context of this article, this purpose is the rendering of a healthcare service. This further means that patients need to consent to the processing of their information, and if consent cannot be obtained any processing of information is lawful only where the EHR was accessed during an emergency;[30]
4. The phrase "further processing limitation" (section 15) builds on the previous condition, since it requires that where a third party must process information, the processing must still be in accordance with the original, specific purpose. This may be relevant where a healthcare service has been delivered but a further opinion is needed to better diagnose or treat the patient. All the information given to the additional HCP must still serve the original purpose for which it was collected. In the context of the NHI system and EHRs, this might also mean that information collected in order to give treatment should not be shared with health researchers, for example, without the consent

27 Tsegaye and Flowerday "POPI Compliance" 4.
28 Prinsen 2023 *AJICL* 216-218.
29 Tsegaye and Flowerday "POPI Compliance" 4.
30 Tsegaye and Flowerday "POPI Compliance" 4.

of the patient. Certain exceptions to the processing conditions may, however, be applicable here;[31]

5. "Information quality" (section 16) means that the IO must take reasonable steps to ensure that the information collected is complete, accurate, not misleading and up to date. This insurance must be performed in a manner that aligns with the purpose for which the information was collected. This may mean that the HCP who makes a referral for a second opinion must ensure that all the information contained in a health record is correct;
6. "Openness" (sections 17 and 18) requires that the responsible party (a public or private body or any other person who, alone or in conjunction with others, determines the purpose of and means for the processing of information) must be open regarding the collection of personal information. The Information Regulator (IR), as established by *POPIA*, must be notified where personal information is processed and where it is to be collected. The responsible party must also ensure that reasonably practicable steps have been taken to guarantee that the patient has been informed that his or her information will be collected. Again, this relates to patient consent not only to the rendering of a healthcare service but also to the collection and processing of his or her personal information, i.e., the creation and keeping of health records. It is not clear whether this would require the IR to be informed whenever a health record is newly created or whenever a patient presents for treatment and new information is added to the existing record, and clarification from the NDoH is needed in this regard;
7. "Security safeguards" (sections 19 to 22) require the responsible party to protect the integrity of the information under his or her control through technical and organisational measures. This relates to the technical aspects of EHRs such as encryptions, for example; and
8. "DS participation" (sections 23 to 25) provides that a DS, the patient, has the right to request that responsible parties confirm whether they have information relevant to the said DS and may also request a description of this information. In these instances, *PAIA* may also be applicable.

Certain exemptions from these processing conditions are, however, provided for by *POPIA*.[32] An exemption from any of the conditions may be granted where it is shown that public interest in the processing of personal

31 Tsegaye and Flowerday "POPI Compliance" 4.
32 Prinsen 2024 *Frontiers in Genetics* 11.

information significantly outweighs any violation of the privacy of the patient. According to section 37(2)(a) of the Act, this includes the interests of national security, which include public safety. This means that where a patient has a dangerous and infectious disease, an argument for the waiver of the processing conditions may be acceptable.[33] It may not be easy, however, to show that public interest significantly outweighs the constitutionally protected right to privacy.[34] It may also be noted that section 37(2)(e) of *POPIA* states that research activities are included as matters of public interest.

Special information may also not be processed, in terms of section 26, unless consent has been obtained from the patient. The IR may also grant an exemption based on (1) the processing occurs in response to the need to establish, exercise or defend a right or legal obligation; (2) the processing is for historical, statistical or research purposes; or (3) the processing serves a purpose in line with public interest, or it is impossible or would entail a "disproportionate effort" to obtain consent from the patient and the required safeguards are in place to guarantee that the patient's privacy is not affected in a disproportionately adverse manner according to section 27 of *POPIA*.

In addition, section 32 of *POPIA* is of particular importance for health-related information. This provision, almost in contrast to section 26, creates express authorisations for processing information concerning a DS's health or sex life notwithstanding the general prohibition in section 26. In particular, section 32(1)(a) allows HCPs, healthcare institutions or facilities and social services to process such information if it is necessary for the proper treatment and care of the patient or for the administration of the institution or professional practice concerned. This authorisation means that, in the context of EHRs, processing by doctors, nurses and health facilities for diagnosis, treatment and administrative functions is lawful without requiring separate patient consent for each particular health intervention, provided that the confidentiality obligations under section 32(2) and (3) are met.[35]

---

33 Although *Minister of Health of the Province of the Western Cape v Goliath* 2009 2 SA 248 (C) predates *POPIA*, this case is interesting to note as it set a precedent for the limitation of rights in the public interest and safety in a health context. In terms of this case**,** public health and safety interests in containing a dangerous infectious disease, extreme drug-resistant tuberculosis (XDR-TB) *in casu*, was stronger than the individual rights being limited. Today this balancing exercise mirrors the logic in s 37 of *POPIA*, which allows exemptions where public interest (including public safety) outweighs privacy.

34 See, for example, however *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors* 2001 1 SA 545 (CC) para 15, confirming that privacy is fundamental but subject to justifiable limitations.

35 These sections state that any responsible party who processes health or sex-life information under s 32 of *POPIA* is bound by confidentiality. Where a confidentiality obligation already exists (by virtue of law, office, profession or employment) it automatically applies. Where it does not exist, the responsible party must still treat

For the NHI and the national EHR system, this means that the routine processing of health information for diagnostic, treatment, referral or administrative actions is expressly provided for. In practice it relieves HCPs and facilities from having to seek renewed consent in each instance where patient information is accessed or transferred within the NHI system, provided that confidentiality safeguards are respected.[36] At the same time, the provision sets clear boundaries: any processing outside the listed purposes remains restricted and subject to stricter consent or exemption requirements. Section 32 does also not negate the initial consent requirement as provided for in section 11 of *POPIA*.[37] In the context of the NHI, section 32 may be regarded as the mechanism that makes the EHR system workable without undue administrative burdens.

Section 32(1)(b) further extends authorisations to insurance companies, medical schemes, administrators and managed healthcare organisations where processing is necessary for risk assessment, the performance of contracts or the enforcement of rights and obligations. It is currently uncertain if the NHI, as medical insurance, will follow processes similar to those of private medical aid schemes in regard to the risk assessment of (potential) clients. Clarification from the NDoH is needed in this regard so that the potential application of section 32(1)(b) to EHRs and the NHI may be fully understood.

Despite the general leniency of section 32, it is important to note that section 32(5) restricts the processing of genetic or inherited health characteristics unless a serious medical interest prevails or the processing is required for

---

the information as confidential, and may share it only if legally required to do so or if it is necessary to share it with another party who is lawfully authorised to process it under s 32(1).

36 Significant scholarly debate remains regarding *POPIA* and consent in health-related contexts. While ethical guidelines in South Africa encourage broad consent for the future and secondary use of data, *POPIA's* statutory wording points toward a stricter requirement of (specific) informed consent, creating an unresolved tension between the medico-legal and privacy frameworks. See Swales 2022 *PELJ* 13-16.

37 Although consent is not directly addressed as problematic in this article, s 11(a) of *POPIA* provides that personal information may be processed only if this is consented to by the DS. In the context of this article, the DS is the patient. S 11(3) of *POPIA*, however, allows for the withdrawal of consent to processing. This creates some tension within the Act as s 27 of *POPIA* does not mention the right to withdraw consent in respect of special information. This raises the question: is a patient entitled to withdraw consent for the processing of his or her (special) health information and if so, what are the larger implications of patients "opting-out" of a system of information processing such as EHRs? What impact will this have on the functioning of the NHI in providing health services across the country? This is a matter that will have to be clarified by the NDoH. In the interim De Stadler *et al Over-thinking* 67 suggest that DSs do have the right to withdraw their consent to processing as a requirement of valid consent is that it be voluntary. Whether this argument will stand, considering the statutorily mandated participation of all South Africans in the NHI scheme, remains to be seen.

historical, statistical or research purposes. *POPIA* further provides for the retention and restriction of records in section 14 and states that records of personal information should not be retained for longer than is needed to achieve the object for which the information was collected or subsequently processed unless this retention is authorised by law; the responsible party reasonably requires the records for any lawful purposes associated with its functions; a contract requires it; or consent has been obtained for such retention. In certain instances records may be kept for longer periods for historical, statistical or research purposes. Again appropriate safeguards against the use of the records for other purposes must be established. Records must be destroyed or de-identified as soon as the holder thereof is no longer authorised to retain such records, and the destruction must be done in a manner which does not allow for the intelligible reconstruction thereof. *POPIA* applies only to "living natural persons," however, and as the purpose for which the information was collected, the provision of healthcare, is nullified by death, uncertainty exists as to whether HCPs and health establishments will have to destroy all health records after the death of a patient, whether the health records need only be de-identified, or whether this merely means that the processing conditions fall away. It is also important to note that section 14(2) of *POPIA* allows for longer retention periods where the information contained in the record may be used for historical, statistical or research purposes where appropriate safeguards against the records being used for any other purposes are in place. Adding to this confusion is the HPCSA provision, as discussed below, that health records be retained indefinitely.

3.4 The Promotion of Access to Information Act

PAIA provides for health records in a few sections. This Act has, however, been amended to some extent by *POPIA*, and only the provisions directly related to these records will be discussed here, as they provide specifically for access. One of the most notable amendments concerns the amendment to the definition of "personal information", which is now largely the same as that provided by *POPIA*.[38]

PAIA makes a distinction between information held by public and private bodies, and it is suggested that this distinction may fall away once the NHI system is in place, as it aims to nationalise healthcare, thereby nullifying this difference in the context of health services. The NDoH should provide clarity in this regard. This discussion will focus on the extant law, however, discussing

[38] The new *PAIA* definition of personal information, however, ends with the following condition: "but excludes information about an individual who has been dead for more than 20 years".

first the provisions relating to public matters (sections 30 and 34) and then those relating to private matters (sections 61 and 63).

A person has the right to request access to a record held by a public body in terms of section 11 of the Act. Where such request is made for a health record, either by the relevant patient or by someone on behalf of the patient, the IO may before granting access, in terms of section 30(1), consult with a HCP where he or she is of the opinion that the disclosure of the record might cause serious harm to the physical or mental health or well-being of the person concerned.[39] Where a person is below the age of 16 or otherwise unable to request access themselves, this should be done on his or her behalf. Section (3)(a) states that if, after being granted access to the relevant record, the HCP consulted is of the opinion that disclosure is likely to cause serious harm, the IO may grant access to the record only if the requester can prove, to the satisfaction of the IO, that proper provisions have been made for counselling, or other reasonably practicable arrangements, during or after the disclosure of the record, to negate such harm. The person responsible for the counselling or other arrangement must also be given access to the record before the requester is granted access.

Section 34 states that an IO of a public body must refuse any request for access to a record if this would involve the unreasonable disclosure of the personal information of a person, including that of a deceased. In terms of subsection (2)(d), however, a record regarding the physical or mental health or well-being of a person who is below the age of 18 or incapable of understanding the nature of the request and who is under the care of the requester may not be refused if granting such access would be in the relevant person's best interests.

A person may also request access to a record held by a private body in terms of section 50 of the Act, and section 61 provides for the same conditions to be met as in section 30, as discussed above. Also, like section 34 section 63 provides for instances where access may be refused. The relevant person may, of course, also consent to access being granted, in which case the IO should not refuse access.

What the above means is that *PAIA* allows for a request for access to be made, which request should be followed by a decision on whether this will be granted. The relevant body is thus given an opportunity to decide if the disclosure would constitute a "serious harm", which would justify refusal of

39 For example, in a custody dispute the court in *WB v RB* ordered the limited disclosure of a patient's treatment details, withholding delicate therapy notes to safeguard both privacy and the best interests of the child involved. This case illustrates how access to EHRs may need nuanced adjudication when the right to information collides with potentially harmful outcomes.

access.[40] *PAIA* clearly requires that a decision must be made before access to records may be granted. The advent of EHRs, however, could lead to a scenario in which patients have the right to view their EHRs online, which could be detrimental to their physical or mental health and well-being.[41] This is an issue which requires clarification.[42]

It must also be kept in mind that although *PAIA* makes provision for the right to access and the necessary procedures to request such access, patients in a developing nation such as South Africa may not be able to access their EHRs due to socio-economic, educational and computer literacy challenges.[43] Despite patients demonstrating an interest in accessing their health records online, further issues of privacy, usability, actual accessibility and costs will also need clarification.[44]

3.5 The Electronic Communications and Transactions Act

Although the *ECTA* is somewhat outdated regarding certain of its provisions (cybercrimes, for example) in the context of EHRs, it still carries some force. It offers valuable guidance in the handling of electronic communications. An "electronic communication" is a communication by means of data messages, and a "data message", according to section 1 of the Act, is data which have been generated, sent, received or stored by electronic means, including a stored record such as a health record.

The *ECTA* is also important in terms of EHRs as it extends legal recognition to these records. In terms of section 11 of the Act information is not without force or effect merely because it is wholly or partly in the form of a data message, which means that EHRs are subject to legal rights and

40 Malcolm, Lyons and Brivik Inc 2019 https://www.lyonsbriviklaw.com/who-owns-patient-records-in-south-africa/.

41 Malcolm, Lyons and Brivik Inc 2019 https://www.lyonsbriviklaw.com/who-owns-patient-records-in-south-africa/. Also see, for example, *Centre for Child Law v Media 24 Ltd* 2020 4 SA 319 (CC), in which the Court underscored the need to protect informational privacy, particularly where disclosure could cause harm.

42 This reflects wider international debates on "regulatory lag", where technological changes outpace legal safeguards, leaving uncertainty over how rights of access, privacy and health should be balanced in digital systems. See Cachalia and Klaaren 2022 *PELJ* 2-3.

43 Malcolm, Lyons and Brivik Inc 2019 https://www.lyonsbriviklaw.com/who-owns-patient-records-in-south-africa/.

44 Malcolm, Lyons and Brivik Inc 2019 https://www.lyonsbriviklaw.com/who-owns-patient-records-in-south-africa/. According to Desfarges 2023 https://www.quicknews.co.za/2023/12/13/the-nhi-will-enforce-the-use-of-ehrs-resulting-in-a-steep-learning-curve-for-60-of-sas-gps/, South Africa lags behind world averages in relation to the use of health technology by patients, with less than a third of South Africans using digital technologies to track their own health. This may be a result of a lack of trust in the security of their health data as well as affordability concerns.

obligations. It is for this reason that this article has attempted to elucidate the regulatory framework surrounding EHRs in South Africa.

Although the *ECTA* does not clarify the uncertainties in the retention-period discussed above, it does provide for the requirements of the lawful retention of a data message in that section 16 states that where the retention of information is legally required, this requirement will be met by retaining such information in the form of a data message, if the information contained in the message is usable and accessible for its intended purpose; if it is in the format in which it was generated, sent or received, or if not, in a format that accurately represents the generated, sent or received information; and if the origin and destination of the data message as well as the date and time it was sent or received can be determined. In the context of EHRs this is in line with the *POPIA* conditions on the security and integrity of a record of personal information, and it also underlies the HPCSA and SAMA guidelines on the integrity of health records, as will be discussed below.

The creation of an EHR involves the collection and storage of patient information using electronic systems. If this involves communication between HCPs or providers and others (insurance companies, the state, etc.), it could potentially qualify as an electronic transaction under the *ECTA*. The key element is whether the creation of the EHR facilitates the exchange of information as part of a broader service or transaction – the rendering of a healthcare service, in the context of this article.

Sections 50 and 51 of the *ECTA*, which previously governed the principles for the electronic collection and processing of personal information, were repealed by *POPIA,* which now offers a robust and expanded framework applicable to all forms of data processing, whether electronic or not. Previously section 50 of the *ECTA* provided for the protection of personal information specifically obtained through electronic transactions.[45] In this regard *POPIA* offers a more comprehensive and cross-sectoral framework for data protection, including the collection, use and disclosure of health-related data. Section 51 of the *ECTA* laid the foundation for consent, the limitation of purpose, recordkeeping and deletion obligations. These principles are now embedded and broadened under *POPIA*, as discussed previously. *POPIA* surpasses and strengthens the *ECTA* regime, offering more comprehensive protection for personal information, including the information contained in EHRs.

---

45 In s 1 the *ECTA* defines a transaction as a "transaction of either a commercial or non-commercial nature and includes the provision of information" while the addition of the identifier of "electronic" might mean to facilitate any communication between persons or to offer or accept any information, goods or services, or to conduct any type of activity in or by electronic means.

Further possible important provisions found in sections 52 to 58 of the *ECTA* relate to the protection of a critical database. "Critical data" are data which have been declared by the Minister of Communications to be of importance to the protection of national security or to the economic and social well-being of South Africa.[46] It is submitted that personal information, and especially personal information relating to a person's health as contained in an EHR, would qualify as being of importance to the social well-being of South Africa. If this argument is accepted, the national EHR system mentioned above might constitute a critical database, which is described as a collection of critical data in an electronic format from which it may be accessed, reproduced or extracted. Again, if this argument is accepted the NDoH, the Department of Science and Technology and the Council for Scientific and Industrial Research will have to adhere to the provisions of the *ECTA* in the development of the national EHR system. A detailed discussion of these provisions, however, falls outside the scope of this article.

3.6 The Cybercrimes Act

While *POPIA* provides the primary framework for the lawful processing of personal information, including the handling of health data in EHR systems, the *Cybercrimes Act* adds an additional layer of protection by criminalising conduct that threatens the integrity, confidentiality and availability of data.[47] Specifically, section 2 criminalises gaining unlawful and intentional access to a computer system or a data set, while section 3 penalises the unlawful interception of data. Importantly, section 4 addresses the unlawful acquisition, possession, provision or use of passwords, access codes or similar data, which is highly relevant in the context of EHR security. Sections 5 and 6 further criminalise interference with data or computer systems, including acts such as the corruption, deletion or hindering of access to data. These are all critical threats in the context of health records, as having incorrect information could lead to incorrect diagnosis or treatment and the

46 Scholars have argued that a national EHR database would almost certainly qualify as such a "critical database", requiring strong governance and interdepartmental coordination to ensure compliance with standards of interoperability, upgradeability and security. See Weeks 2013 *Journal of Contemporary Management* 140; Cachalia and Klaaren 2022 *PELJ* 8.

47 Although the *Cybercrimes Act* adds an additional layer of protection to EHRs in general, *POPIA* does make provision for certain offences and penalties. Roos "Data Protection" 221 is of the opinion that there exist some offences that are considered more serious than others. For example, hindering, obstructing or unlawfully influencing the IR would constitute a serious offence and carry a penalty of a maximum period of 10 years imprisonment and/or a fine. A less serious offence would be, for example, a breach of the duty of confidentiality imposed on persons acting on behalf of the IR, and these lesser offences carry a penalty of a maximum of one year's imprisonment.

hindering of access could lead to life threatening situations, as where a health record is needed in an emergency.

These *Cybercrimes Act* provisions offer deterrent force against unauthorised access to, the abuse of or the manipulation of EHRs which complement the administrative safeguards found in *POPIA* with enforceable criminal sanctions. Together with the protective mechanisms in section 17(2) of the *NHA* and sections 19 to 22 of *POPIA*, the *Cybercrimes Act* creates a strong and enforceable deterrent regime. However, there is still fragmentation, as the overlapping and often uncoordinated application of these laws would call for greater legislative alignment, particularly within the NHI framework. This is an issue that will need further clarification.

4 Regulatory and other authorities: guidelines

4.1 Health Professions Council of South Africa

Although the *HPA* itself is silent on the issue of medical records, it does in section 2 establish the HPCSA. This is the statutory body in charge of the education, training and registration of HCPs in South Africa, and it provides regulatory guidance in the form of guidelines.

The HPCSA Guidelines on patient recordkeeping,[48] which should be read in conjunction with the guidelines on patient consent[49] and those on confidentiality,[50] provide detailed guidance on the purpose, content, related rules, alteration, privacy and security, retention, ownership of and access to patient records, amongst other matters. The Guidelines even provides a checklist for health recordkeeping.[51] As mentioned above in the definition of a health record, it is a collection of health information which is recorded by an HCP "regardless of the form or medium used to make such a record",[52] which indicates that the HPCSA Guidelines does not strictly distinguish between paper and electronic records. The Guidelines offers valuable insight into the regulatory expectations surrounding EHRs.

According to the Guidelines, the purpose of a health record is threefold. First it acts as a reminder of what has been found, decided or done; second it promotes continuity of care; and third, it provides evidence of the standard of care given. Secondary uses include promoting good clinical practice,

48 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf.

49 HPCSA 2021 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_4_Informed_Consent_vDec_2021.pdf.
HPCSA 2021 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_5_Confidentiality_Protecting_and_Providing_Information_vDec_2021.pdf.

51 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 9.

52 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 1.

conducting clinical audits, teaching and research, and administration. It acts as evidence for occupational disease or injury compensation, and to provide evidence during litigation.[53]

The Guidelines also provides comprehensive provisions on what health records should include, and identifies the compulsory elements of a patient record. These are the:

- Personal (identifying) particulars of a patient;
- Full biopsychosocial history of a patient, including allergies and idiosyncrasies;
- Time, date and place of consultation(s);
- Assessment of the patient;
- Proposed management of the patient;
- Medication and dosage prescribed;
- Details of referrals to specialists and other healthcare professionals;
- Patient's response to treatment, which includes adverse effects;
- Any investigations ordered and their results;
- Details of the patient being booked off work or similar activities and the relevant reasons; and
- Written proof of informed consent when this is relevant.[54]

It is submitted that the aspects listed here would constitute "the least amount of information needed to enable a healthcare service" as mentioned above under the discussion of *POPIA*'s processing limitation.

Further thorough guidelines on what the records should include, such as all relevant clinical findings, and what need not be included, such as certain interactions (all correspondence related to a patient's care), are also provided.[55]

Patient records must be contemporaneous, and where alterations are made to a record, late or additional entries must be signed in full or fully attributable to the person making such a change, and it must be dated. The reason for the amendment must also be specified on the record.[56] In addition to these content-related aspects, the Guidelines also requires that

---

53 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 1

54 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 2-3

55 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 1-3. HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 4.

health records have integrity in that they be accurate, comprehensive and complete; clear and legible; unambiguous; have not been tampered with; may not contain any derogatory language; must be checked regularly; and must identify the patient to which the notes refer.[57]

As was mentioned above, section 17(1) of the *NHA* requires that control measures should be in place to prevent any unauthorised access to health records, their storage facility or system. This means that patient records must be securely stored, and in this regard the Guidelines provides that this requirement applies regardless of the record's format (electronic or hardcopy).[58] Ensuring timely and secure access to a health record is essential for the effective and safe delivery of a healthcare service, and all records must be protected against inappropriate access and disclosure. This mandate also extends to protecting privacy and confidentiality during electronic data transmission or when information is transferred between facilities and/or HCPs.[59]

Related to the storage of records is the issue of retention, for which the HPCSA has also made guiding provisions. According to the Guidelines health records should be stored indefinitely, especially if this is made possible by using electronic formats.[60] Where this is not possible or practical, a record should be stored for a minimum of at least six years from the date of dormancy (the time when a healthcare practitioner last treated a patient). Certain exceptions exist where records may have to be retained for a longer period, such as where patients were under the age of 18 years when they were cared for; for mentally incapacitated patients; where matters relate to the *Occupational Health and Safety Act* 85 of 1993; where statutory obligations in this regard exist; and where the facts of the case at hand require longer retention periods, such as in instances of asbestos poisoning.[61] The practicality problem of retaining records should be nullified by the use of a national EHR system, which means that health records could be kept indefinitely. With reference to the *POPIA* provisions on record retention, however, personal information may be kept for only as long as is justified by the purpose for which they were created. In the context of the provision of healthcare services, this purpose comes to an end at the death

57 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 3.

58 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 4.

59 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 5.

60 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 5.

61 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 5.

of a patient.[62] It is suggested that since the *POPIA* processing conditions apply only to living persons, patients' medical records fall outside *POPIA*'s scope after death. This creates two viable options. First, to destroy the records, or second, to de-identify them for historical, statistical or research purposes. Where records have been de-identified, they may be kept for an extended time on condition that appropriate safeguards are in place to protect against the misuse of the information. It is strongly suggested, however, that the NDoH provide clarification on this matter.

Health records must be readily available whenever a patient is treated in a healthcare facility and the information in the record must be stored in such a way as to allow easy access to be able to provide the patient with quality care. Information regarding allergies to certain medications or special needs, for example, is of the utmost importance in assuring proper care.[63] It is submitted that this does not negate any responsibilities regarding the restriction of access to a health record or personal information. Access to health records should be contingent on the relevant consent, as with access comes risks to privacy and confidentiality. There are, however, instances in which access may be obtained without such consent. Here the HPCSA Guidelines provide that HCPs may make health records available to third parties without the patient's consent: where a court has made an order to this effect; where a patient is suing a third-party HCP or the HCP has HPCSA disciplinary proceedings instituted against him or her and requires access to the records to mount his defence; where the HPC is under a statutory obligation to disclose certain medical facts such as suspected child abuse; and where the non-disclosure of patient information would constitute a serious threat to public health.[64] It must be noted that all requests to access patient records should comply with *PAIA*, as noted above. The *POPIA* conditions, as discussed above, will also be applicable and must be complied with in general. These include the provisions regarding special personal information and the authorisations as provided for by section 32 of *POPIA*. In this regard it must be kept in mind that information on a patient's religious beliefs, race, health or sex life and biometric information is deemed "special personal information" according to *POPIA* and may be processed only if necessary for the proper treatment and care of the patient.

---

62 This ambiguity has also been identified in scholarly work as a pressing legal gap: while the HPCSA Guidelines recommend indefinite retention, *POPIA* restricts data processing to living persons, leaving uncertainty over obligations towards deceased patients' records. See Swales 2022 *PELJ* 11; Katurura and Cilliers 2018 *African Journal of Primary Health Care and Family Medicine* 6.

63 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 4.

64 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 8.

Lastly, the HPSCA Guidelines requires that health records must be attributable, meaning that any person who creates an entry in a record must be identifiable, and where multiple HCPs are responsible for a health record, as in a hospital setting, each entry made must be dated, timed and signed in full. The HCP's name must also be recorded alongside his or her signature in block letters, and the relevant contact details must be included in the record.[65]

4.2 South African Medical Association

SAMA has broadly addressed the issue of EHRs in its statement on digital health.[66] This statement describes digital health as an umbrella term which refers to "the use of information and communication technologies in medicine and other health professions to manage illnesses and health risks and to promote wellness", and this includes telehealth, telemedicine, EHRs and mobile health.[67]

HCPs must ensure that the privacy, data confidentiality and integrity of a patient are not compromised and must also ensure that the electronic transmission of information, EHRs, is safeguarded against unauthorised access. Should a data breach occur, the patient must be notified immediately.[68] The provisions of the *Cybercrimes Act*, as set out above, will also be relevant in this context.

SAMA further recommends that users of digital health services should be informed of how the collection, storage, protection and processing of their health information is performed and that their consent must be obtained before any of their personal health data are disclosed to third parties, such as researchers, government agencies or insurance companies.[69] In the absence of such consent, the provisions found in *POPIA* regarding consent exemptions may be applicable where appropriate, such as the provisions of section 32(1)(b), discussed previously.

Patients must be able to access their health records, request the correction of errors, be informed of how their health information has been used, which then includes being informed of the persons or organisations to whom the information has been disclosed, request restricted access to their

---

65 HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf 4.

66 SAMA 2022 https://www.samedical.org/files/SAMA_Statement_Digital_Health_2022Mrch23.pdf.

67 SAMA 2022 https://www.samedical.org/files/SAMA_Statement_Digital_Health_2022Mrch23.pdf1.

68 SAMA 2022 https://www.samedical.org/files/SAMA_Statement_Digital_Health_2022Mrch23.pdf3.

69 SAMA 2022 https://www.samedical.org/files/SAMA_Statement_Digital_Health_2022Mrch23.pdf3.

information and limit the use of their information.[70] These requirements are in line with the processing limitations provided for by *POPIA,* which were discussed previously.

Should a patient believe that his or her privacy has in fact been violated, the patient may file a complaint with the relevant Privacy Officer or data protection authorities according to domestic law.[71] Again, *POPIA*'s establishment of an IR and IOs may be applicable in these instances.

5 Conclusion

Digital health technologies such as EHRs generally involve the collection of medical, physiological, lifestyle, activity and environmental information to fulfil the purpose of the provision of a healthcare service. This large amount of data also offers vast opportunities to conduct research into effective healthcare delivery and disease prevention. Still, this potential for secondary use also presents great potential for abuse, in addition to issues of the unauthorised access and misuse of information by persons with authorised access.[72] Robust policies and safeguards are required to regulate and secure the collection, storage, protection and processing of a patient's electronic health data. South Africa has a robust and comprehensive regulatory framework. Still, for this to be properly adhered to and in the context of the looming implementation of the NHI system, knowledge of the existing regulatory framework surrounding EHRs is imperative, and this article has attempted to provide elucidation in this regard. This should allow HCPs to better prepare for what the future holds.

The South African regulatory instruments providing for the required safeguards, although comprehensive,[73] are not perfect, and some issues in need of clarification were identified. These include whether an IR should be informed whenever a health record is newly created or when a patient presents for treatment and new information is entered into their existing health record; how information originally stemming from private and public health facilities or practitioners may be collected or accessed once the NHI

70 SAMA 2022 https://www.samedical.org/files/SAMA_Statement_Digital_Health_2022Mrch23.pdf3.

71 SAMA 2022 https://www.samedical.org/files/SAMA_Statement_Digital_Health_2022Mrch23.pdf3.

72 SAMA 2022 https://www.samedical.org/files/SAMA_Statement_Digital_Health_2022Mrch23.pdf2.

73 As several scholars have stressed, South Africa's challenge is not the absence of legal frameworks but their fragmentation and the lack of coordinated governance across national and provincial levels. Without strong leadership, adequate technical capacity and effective monitoring of processes, legal safeguards risk being undermined in practice. See Zharima, Griffiths and Goudge 2023 *Frontiers in Digital Health* 7; Katurura and Cilliers 2018 *African Journal of Primary Health Care and Family Medicine* 6; Weeks 2013 *Journal of Contemporary Management* 149.

EHR system is created; how the patient's right to access to his or her health information may be regulated so as to reduce the chances of serious harm being done by access to such information, as well as how issues of privacy, usability, actual accessibility and costs will be dealt with. Lastly, issues of record retention need clarification. Greater clarity on the issues mentioned and proper adherence to the regulatory framework would make a more effective NHI system possible.

The following recommendations are made for now. They are drawn directly from the regulatory gaps, overlaps and ambiguities identified throughout this article, and aim to create a cohesive legal and operational framework for EHRs under the NHI.

First, the *NHI Act* could be amended to expressly reference the Acts discussed in this article, to create an interlocking legislative framework for EHRs. This recommendation would respond to the fragmentation noted throughout this article, where it has been shown that the *NHI Act* itself provides minimal guidance on EHR governance. As things stand the *Constitution*, the *NHA*, the *POPIA*, the *PAIA*, the *ECTA*, the *Cybercrimes Act* and the *HPA* must be read together when implementing the NHI. Such interlocking references would clarify for HCPs, health establishments and regulators that compliance with the NHI is not merely a matter of administrative registration but requires adherence to constitutional rights, the protection mechanisms afforded in sections 15 to 17 of the *NHA*, the eight processing conditions of *POPIA*, and the authorisations under section 32 of *POPIA* for routine health data processing. If these references were to be embedded in the *NHI Act*, the legislation would become a statutory roadmap guiding practitioners through the otherwise disparate legal terrain, thus reducing the risk of inadvertent non-compliance.

Second, further amendments to the *NHI Act* could be made relative to EHR data governance, safeguards for (cloud-based) storage and inter-facility sharing, audit mechanisms for data access, and use and retention periods. Implementing this recommendation would directly address the technical and procedural silences identified in this article. The *NHI Act* currently leaves unresolved the issues of how health information will be stored, who may access it, under what circumstances and for how long. As discussed above, *POPIA* sets out processing conditions including security safeguards and retention limitations, but does not specify operational protocols for a national EHR system. It has also been noted that the *NHA* requires control measures to prevent unauthorised access, yet offers no detail on audit trails, encryption standards or disaster recovery, factors identified as key enablers of a functioning national EHR system. Amending the *NHI Act* to incorporate explicit provisions on data governance structures, technical standards for cloud storage, protocols for lawful inter-facility data sharing (aligned with

section 15 of the *NHA* and the further processing limitation in section 15 of *POPIA*), mandatory audit logs (to complement the *Cybercrimes Act* provisions discussed), and clear retention timelines would fill these gaps. Such amendments would operationalise the abstract legal principles into enforceable, practical rules. For example, clarifying that health records under the NHI must be retained indefinitely in de-identified form, as suggested by the HPCSA Guidelines, unless *POPIA*'s conditions for destruction apply, would resolve the tension between section 14 of *POPIA* and the HPCSA's guidance on indefinite retention.

Third, a dedicated national EHR policy framework could be developed by the NDoH to align technical standards with legal norms from all relevant statutes to ensure regulatory alignment. This recommendation builds on the regulatory complexity outlined throughout this article. As demonstrated, HCPs must navigate the *Constitution*, six major Acts and guidelines from the HPCSA and SAMA, all of which intersect but are not coordinated. It has been noted that the *Constitution* is the supreme law, requiring all other instruments to align with it; that the *NHA* governs access to and the protection of records but refers to *PAIA*'s outdated definition of personal information; and that *POPIA* now provides the controlling definition and processing framework, including the crucial section 32 authorisations for health data, yet leaves unresolved how the NHI should notify the IR when creating or updating records. This article has also highlighted *PAIA*'s distinction between public and private bodies, a distinction the NHI may collapse, and raised concerns about online access to EHRs without the intermediary safeguards *PAIA* requires. The article has further noted that the *ECTA* provides legal recognition for electronic records and retention requirements, and may categorise a national EHR system as a critical database - yet this has not been declared. The *Cybercrimes Act* has also been discussed and it has been noted that it criminalises EHR breaches but operates in parallel with *POPIA* and the *NHA*, creating potential overlap or gaps in enforcement. A comprehensive NHI-EHR policy framework, developed by the NDoH in collaboration with the IR, HPCSA, and relevant technical bodies, would synthesise these legal instruments into a single, coherent set of standards and procedures. This framework should specify:

- Consent protocols: reconciling section 11 of *POPIA* with the section 32 authorisations and the consent provisions in sections 15 and 16 of the *NHA*;
- Technical interoperability standards: addressing the *ECTA* retention and format requirements in section 16;
- Data minimisation and purpose specification rules: sections 9-14 of *POPIA*;

- Access control hierarchies: balancing section 32 of *PAIA* with section 17 of the *NHA* and sections 2-4 of the *Cybercrimes Act*; and
- Breach notification procedures: integrating *POPIA*'s reporting requirements with the *Cybercrimes Act* and SAMA's guidance.

Such a policy would transform the fragmented legal landscape into a unified governance model, enabling HCPs to comply with all relevant laws simultaneously rather than having to navigate them in isolation. This might be done with assistance from a multi-stakeholder group including the IR, HPCSA and NDoH to oversee the process from an ethical standpoint and to secure the implementation of EHRs. The establishment of such a body is a logical extension of the third recommendation and responds to the institutional coordination failures identified throughout the regulatory analysis in this article. The IR was established as the body responsible for enforcing *POPIA*, including its application to health data; the HPCSA issues binding guidelines on recordkeeping, consent, and confidentiality, which HCPs are ethically and professionally obligated to follow; and SAMA provides additional ethical guidance on digital health, including EHR security and patient rights. Yet these bodies operate independently, with no formal mechanism to align their standards or resolve conflicts. The NDoH, as the custodian of the NHI and the national EHR system, must coordinate with these regulators to ensure that legal compliance, professional ethics and technical implementation are harmonised. A multi-stakeholder oversight body could: develop and update the national EHR policy framework recommended above; adjudicate disputes over data access (such as those arising under sections 30 and 34 of *PAIA* or section 32 of *POPIA*); monitor compliance with the eight *POPIA* conditions and the *NHA* protection measures; issue binding interpretations on unresolved issues (such as whether the IR must be notified for each new EHR entry or whether the NHI will apply section 32(1)(b) of *POPIA* for risk assessment; and provide technical assistance to HCPs and health establishments in meeting their legal and ethical obligations. This body would embody the principle of accountability at a systemic level, ensuring that the national EHR system is implemented lawfully, ethically, and effectively.

Lastly, and this speaks to the aim of this article, guidance for practitioners should be issued to provide clarity on the scope and limits of data access, consent protocols, retention practices and the regulatory framework overall. This final recommendation addresses the gap in practical knowledge that motivated the writing of this article. As noted in the introduction, HCPs must be educated on the regulatory instruments governing EHRs to ensure that they practice lawfully and to prepare for the implementation of the NHI system. The present complexity of the framework, spanning constitutional rights, statutory obligations, criminal prohibitions and professional

guidelines, creates significant barriers to compliance. This article has demonstrated that HCPs must understand: when personal information (as defined in section 1 of *POPIA*) becomes special personal information (per section 26 of *POPIA*) requiring heightened protection; how the section 32 authorisations permit routine processing without renewed consent, yet do not override the initial consent requirement or confidentiality duties; when they may disclose information without consent under section 15 of the *NHA* or rely on public interest exemptions under section 37 of *POPIA*; how to comply with *PAIA*'s access request procedures while protecting patients from serious harm; what constitutes lawful retention under section 14 of *POPIA*, section 16 of the *ECTA*, and the HPCSA Guidelines' recommendation of indefinite storage; and how to protect EHRs from the criminal conduct proscribed by the *Cybercrimes Act*. Practical guidance documents, issued jointly by the NDoH, IR and HPCSA, should distil these complex legal provisions into clear, actionable protocols. These should include:

- Step-by-step consent templates covering initial consent, section 32 processing and withdrawal rights;
- Access control checklists operationalising section 17 of the *NHA* and sections 19-22 of *POPIA*;
- Decision trees for responding to access requests, implementing sections 30 and 34 of *PAIA*;
- Retention flowcharts reconciling *POPIA*, the *ECTA* and HPCSA standards; and
- Breach response protocols integrating *POPIA*, the *Cybercrimes Act* and SAMA guidance.

Such guidance would empower HCPs to navigate the regulatory framework confidently, reducing the risk of non-compliance and ultimately supporting the effective, lawful and ethical implementation of EHRs under the NHI.

By implementing these recommendations South Africa could transform its comprehensive but fragmented regulatory framework into a coherent, enforceable system that protects patient rights, enables effective healthcare delivery and supports the realisation of universal health coverage under the NHI. These recommendations are not abstract ideals but necessary steps to operationalise the constitutional mandates, statutory protections and professional ethics analysed throughout this article. Only through such integrated action could the promise of EHRs of improved continuity of care, enhanced data sharing and better health outcomes be realised without sacrificing the privacy, security and dignity of South African patients.

Bibliography

Literature

Cachalia and Klaaren 2022 *PELJ*
Cachalia F and Klaaren J "Digitisation in the Health Sector: A South African Public Law Perspective" 2022 *PELJ* 1-24

De Stadler *et al Over-thinking*
De Stadler E *et al Over-thinking the Protection of Personal Information Act: The Last POPIA Book You Will Ever Need* (Juta Cape Town 2021)

Katurura and Cilliers 2018 *African Journal of Primary Health Care and Family Medicine*
Katurura M and Cilliers L "Electronic Health Record System in the Public Health Care Sector of South Africa: A Systemic Literature Review" 2018 *African Journal of Primary Health Care and Family Medicine* 1-8

Prinsen 2023 *AJICL*
Prinsen L "Challenges to and Regulation of Telemedicine in South Africa" 2023 *AJICL* 204-227

Prinsen 2024 *Frontiers in Genetics*
Prinsen L "Introducing Dynamic Consent for Improved Trust and Privacy in Research Involving Human Biological Material and Associated Data in South Africa" 2024 *Frontiers in Genetics* 1-14

Roos "Data Protection"
Roos A "Data Protection Law in South Africa" in Makulilo A (ed) *African Data Privacy Laws* (Springer Cham 2016) 189-227

Swales 2022 *PELJ*
Swales L "The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock?" 2022 *PELJ* 1-32

Tsegaye and Flowerday "POPI Compliance"
Tsegaye T and Flowerday S "POPI Compliance Through Access Control of Electronic Health Records" Unpublished contribution delivered at *SAICSIT '19: Proceedings of the South African Institute of Computer Scientists and Information Technologists* (17-18 September 2019 Skukuza)

Weeks 2013 *Journal of Contemporary Management*
Weeks R "Electronic Health Records: Managing the Transformation from a Paper-Based to an Electronic System" 2013 *Journal of Contemporary Management* 135-155

Zharima, Griffiths and Goudge 2023 *Frontiers in Digital Health*
Zharima C, Griffiths F and Goudge J "Exploring the Barriers and Facilitators to Implementing Electronic Health Records in a Middle-income Country: A Qualitative Study from South Africa" 2023 *Frontiers in Digital Health* 1-12

Case law

Bernstein v Bester 1996 2 SA 751 (CC)

Centre for Child Law v Media 24 Ltd 2020 4 SA 319 (CC)

De Jager v Netcare Limited (42041/16) [2025] ZAGPPHC 141 (17 February 2025)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd 2001 1 SA 545 (CC)

Minister of Health of the Province of the Western Cape v Goliath 2009 2 SA 248 (C)

Minister of Health v Treatment Action Campaign (TAC) (No 2) 2002 5 SA 721 (CC)

Soobramoney v Minister of Health (KwaZulu-Natal) 1998 1 SA 765 (CC)

WB v RB 2024 4 SA 316 (KZD)

Legislation

Constitution of the Republic of South Africa, 1996

Cybercrimes Act 19 of 2020

Electronic Communication Transaction Act 25 of 2002

Health Professions Act 56 of 1974

National Health Act 61 of 2003

National Health Insurance Act 20 of 2023

Occupational Health and Safety Act 85 of 1993

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

Internet sources

Desfarges 2023 https://www.quicknews.co.za/2023/12/13/the-nhi-will-enforce-the-use-of-ehrs-resulting-in-a-steep-learning-curve-for-60-of-sas-gps/

Desfarges, A 2023 *The NHI Will Enforce the Use of EHRs – Resulting in a Steep Learning Curve for 60% of SA's GPs* https://www.quicknews.co.za/2023/12/13/the-nhi-will-enforce-the-use-of-ehrs-resulting-in-a-steep-learning-curve-for-60-of-sas-gps/ accessed 28 August 2025

HPCSA 2022 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf
Health Professions Council of South Africa 2022 *Guidelines for Good Practice in the Healthcare Professions: Guidelines on the Keeping of Patient Health Records (Booklet 9)* https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_9_Keeping_of_Patient_Records_Review-Draft_vSept_2022.pdf accessed 12 November 2025

HPCSA 2021 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_4_Informed_Consent_vDec_2021.pdf
Health Professions Council of South Africa 2021 *Guidelines for Good Practice in the Healthcare Professions: Seeking Patients' Informed Consent: The Ethical Considerations (Booklet 4)* https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_4_Informed_Consent_vDec_2021.pdf accessed 12 November 2025

HPCSA 2021 https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_5_Confidentiality_Protecting_and_Providing_Information_vDec_2021.pdf
Health Professions Council of South Africa 2021 *Guidelines for Good Practice in the Healthcare Professions: Confidentiality: Protecting and Providing Information (Booklet 5)* https://ethiqal.co.za/wp-content/uploads/2024/03/Booklet_5_Confidentiality_Protecting_and_Providing_Information_vDec_2021.pdf accessed 12 November 2025

Malcolm, Lyons and Brivik Inc 2019 https://www.lyonsbriviklaw.com/who-owns-patient-records-in-south-africa/
Malcolm, Lyons and Brivik Inc 2019 *Who Owns Your Patient Record in South Africa?* https://www.lyonsbriviklaw.com/who-owns-patient-records-in-south-africa/ accessed 6 August 2024

Moonsamy 2025 https://www.itweb.co.za/article/working-towards-a-single-electronic-health-record-for-sa/Pero37Z38KyMQb6m
Moonsamy W 2025 *Working Towards a Single Electronic Health Record for SA* https://www.itweb.co.za/article/working-towards-a-single-electronic-health-record-for-sa/Pero37Z38KyMQb6m accessed 28 August 2025

Prinsen 2024 https://theconversation.com/south-africas-national-health-insurance-bill-has-noble-aims-but-leaves-too-much-uncertain-it-needs-more-work-208604

Prinsen L 2024 *South Africa's National Health Insurance Bill has Noble Aims but Leaves Too Much Uncertain: It Needs More Work* https://theconversation.com/south-africas-national-health-insurance-bill-has-noble-aims-but-leaves-too-much-uncertain-it-needs-more-work-208604 accessed 6 August 2024

SAMA 2022 https://www.samedical.org/files/SAMA_Statement_Digital_Health_2022Mrch23.pdf
South African Medical Association 2022 *Statement on Digital Health* https://www.samedical.org/files/SAMA_Statement_Digital_Health_2022Mrch23.pdf accessed 6 August 2024

List of Abbreviations

AJICL	African Journal of International and Comparative Law
DC	Data Controller
DS	Data Subject
ECTA	Electronic Communication Transaction Act 25 of 2002
EHRs	electronic health records
HCPs	healthcare practitioners
HPA	Health Professions Act 56 of 1974
HPCSA	Health Professions Council of South Africa
IO	Information Officer
IR	Information Regulator
NDoH	National Department of Health
NHA	National Health Act 61 of 2003
NHI	National Health Insurance
NHI Act	National Health Insurance Act 20 of 2023
PAIA	Promotion of Access to Information Act 2 of 2000
PELJ	Potchefstroom Electronic Law Journal
POPIA	Protection of Personal Information Act 4 of 2013
SAMA	South African Medical Association