The Journal of Sustainable Development Law and Policy

ISSN: 2467-8406 (Print) 2467-8392 (Online) Journal homepage: https://www.ajol.info/index.php/jsdlp

Protecting the Patient's Data in the 21st Century Healthcare Industry: Is the African Continent Ready for the Digital Space?

Nkiruka Chidia Maduekwe

To cite this article: Nkiruka Chidia Maduekwe (2024). Protecting the Patient's Data in the 21st Century Healthcare Industry: Is the African Continent Ready for the Digital Space? The Journal of Sustainable Development, Law and Policy. Vol. 15:1. 206-237, DOI: 10.4314/jsdlp.v15i1.7

To link this article: DOI: 10.4314/jsdlp.v15i1.7

Received: 13 July, 2023;
Final Version Received: 15 September, 2023;
Published online: 30 January, 2024

PROTECTING THE PATIENT'S DATA IN THE 21ST CENTURY HEALTHCARE INDUSTRY: IS THE AFRICAN CONTINENT READY FOR THE DIGITAL SPACE?

Nkiruka Chidia Maduekwe PhD*

ABSTRACT

To ensure proper healthcare services and automation, including minimising medical errors and providing faster and more efficient healthcare, the medical field is experiencing innovative technological trends. They include automated patient records, hospital management system software, telemedicine, and the use of artificial intelligence devices. These innovations exist in more than just the global north, as they are slowly finding residence in African countries. Focusing on automated patient record, the article examines existing data protection legal frameworks in Africa to ascertain whether they provide effective remedy mechanisms patients can access should a breach occur. Taking cognisance of the current African Continental Free Trade Area Agreement (AfCFTA) aimed at creating a single market for goods and services; it is evident that healthcare services might have a continental approach. Thus, the article adopts a continental, regional, and national perspective. Using doctrinal method, the article compares the African Union Data Protection Convention with the European Union General Data Protection Regulation to draw lessons from the European Union Experience. The article finds that strengthened national mechanisms might provide the requisite

remedy mechanisms patients can access to ensure enforcement of their rights to data protection.

Keywords: healthcare system, data protection, electronic medical records, metadata, cyber security, SDGs, Agenda 2063, AfCFTA, African Union, ECOWAS, COMESA, EAC, SADC, automated patient record system

1. INTRODUCTION

Good health combines social, physical, and mental well-being, not just the absence of illness[1]. This definition highlights the intricate link between life and health, as health is life and life is wealth. This complicated link underscores healthcare practitioners and services' vital role in society. In addition to being internationally recognised as a fundamental human right,[2] both the Sustainable Development Goals (SDGs) Agenda 2030[3] – which is the global development blueprint – and the African Union (AU) Agenda 2063[4] – the continental development blueprint for Africa – highlight health as an

* LL. B (Abuja), B.L., LLM (Dundee), MSc. (Dundee), PGDip (Hull), PhD (Hull); Senior Research Fellow/Special Assistant to the Director General on Consultancy and International Relations Nigerian Institute of Advanced Legal Studies (NIALS), Supreme Court of Nigeria Complex, Three Arms Zone, FCT, Abuja. Email address: ncmaduekwe@yahoo.co.uk ORCID ID: 0000-0002-9726-6520

1 Preamble to the Constitution of the World Health Organisation – see World Health Organisation, 'Basic Documents' (49th edn, 2020) 1 <https://apps.who.int/gb/bd/pdf _files/BD_49th-en.pdf#page=7> accessed 12 July 2023.

2 Art 25 Universal Declaration of Human Rights, U.N. Doc. A/RES/217(III)A (Dec. 10, 1948) [hereinafter UDHR]; art 12 International Covenant on Economic, Social and Cultural Rights, U.N. Doc. A/RES/2200A(XXI) (Dec. 16, 1966); art 16 African (Banjul) Charter on Human and Peoples' Rights, O.A.U. Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982) (June 27, 1981).

3 U.N. GAOR 70th Sess., U.N. Doc. A/RES/70/1 (Sep. 25, 2015).

4 African Union, 'Agenda 2063: Framework Document, African Union' <https://au.int/sites/default/files/documents/33126-doc-framework_document_book.pdf> accessed 12 July 2023.

essential component to ensuring sustainable development and realising Africa, Africans want. SDG 3 seeks to "ensure healthy lives and promote wellbeing for all ages," Goal 3 of AU Agenda 2063 Aspiration 1 seeks to realise healthy and well-nourished African citizens by 2063. Both development blueprints are linked and aim to achieve the same objectives.[5]

Heralded as the new face of quality and efficient healthcare service and the basic block of eHealth,[6] automated patient records are rapidly replacing paper-based patient records.[7] According to the United States Institute of Medicine (IOM) Committee, automated patients record can reduce waste and assist in improving patient care [8] The automated patient record is a critical component of universal health care.[9] The IOM strongly recommended that healthcare professionals and organisations adopt automated patient record system as the

---

5 African Union, 'Agenda 2063 Linkages with Sustainable Development Goals, African Union' <https://au.int/sites/default/files/documents/33126-doc-07_linkage_with_the_ sdg.pdf> accessed 12 July 2023.

6 World Health Organisation, 'Global diffusion of eHealth: making universal health coverage achievable. Report of the third global survey on eHealth 100' <https://apps.who.int/iris/bitstream/handle/10665/252529/9789241511780-eng.pdf;jsessionid=CC249229D339E59B186CC71B83A29C7E?sequence=1> accessed 12 July 2023.

7 Gregory Makoul and others, 'The Use of Electronic Medical Records: Communication Patterns in Outpatient Encounters' (2001) 8 JAMIA 610, 610; Todd Swanson and others, 'Recent Implementations of Electronic Medical Records in Four Family Practice Residency Programs' (1997) 42 AM 607, 607; Lara Varpio and others, 'Working Off the Record: Physicians' and Nurses' Transformations of Electronic Patient Record-Based Patient Information' (2006) 81 AM S35, S35; Albert Boonstra and Manda Broekhuis, 'Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions' (2010) 10 BMCHSR 1, 1.

8 Richard S Dick, Elaine B Steen, and Don E Detmer (eds), Committee on Improving the Patient Record, Institute of Medicine, The Computer-Based Patient Record: An Essential Technology for Health Care (National Academy Press rev. ed. 1997) xi.

9 World Health Organisation, (n 6) 94.

"standard for medical and all other records related to patient care."[10]

Notwithstanding its far-reaching benefits, an automated patient records system draws the risk of exposing patients' confidential information to unauthorised persons through data thefts and cyber-attacks, thus, breaching patients' privacy. Hence, an automated patient records system highlights the need to protect the patient's data effectively. Even though health information technology originated in the global north, albeit slowly, there is a steady increase in adopting automated patient record systems in Africa.[11] As Africa moves towards ensuring a single and

---

10 Ibid 50.

11 Maxwell Oluwole Akanbi and others, 'Use of Electronic Health Records in sub-Saharan Africa: Progress and challenges' (2012) 14 JMT 1; Florence Femi Odekunle and others, 'Why sub-Saharan Africa lags in electronic health record adoption and possible strategies to increase its adoption in this region'(2017) 11 IJHS 59; Oluyemi E Adetoyi and Olayanju A Raji, 'Electronic health record design for inclusion in sub-Saharan Africa medical record informatics' (2020) 7 SA 1; Michael Kavuma, 'The Usability of Electronic Medical Record Systems Implemented in Sub-Saharan Africa: A Literature Review of the Evidence' (2019) 6 JMIRHF 1; Badeia Jawhari, 'Benefits and challenges of EMR implementations in low resource settings: a state-of-the-art review' (2016) 16 BMCMIDM 1; Victor Alangibi Kiri and Aaron C Ojule, 'Electronic medical record systems: A pathway to sustainable public health insurance schemes in sub-Saharan Africa' (2020) 27 NPMJ 1; Munyaradzi C Katurura and Liezel Cilliers, 'Electronic health record system in the public health care sector of South Africa: A systematic literature review' (2018) 10 AJPHCFM 1; RV Weeks, 'The implementation of an electronic patient healthcare record system: a South African case study' (2014) 11 JCM 101; Everleen Wanyonyi and others, 'Effectiveness of Security Controls on Electronic Health Records' (2017) 6 IJSTR 47; Chris Paton and Naomi Muinga, 'Electronic Health Records: A case study from Kenya' <https://pathwayscommission.bsg.ox. ac.uk/sites/default/files/2019-09/electronic_health_records.pdf> accessed 12 July 2023; Paula Braitstein and others, '"Talkin' About a Revolution": How Electronic Health Records Can Facilitate the Scale-Up of HIV Care and Treatment and Catalyze Primary Care in Resource-Constrained Settings' (2019) JAIDS <https://ghdonline .org/uploads/ JAIDS_supplement_AMRS_description_galleys_1.pdf> accessed 12 July 2023

liberalised market for goods and services,[12] this creates a massive potential for health information technology services such as automated patient records systems. The critical question is, how prepared is Africa to guarantee the protection of the metadata generated from this system?

Although existing legal frameworks indicate data security breach as a criminal offence which often attracts administrative penalties, the critical question is what happens to the data subject (the patient); who is the real victim? Apart from the criminal liability and the administrative penalties placed on the data processor or controller, what remedies are available to the patient whose data has been breached? Is the patient entitled to compensation? And if so, how effective is the redress mechanism?

Significantly, there needs to be more literature which examines redress mechanisms available to data subjects whose data privacy has been breached in Africa. Contributing to current research on data protection, this article examines existing data protection legal frameworks and policies in Africa from a continental, regional, and national perspective. The objective is to ascertain the existence of an effective redress mechanism through which such patients whose data privacy has been breached can efficiently access remedy. Note that the article is focused on redress mechanisms; as such, discussions on other data protection-related issues are outside the remit of this article. The article is further structured into four sections. Section Two gives a background on patient automated records. Section Three examines existing continental, regional, and national policies, and legal frameworks on data protection.

[12] African Union, 'Agreement Establishing the African Continental Free Trade Area (AfCFTA), <https://au.int/en/treaties/agreement-establishing-african-continental-free-trade-area> accessed 12 July 2023.

Section Four investigates the existing national redress mechanism while Section Five deals with the conclusion.

2. DEFINITION AND SCOPE OF AUTOMATED PATIENTS RECORD SYSTEM

Given that this article is focussed on automated patient record system, it is essential that the meaning and scope of this term within the context of this article is explicitly discussed. The patient record is the patient information a healthcare professional collates either directly from the patient or from an individual with personal knowledge of the patient.[13] Before automated patient records, this repository had always been paper-based.[14] The patient record can either be primary or secondary.[15] The primary record is "used by health care professionals while providing patient care services to review patient data or document their observations, actions, or instructions."[16] Conversely, "the secondary record stems from the primary record and provides aid to nonclinical users in supporting, evaluating, or advancing patient care."[17] The patient record system is a set of components that comprise avenues for creating, using, storing, and retrieving patient record, and this is domicile with the healthcare provider.[18]

As stated above, patients' records are paper based; however, as part of the innovations in health information technology, there is a rapid move to automated records. The paper-based record

---

13 Dick, Steen, Detmer (n 8) 55.
14 Ibid, 55; Makoul and others (n 7) 610.
15 Dick, Steen, Detmer (n 8) 55.
16 Ibid.
17 Ibid.
18 Ibid 56.

system is criticised as inadequate to meet the 21st-century healthcare system environment needs.[19] For example, in an emergency, healthcare practitioners are unable to access a patient's record in real time;[20] also, high incidences of the patient's paper record being lost and difficulty tracing the file,[21] illegible handwritten notes,[22] and consuming physical storage space that can be used for other health care service needs.[23]

Varied terms have been coined to describe non-paper patient records, namely, (i) "computer-based patient record,"[24] (ii) "computer-based medical record,"[25] (iii) electronic medical record,[26] (iv) electronic health record,[27] and (v) electronic

---

19 Edward H Shortliffe, 'The Evolution of Electronic Medical Records' (1999) 74 AM 414, 415; Astrid M. van Ginneken, 'The computerized patient record: balancing effort and Benefit' (2002) 65 IJMI 97, 97.

20 Dena E. Rifkin, 'Electronic Medical Records: Saving Trees, Saving Lives, (2001) 285 JAMA 1764, 1764

21 Wanyonyi and others (n 11) 47.

22 Ibid.

23 Boonstra and Broekhuis, (n 7) 2.

24 Dick, Steen, Detmer (n 8).

25 Randolph C Barrows and Paul D Clayton, 'Privacy, Confidentiality, and Electronic Medical Records' (1996) 3 JAMIA 139, 139.

26 Shortliffe (n 19); Swanson and others (n 7); Rifkin (n 20); Mohammed Sajedur Rahman and Christopher Kreider, 'Information Security Principles for Electronic Medical Record (EMR) Systems' (2012) AMCISP 2; Christopher C Tsai and Justin Starren, 'Patient Participation in Electronic Medical Records' (2001) 285 JAMA 1785; Charles Safran, 'Electronic Medical Records: A Decade of Experience' (2001)285 JAMA 1766; Troy R Mills and others, 'Electronic Medical Record Systems in Critical Access Hospitals: Leadership Perspectives on Anticipated and Realized Benefits'(2010) 7 PHIM 1; Boonstra and Broekhuis (n 7).

27 Lauren M Foster and others, 'Medical Student Use of Electronic and Paper Health Records During Inpatient Clinical Clerkships: Results of a National Longitudinal Study' (2018) 93 AM 514; Jeremy L Warner and others, 'It's Time to Wikify Clinical Documentation: How Collaborative Authorship Can Reduce the Burden and Improve the Quality of the Electronic Health Record' (2019) 94 AM 645; Christina E Milano and others, 'Simulated Electronic Health Record (Sim-EHR) Curriculum: Teaching EHR Skills and Use of the EHR for Disease Management and Prevention' (2014) 89 AM 399.

patient records.[28] Within the context of this article, the term automated patient record system is adopted and is broadly defined as using an electronic device or application software to create, manage, monitor, collect, and store primary and secondary patient records accessible to healthcare professionals, nonclinical users, and sometimes, the patient.

The advantages of automated patient records are indicated to include "instant (remote) access to patient information to all providers in the healthcare chain;"[29] saves healthcare providers' time;[30] eases communication between medical teams;[31] aids healthcare collaborations;[32] increases identification of high-risk patients;[33] reduces medication errors,[34] duplication of testing,[35] and time spent locating missing records.[36] These benefits, in effect, improve quality and continuity of care,[37] reduces cost,[38] and improve adherence to clinical practice guidelines[39] and implementation of patient care guidelines,[40] thus, ensuring comprehensive, consistent, and efficient delivery of health care services.[41] Another benefit is that automated patient records

---

28 Varpio and others (n 7); Mills (n 26); Boonstra and Broekhuis (n 7).
29 Boonstra and Broekhuis (n 7) 1.
30 Safran (n 26) 1766.
31 Boonstra and Broekhuis (n 7) 1; Tsai and Starren (n 26) 1765; Shortliffe (n 19) 415.
32 Safran (n 26) 1766.
33 Sheldon M Retchin and Richard P Wenzel, 'Electronic Medical Record Systems at Academic Health Centres: Advantages and implementation Issues' (1999) 74 AM 494, 494.
34 Varpio and others (n 7) S35; Retchin and Wenzel (n 33) 494.
35 Retchin and Wenzel (n 33) 494.
36 Ibid.
37 Siddharta G Reddy and others, 'Prevalence and Functionality of Electronic Health Records in Internal Medicine Continuity Clinics' (2010) 85 AM 1369; Retchin and Wenzel (n 33) 494; Boonstra and Broekhuis (n 7) 2.
38 Warner (n 27) 645; Milano (n 27) 399; Mills (n 26) 1.
39 Varpio and others (n 7) S35;
40 Retchin and Wenzel (n 33) 494.
41 Varpio and others (n 7) S35; Mills (n 26) 1.

provide valuable data for conducting clinical research as they aid in identifying patients who are eligible for a study[42] and improve resident and medical student clinical precepting.[43] In fact, according to Foster and others, using automated patient records is a critical skill medical students have to acquire in the 21st-century healthcare system environment.[44]

Notwithstanding these advantages, automated patient records increase the patient's exposure to a breach of privacy.[45] This is because, unlike paper-based records, at the click of a button, the patient's health data is easily accessible to unauthorised persons. According to the "Committee on Improving the Patient Record, Institute of Medicine,"

> [K]eeping computer-based records confidential and free from unauthorised access poses unique challenges, and a

---

42 Shortliffe (n 19) 415; Michael G Kahn and others, 'Configuration Challenges: Implementing Translational Research Policies in Electronic Medical Records' (2007) 82 AM; Retchin and Wenzel (n 33) 494.

43 Safran (n 26) 1766.

44 Foster and others (n 27) 514.

45 Shortliffe (n 19) 415; Julie D Cantor, 'Privacy Protections for Cybercharts: An Update on the Law' (2001) 285 JAMA 1767, 1767; Kenneth D Mandl and others, 'Public standards and patients' control: how to keep electronic medical records accessible but private' (2001) 322 BMJ 283, 284; Roderick Neame, 'Effective Sharing of Health Records, Maintaining Privacy: A Practical Schema' (2013) 5 OJPHI 1, 2-3 ; Dick, Steen, Detmer (n 8) 208-209; Wanyonyi and others (n 11) 47; Tatiana Ermakova and others, 'Antecedents of Health Information Privacy Concerns' (2015) 63 PCS 376; Shekha Chenthara and others, 'Privacy-Preserving Data Sharing using Multi-layer Access Control Model in Electronic Health Environment' (2019) 6 EAI 1; Mohamed Abdelhamid and others, 'Putting the Focus Back on the Patient: How Privacy Concerns Affect Personal Health Information Sharing Intentions' (2017) 19 JMIR <https://www.jmir.org/> accessed 12 July 2023; Natasha Singer, 'When Apps Get Your Medical Data, Your Privacy May Go With It' (The New York Times, 3 September 2019) <www.nytimes .com/2019/09/03/technology/smartphone-medical-records.html> accessed 12 July 2023; HIPAA Journal, 'January 2018 Healthcare Data Breach Report' (HIPAA Journal, 14 February 2018) <www.hipaajournal.com/january-2018-healthcare-data-breach-report/> accessed 12 July 2023.

failure to do so can have more onerous consequences than may occur in the case of paper records. The computer's capacity for collecting, storing, and permitting access to large quantities of information often means that more information is collected and stored on computer-based record systems than is collected and stored in paper records. Because of the computer's capacity for mass storage and copying, one breach of a system's security can result in the unauthorised disclosure of extensive information about large numbers of patients. In addition, the computer's capacity to provide health information on large numbers of patients at one time makes computer-based patient record systems an even more tempting target than paper records. This temptation will only increase as the medical information in patient records becomes more sophisticated (for example, genetic information).[46]

Automated patient records contain large volumes of sensitive personal health information, which are extremely valuable in the dark web, sometimes sold from $1,000 to $2,000.[47] This makes them a primary target for hacking and theft.[48] Examples of these security threats include malware,[49]

---

[46] Dick, Steen, Detmer (n 8) 214-215.

[47] Marianne Kolbasuk McGee, 'Research Reveals Why Hacked Patient Records Are So Valuable, Data Breach' <www.databreachtoday.com/interviews/research-reveals-hacked-patient-records-are-so-valuable-i-3341> accessed 12 July 2023; Thomas H.McCoy and Roy H Perlis, 'Temporal Trends and Characteristics of Reportable Health Data Breaches, 2010-2017' (2018) 320 JAMA 1282, 1282-1283; CBS News, 'Hackers are stealing millions of medical records – and selling them on the dark web' (CBS News, 14 February 2019) <www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/> accessed 12 July 2023; Mackenzie Garrity, 'Patient medical records sell for $1K on dark web' (Becker's Healthcare, (20 February 2019) <www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html> accessed 12 July 2023.

[48] McGee (n 47); Center for Internet Security, 'Data Breaches: In the Healthcare Sector' <www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/> accessed 12 July 2023; Norwich University, 'Healthcare Data Breaches - The Costs

ransomware,[50] encryption blind spots,[51] phishing attacks,[52] and denial-of-service (DDoS).[53] However, an effective security system is critical to avoid such breaches. Nonetheless, mechanisms for breaching these systems get more sophisticated by the day.[54] The pertinent question is, what remedy is available to such patients, and is there an efficient redress mechanism? The following section examines this subject matter.

---

and Solutions' <https://online.norwich.edu/academic-programs/masters /nursing/ resources/infographics/healthcare-data-breaches-the-costs-and-solutions > accessed 12 July 2023; Jay G Ronquillo and others, 'Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information' (2018) 1 JAMIAO 15; Mariya Yao, 'Electronic Medical Records Could Be Worth $1000 To Hackers' (Forbes, 14 April 2017) <www.forbes.com/sites/mariyayao /2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers /#49d79f4150cf> accessed 12 July 2023.

49 UIC, 'Cybersecurity: How Can It Be Improved in Health Care?' <https:// healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/> accessed 12 July 2023; Gerry Grealish, 'The top 5 cybersecurity threats hospitals need to watch for' (Becker's Healthcare, 20 June 2016) <www.becker shospitalreview.com/healthcare-information-technology/the-top-5-cybersecurity-threats-hospitals-need-to-watch-for.html> accessed 12 July 2023.

50 Infosec, 'Top Cyber Security Risks in Healthcare, Infosec' <https://resources .info secinstitute.com/top-cyber-security-risks-healthcare/#gref> accessed 12 July 2023; Center for Internet Security, 'Ransomware: In the Healthcare Sector' <www.cis ecurity.org/blog/ransomware-in-the-healthcare-sector/> accessed 12 July 2023; Grealish (n 49).

51 UIC (n 49); Grealish (n 49).

52 UIC (n 49); Grealish (n 49).

53 Center for Internet Security, 'DDoS Attacks: In the Healthcare Sector' <www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/> accessed 12 July 2023.

54 World Medical Association, 'WMA Statement on Cyber-Attacks on Health and Other Critical Infrastructure' (October 2016) <www.wma.net/policies-post/wma-statement-on-cyber-attacks-on-health-and-other-critical-infrastructure/> accessed 12 July 2023.

3. DATA PROTECTION AND PRIVACY LEGAL FRAMEWORKS AND POLICIES

Even though health information technology originated in the global north climes, these technologies are fast finding residence in Africa, more so, automated patient records. Thus, this article examines existing data privacy and protection legal frameworks in Africa to ascertain whether they provide efficient redress mechanisms for patients who might suffer health data privacy breaches. It is necessary to note that although an extensive examination of these legal frameworks and policies does not fall within the remit of this article as the objective is to broadly discuss what exists and whether there is a remedy mechanism. However, in discussing generally the regime existing in Africa, it is necessary to provide information on what broadly exists. Thus, the table below shows the existing data privacy and protection laws and policies at the continental, regional, and national levels in Africa.

DATA PROTECTION AND PRIVACY LAWS AND POLICIES IN AFRICA		
	Organisations	**Legal Instrument and Commentary**
Continental Framework	African Union	African Union Convention on Cybersecurity and Personal Data Protection. Came into existence on 27 June 2014. Only eight (8) countries have ratified the instrument. Requires fifteen (15) countries to enter into force. Not yet in force.
Regional Framework	Economic Community of West African States (ECOWAS)	Supplementary Act/A/SA.1/01/10/on Personal Data Protection. Adopted 16 February 2010. Supplementary Acts are binding on ECOWAS member states. Thus, the Act is in force.

	Southern African Development Community (SADC)	Model Law: Data Protection Act. Published in 2013.
	East African Community (EAC)	Draft Legal Framework for Cyberlaws. Developed November 2008
	Common Market for Eastern and Southern Africa (COMESA)	See Reports by COMESA Institutions: COMESA Business Council, Decision 123 (g) Official Gazette of the Common Market for Eastern and Southern Africa (COMESA), Volume 21 No. 1, 24 January 2018.

African countries with Data Protection and Privacy Law / Regulation

SN	Countries	Title of Law / Regulation
1.	Angola	Law 22/11 on Personal Data Protection. Enacted 17 June 2011.
2.	Benin	Benin has two legal frameworks that govern data protection, namely, (i) Law N° 2009-09 of May 22, 2009. Dealing with the protection of Personally Identifiable Information (PII). (ii) Loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin (Digital Code Act of Benin Republic).
3.	Burkina Faso	Loi n° 010-2004/AN Portant Protection des Données à Caractère Personnel. Enacted 20 April 2004.
4.	Cape Verde	Data Protection Act, Law 133/V/2001 of 22 January 2001. Supplemented and updated by "Lei n.° 41/VIII/2013. Enacted 17 September 2013.
5.	Chad	Law 007/PR/2015 on the Protection of Personal Data. Enacted 10 February 2015.
6.	Côte d'Ivoire	Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.
7.	Equatorial Guinea	Law 1/2016 (Data protection law), enacted 22 July 2016.
8.	Gabon	Loi n°001/2011 relative à la protection des données à caractère personnel.
9.	Ghana	Data Protection Act (Act No. 843) 2012. Came into force on 18 May 2012.

10.	Kenya	The Data Protection Act No. 24 of 2019. Enacted in November 2019.
11.	Lesotho	Data Protection Act 2012 No. 5 of 2012.
12.	Madagascar	LOI N° 2014 – 038 Sur la protection des données à caractère personnel. Enacted 9 January 2015.
13.	Malawi	Electronic Transactions and Cybersecurity Act No. 33 of 2016.
14.	Mali	Law No. 2013-015 of 21 May 2013 on the Protection of Personal Data.
15.	Mauritius	Data Protection Act 2017 No. 20 of 2017. Enacted 22 December 2017. Repeals and replaces the Data Protection Act 2004 No. 13 of 2004. Enacted 17 June 2004.
16.	Morocco	Law No. 09-08/2009 on the protection of people toward data protection of a personal nature
17.	Niger	Law No. 2017-28 of 3 May 2017 on the Protection of Personal Data.
18.	Nigeria	Nigeria Data Protection Regulation 2019.
19.	Sao Tome and Principe	Law No. 03/2016 on the Protection of Personal Data.
20.	Senegal	Loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel.
21.	South Africa	Protection of Personal Information Act 4 of 2013. Enacted 19 November 2013.
22.	Togo	Loi n° 2019-014 relative à la protection des données àcaractère personnel. Published 29 October 2019.
23.	Tunisia	Loi organique numéro 63 en date du 27 juillet 2004 portant sur la protection des données à caractère personnel.
24.	Uganda	The Data Protection and Privacy Act, 2019. Date of Presidential Assent 25 February 2019.
25.	Zambia	The Electronic Communications and Transactions Act, Act Number 21 of 2009. There is, however, a Data Protection Bill 2018, which, if passed, shall repeal, and replace the existing 2009 Act.

African countries with Draft Data Protection and Privacy Law / Regulation

SN	Countries	Title of Law / Regulation
1.	Botswana	Data Protection Act 2018 No. 32 of 2018. (Not yet enforced. Awaiting Order by the Minister as to date Act shall come into operation)

2.	Egypt	Data Protection Draft Law.
3.	The Gambia	Draft Data Protection and Privacy Policy and Strategy, 2019.
4.	Seychelles	Data Protection Act 2003. (Not yet in force. Still awaiting Minister's notice in the Gazette when it shall come into operation).
5.	Swaziland	Data Protection Bill.
6.	United Republic of Tanzania	Data Protection Bill 2013.
7.	Zimbabwe	Has revised ICT Policy which provides for the enactment of data protection and privacy. There is currently a "Draft Data Protection Bill 2016."

3.1 Continental Framework

The African Union adopted its Convention on Cybersecurity and Personal Data Protection in 2014.[55] Noting the absence of a specific legal framework which protects consumers' data[56] and the major challenge of establishing a balance between protecting personal data and privacy,[57] also developing electronic commerce and the Knowledge Economy in Africa.[58] The AU Convention provides "the security rules essential for establishing credible digital space"[59] to protect "the privacy of citizens in their daily or professional lives…while guaranteeing the free flow of information."[60]

The AU Convention explicitly defines relevant terms: "the data controller, the data subject, health data, personal data, personal

---

55 African Union Convention on Cyber Security and Personal Data Protection <https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.> accessed 12 July 2023. Hereinafter AU Convention.

56 Ibid preamble.

57 Ibid.

58 Ibid.

59 Ibid.

60 Ibid.

data file, processing of personal data, and the third party."[61] The AU Convention mandates State Parties to establish data protection legal frameworks[62] and authority in charge.[63] Part of the duties of the national authority is "entertaining claims, petitions, and complaints regarding the processing of personal data and informing the authors of the results."[64] Also, "impose administrative and monetary sanctions on data controllers."[65] Besides, the authority must "speedily inform the judicial authority of certain types of offences that have come to their attention."[66]

As indicated in its preamble, the AU Convention seeks to provide a template for African Union Member states to establish an effective cybersecurity and data protection mechanism. Hence, the focus is on actions to be taken at the national rather than the continental level. This is highlighted in section II of the AU Convention, which, even though it states, Institutional Framework for the protection of personal data, makes it clear that this institutional framework refers to National Data Protection Authorities.[67]

Even though the AU Convention does not provide a continental mechanism through which African Union Member State citizens can seek and obtain redress for breach of data privacy, the AU Convention provides a valuable template that African countries can adopt in creating national data protection legal framework.

---

61 Ibid art 1.
62 Ibid art 8.
63 Ibid art 11.
64 Ibid art 12 para 2 (e).
65 Ibid art 12 para 2 (h).
66 Ibid art 12 para 2 (f).
67 Ibid art 11.

3.1.1 Comparison: The AU Convention on Cybersecurity and Personal Data and the European Union General Data Protection Regulation, Directive 95/46/EC

The comparison focuses on the redress mechanisms available to patients whose data privacy has been breached.

Adopted in 2016, the European Union General Data Protection Regulation (EU GDPR) repeals the EU Directive 95/46/EC (General Data Protection Regulation),[68] which protects how personal data is processed and regulates its free movement.[69] Like the AU Convention, the EU GDPR provides for national data protection authorities, called supervisory authorities.[70]

However, unlike the AU Convention, which is silent regarding the data subject's right to seek judicial remedy should a breach occur, the EU GDPR extensively provides for this. Chapter VIII of the EU GDPR provides remedies, liability, and penalties. Article 77 of the GDPR gives the data subject the right to administrative redress and mandates the supervisory authority to provide the data subject progress updates on the compliant made, including the option of judicial remedy. Also, the data subject has the right to seek judicial remedy against the supervisory authority where it fails to handle the complaint or fails to within three provide the data subject with update on the progress and outcome of the compliant.[71]

---

68 Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing EU Directive 95/46/EC (General Data Protection Regulation). [Hereinafter EU GDPR].

69 Ibid art 1.

70 Ibid art 4 para 21.

71 Ibid art 78.

In addition to the administrative remedy, the data subject has the right to seek judicial redress against the data controller or processor.[72] The proceedings shall be instituted "before the courts of the EU member state where the controller or processor has an establishment or where the data subject has a habitual residence."[73] The exception is where the "controller or processor is a public authority of a member state acting in the exercise of its public powers."[74]

Besides, the administrative fine which the "supervisory authority has the power to impose,"[75] "[a]ny person who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to receive compensation from the controller or processor for the damage suffered."[76] Where administrative fines are absent from a member state's legal system, the supervisory authority has the discretion to apply Article 83 to initiate the imposition of this fine through the competent national court.[77]

Given the focus of this article on redress mechanisms for the data subject (patient), it is evident that when compared with the EU GDPR, the AU Convention lacks an elaborate redress mechanism. The data subject can only complain to the National Authority, which can adopt several sanctions, such as issuing a warning, imposing a monetary fine or temporary or permanent withdrawal, and so on.[78] However, there is to time limit within which the National Authority is mandated to undertake these actions. Also, the data subject has no judicial remedy against a

---

72 Ibid art 79.
73 Ibid art 79 para 2.
74 Ibid.
75 Ibid art 58 para (i) and art 83.
76 Ibid art 82 para 1.
77 Ibid art 83 para 9.
78 Art 12 AU Convention (n 55).

lackadaisical National Authority that fails to take up the complaint.[79]

Given the absence of these explicit provisions on remedies, liabilities, and penalties in the AU Convention, this article recommends that African States may choose to borrow these provisions from the EU GDPR and reflect them in their national legal framework. Therefore, this article adopts the EU GDPR as the template to examine what constitutes an efficient redress mechanism. This is because the "data subject has the right to judicial and non-judicial redress against the processor and controller" and has judicial redress against the data protection authority. This checks the data protection authority, ensuring it fulfils its duty to the data subject.

3.2 Regional Framework

Concerning regional framework, the Economic Community of West African States (ECOWAS) has a Supplementary Act on Data Protection,[80] Southern African Development Community (SADC) has a model law,[81] the East African Community (EAC) is in the draft stage,[82] and that of the Common Market for Eastern and Southern Africa (COMESA) stems from a Decision of its Business Council.[83]

---

79 Art 78 para 2 EU GDPR (n 68).

80 Economic Community of West African States (ECOWAS) Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (Feb. 16, 2010). [Hereinafter ECOWAS Supplementary Act].

81 Southern African Development Community (SADC) Data Protection Model Law (2013). [Hereinafter SADC Model Law].

82 Draft EAC Legal Framework for Cyberlaws (Nov. 2008). [Hereinafter EAC Draft Framework].

83 Official Gazette of the Common Market for Eastern and Southern Africa (COMESA), Vol. 21, No. 1 (Jan. 24, 2018). [Hereinafter COMESA Official Gazette].

The EAC Draft Framework briefly explains the meaning of data protection within the context of the framework, entities to which it would apply, obligations of the data processor, and the establishment of a data protection authority.[84] The draft is a work in progress and indicates the need for further work to be carried out on data protection and privacy.[85] The COMESA document calls on member states to be aware of the EU GDPR and "its impact on businesses and stakeholders doing business with EU firms."[86] Also, for member states to establish national data protection legislation and data protection authorities.[87]

Adopted in 2010, the ECOWAS Supplementary Act mandates "each member state to establish a data protection legal framework"[88] and data protection authority. [89] The ECOWAS Supplementary Act shares similar provisions with the AU Convention, more so failing to explicitly provide for the right of the data subject to judicial and non-judicial remedies, the monetary fines that shall be imposed on the defaulter, and the extent of liability.

In 2013, SADC published a model law for member countries.[90] In addition to establishing a data protection authority,[91] the Model Law "explicitly provides for the data subject's right to pursue legal appeals with the relevant judicial authorities."[92] This is, however, subject to exhausting the appeal offered through the data protection authority.[93] The Model Law is

84 s 2.5 EAC Draft Framework (n 82) 17-18.
85 Ibid 18.
86 Decision 123 COMESA Official Gazette (n 83) 37.
87 Ibid.
88 Art 2 ECOWAS Supplementary Act (n 80).
89 Ibid art 14.
90 SADC Model Law (n 81).
91 Ibid prt III.
92 Ibid prt VIII.
93 Ibid.

intended to serve as a template that SADC member countries can adopt and adapt.[94]

Compared with the AU Convention, the explicit provision on judicial recourse in the SADC Model Law is a welcomed addition. However, unlike the EU GDPR, this is limited to having exhausted the appeals at the data protection authority. The SADC Model Law also does not provide for the right of the data subject to judicial redress against the data protection authority should it delay in providing redress.

3.3 National Framework

Having discussed continental and regional frameworks, what subsists leaves much to be desired regarding providing redress mechanisms. Also, these frameworks all point towards the national level. Thus, it can be argued that Africa's data protection redress mechanism is only as good as what exists at the national level. This subsection examines the data protection legal framework in three selected African countries, namely, South Africa, Nigeria, and Kenya, to ascertain whether they provide an effective redress mechanism for a patient whose data privacy has been breached. The justification for selecting these countries is based on the shared common law history, and they represent the largest economies in their regions.[95]

3.3.1 South Africa

The Protection of Personal Information Act 4 of 2013[96] recognises the Constitutional provision on the right to privacy.

---

94 Ibid preamble.

95 World Bank, 'Overview' <www.worldbank.org/en/region/afr/overview> accessed 12 July 2023; Dominic Omondi, 'Kenya regains position as region's biggest economy' (The Standard, 23 February 2020) <www.standardmedia.co.ke/business/article/2001361459/kenya-regains-position-as-region-s-biggest-economy> accessed 12 July 2023.

96 Hereinafter POPIA 2013.

It explicitly delineates it to include "the right to protection against the unlawful collection, retention, dissemination and use of personal information."[97] Even though POPIA 2013 received Presidential assent on 19 November 2013,[98] commencement has been in batches. Thus, while section 1, 112, 113, and Part A Chapter 5 commenced on the 11th of April 2014, the other section – except section 110 and 114(4) – started on the 1st of July 2020.[99]

Chapter 10 of the POPIA 2013 extensively provides for its enforcement. In addition to lodging a complaint with the Regulator,[100] the data subject has the discretion to "institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act[101]…whether or not there is intent or negligence on the part of the responsible party."[102] The Act "defines 'responsible party' to mean a public or private body or any other person who alone or in conjunction with others, determines the purpose of and means for processing personal information."[103] The Regulator also has the discretion to "institute a civil action against the responsible party at the request of the data subject."[104] The court has the discretion to award an amount that is "just and equitable, and this includes compensation for

---

97 Ibid preamble.

98 Protection of Personal Information Act (POPI Act) <https://popia.co.za/> accessed 12 July 2023.

99 Id.

100 s 74 POPIA 2013, supra note 98.

101 Relates to interference with protection of personal information of data subject – see id., at s73.

102 Ibid s 99 (1).

103 Ibid s 1.

104 Ibid s 99(1).

patrimonial and non-patrimonial loss suffered by the data subject, aggravated damage, interest, and cost of suit."[105]

It is important to note that even though "any person may submit a complaint to the Regulator alleging interference with the protection of the personal information of a data subject,"[106] the Regulator has the discretion not to take action on the complaint.[107] The reasons include where the complainant has no sufficient personal interest in the subject matter of the complaint[108] or where "the length of time that had elapsed between the date when the subject matter arose, and the date the complaint was made is such that an investigation of the complaint is no longer practicable."[109] The Regulator must inform the complainant of its decision not to take action and its reasons.[110]

Bearing in mind the stated objective of this article, which is to ascertain an effective redress mechanism, it can be argued that the South Africa POPIA 2013 does provide a feasible redress mechanism through which the patient whose personal information has been interfered with can institute a civil action against the responsible party and receive compensation for the infringement.

3.3.2 Nigeria

Developed in furtherance of its mandate as stipulated in the National Information Technology Development Agency (NITDA) Act of 2007, the NITDA Nigeria Data Protection

---

105 Ibid s 99(3).
106 Ibid s 74(1).
107 Ibid s 77.
108 Ibid s 77(1)(e).
109 Ibid s 77(1)(a).
110 Ibid s 77(3).

Regulation 2019[111] seeks to, amongst others, "safeguard the rights of natural persons to data privacy."[112]

Where a data privacy breach occurs, the data controller is liable to a fine in addition to any criminal liability.[113] The NDPR 2019 explicitly mandates NITDA to convene an administrative panel to investigate allegations of any breach and invite any party to respond to the allegation within seven days.[114] The duration of the investigation and determination of the appropriate redress is stated as within 28 working days.[115] The NDPR 2019, however, is silent regarding the procedure for submitting a complaint, the timeline for the investigation, compensation to the data subject, and the redress mechanism where the Agency fails to conduct the investigation.

Nevertheless, it is good to note that the data subject has the right to seek redress in a court of competent jurisdiction.[116] Given that Nigeria has both State High Courts and a Federal High Court, the pertinent question is, which can be considered the court with competent jurisdiction?

Notwithstanding the above, given the focus of this article, the NDPR 2019 might provide a tool which the data subject can use to seek redress at the court. Unlike the legal frameworks discussed above, NDPR 2019 uniquely defines personal data to include medical information.[117] This limits confusion as to what personal data breach means.[118]

---

111 Hereinafter NDPR 2019.
112 Ibid reg 1(a).
113 Ibid reg 2.10.
114 Ibid reg 3.2.
115 Ibid reg 3.2.1 (d).
116 Ibid reg 3.2.1.
117 Ibid reg 1(q).
118 Ibid reg 1(s).

3.3.3 Kenya

Enacted in November 2019, the Data Protection Act, No. 24 (2019), Kenya Gazette Supplement No. 181,[119] seeks to, amongst others, protect individuals' privacy and provide remedies to protect their data.[120] To this end, the DPA 2019 makes provision for "a data subject who has been aggrieved by a decision of any person under the Act"[121] to lodge a complaint with the Data Protection Commissioner,[122] who is empowered by the DPA 2019 to conduct investigations on the complaint.[123] The Commissioner is mandated to investigate and conclude the matter within ninety days.[124] Where the Commissioner finds that a person has failed or is failing to comply with the DPA 2019, the Commissioner has the discretion to serve such person an enforcement notice.[125] "Failure to comply with the enforcement notice is an offence which upon conviction attracts a fine of not more than five million shillings or a term of not more than two years or both."[126] In addition to the above, the data subject is "entitled to compensation for the damage caused by the data controller or processor."[127] Damage includes financial loss and non-financial loss, such as distress.[128]

Given the focus of this article, it is evident that the DPA 2019, to some extent, provides a redress mechanism that can be utilised by a patient whose data privacy has been breached. However, the DPA 2019 is silent on specific issues, namely,

---

119 Hereinafter DPA 2019.
120 Ibid s 3(c)(e).
121 Ibid s 56(1).
122 Ibid s 5(1).
123 Ibid s 9(1)(a).
124 Ibid s 56(5).
125 Ibid s 58(1).
126 Ibid s 58(3).
127 Ibid s 65(1).
128 Ibid s 65(4).

what happens when the Commissioner does not issue an enforcement notice having found the data controller or processor liable to the complaint? Also, who enforces the compensation, the Commissioner, or the court? Additionally, the data subject is restricted to the administrative mechanism and does not have the option of judicial redress. Thus, the DPA 2019 requires further improvement.

4. USING HUMAN RIGHTS APPROACH TO ENSURE EFFICIENT PROTECTION OF PATIENT DATA

Partnering and alliancing methods are relatively new methods which emphasise on collaboration between project stakeholders.

Having examined the existing continental, regional, and selected national legal frameworks, it is apparent that there remains a specific deficiency, and these frameworks may need to holistically provide an adequate mechanism through which a patient can seek redress for a breach of data privacy. The pertinent question is, what mechanism best provides this platform?

Interestingly, the right to privacy is recognised as a fundamental human right. Article 12 of the Universal Declaration of Human Rights (UDHR) states that "no one shall be subjected to arbitrary interference with his privacy…Everyone has the right to the protection of the law against such interference or attacks."[129] This right is echoed in Article 17 of the International Covenant on Civil and Political

[129] UDHR (n 2).

Rights (ICCPR) 1966.[130] Although this right is absent in the African Charter on Human and Peoples' Rights (the Banjul Charter), it is reflected in the Constitution of several African States – specifically, the selected countries discussed in this article. Thus, this article proposes that the human rights approach might provide an efficient redress mechanism through which a patient can seek redress for infringing their right to data privacy.

Per section 14 of the Constitution of the Republic of South Africa Act, 1996, "everyone has the right to privacy,"[131] and this includes "the right not to have – the privacy of their communications infringed."[132] The Constitution, Article 31 (2010) (Kenya) is the same as the South African provision. Section 37 of the Constitution of Nigeria (1999) (as amended) guarantees and protects the privacy of the Nigerian citizen.

The South African and Kenya constitutions recognise public interest litigation in enforcing the right to privacy.[133] Anyone alleging that the right to privacy has been infringed, denied, violated, or threatened has the right to approach a court for redress,[134] which includes the declaration of rights as an appropriate relief.[135] For Kenya, appropriate relief includes, amongst others, a "declaration of rights, injunction, order for compensation."[136]

---

130 International Covenant on Civil and Political Rights, U.N. Doc. A/RES/2200A(XXI) (Dec. 16, 1966).
131 S. Afr. Const., 1996.
132 Ibid s 14(d).
133 s 38(d) S. Afr. Const., 1996; Constitution, art. 22(2)(c) (2010) (Kenya).
134 s 38 S. Afr. Const., 1996; Constitution, art. 22(1) (2010) (Kenya).
135 s 38 S. Afr. Const., 1996.
136 Constitution, art. 23(3) (2010) (Kenya).

In Kenya, the High Court is empowered to determine the question as to the denial, violation, infringement, or threat to the right to privacy.[137] In South Africa, the Constitutional Court is the designated court having jurisdiction in all constitutional matters,[138] which "includes any issue involving the interpretation, protection or enforcement of the Constitution."[139]

In Nigeria, the Fundamental Rights (Enforcement Procedure) Rules 2009[140] provides the framework for enforcing fundamental rights in Nigeria. The FREP Rules 2009 mandates the "court to encourage and recognise public interest litigation"[141] and "no human rights case is dismissed or struck out for want of *locus standi*."[142] The federal and state high courts have the jurisdiction to entertain human rights infringement matters.[143]

Unlike tort claims, the human rights approach in Nigeria provides a cheaper, faster, and more straightforward route. The courts have described the procedure as being in a class of its own, *sui generis*.[144] The applicant does not need the leave of the court;[145] there is no limitation of time within which to apply;[146] hearing of the application takes seven days from the day

---

137 Ibid art. 23(1).
138 s 167(3)(a) S. Afr. Const., 1996.
139 Ibid s 167(7).
140 Hereinafter FREP Rules 2009.
141 Ibid preamble para 3(e).
142 Ibid.
143 Ibid ord I r 1.
144 Luke Loveday v The Comptroller of Prisons Federal Prisons Aba & ors (2013) LPELR-22072 (CA) 38-39, paras E-A.
145 FREP Rules 2009 (n 140) ord II r 2.
146 Ibid ord III r 1; Mr James Olusegun Omoleye v Francis Oginni Olaniran & others (2010) 10 NMLR 460-461 para 11.

filed;[147] the infringement can be filed against the government, natural and artificial person,[148] common law principles on the award of damages do not apply;[149] infringement attracts the award of exemplary damages, compensatory damages, and a written apology.[150]

Given its simple process, legal practitioners used to torts applications often do not avert their minds to the essential procedure requirement, which could make or mar the success of the FREP Rules 2009 application. To succeed, the application must demonstrate the infringement or likely infringement of the fundamental rights.[151] The application must specify which fundamental rights are likely to be infringed.[152] The application cannot be based on a tort claim and cannot combine human rights and torts.

Notwithstanding data protection legal frameworks in South Africa, Kenya, and Nigeria, this article argues that the human rights approach might provide an effective mechanism for a patient whose data has been breached to access and receive redress. Take, for instance, Nigeria; a comparison of the current framework and the FREP Rules 2009 shows a more robust mechanism. Indigent patients who lack funds to access the courts can do so through civil society organisations that

---

147 FREP Rules 2009 (n 140) ord IV r 1.

148 Alhaji Ibrahim Abdulhamid v Talal Akar & anor (2006) 1449-1450 NSCQR Vol 26.

149 Gabriel Jim-Jaja v Commissioner of Police Rivers State & ors (2012) 363 NSCQR Vol 52; Jide Arulogun v Commissioner of Police Lagos State & Ors (2016) LPELR-40190 (CA) 13-14, paras A-A.

150 Oliver Iwununne v Morris Egbuchulem & Ors (2016) LPELR-40515 (CA) 37-38, paras D-F; Jide Arulogun v Commissioner of Police Lagos State & Ors (2016) LPELR-40190 (CA) 20-21 paras D-B.

151 Faith Okafor v Lagos State Government & anor (2016) LPELR-41066 (CA) 28 paras D-F

152 Ibid 28-29, paras F-C.

may choose to take the matter in the public interest. Also, there is no limitation of time as to when to file the process.

5. CONCLUSION

The 21st-century healthcare system is rapidly evolving with the introduction of health information technology. The African continent is not left behind as countries adopt eHealth mechanisms such as automated patient records systems to ensure the realisation of universal healthcare. Even with the positive benefits of an automated patient records system, given these systems' interconnectedness (internet or intranet), vast amounts of health information are at risk of being stolen or hacked. Over the past few years, the healthcare system has witnessed a steady increase in cybersecurity breaches such as theft and hacking, leaving patients and healthcare providers needing help deciding the best ways to protect health data.

Even though strengthened security systems are identified as paramount to protecting the patient from data privacy breaches, given the increase in the use of this technology and the high value of stolen health information in the dark web, it is evident that the healthcare system would continue to deal with data theft and hacking. Thus, the pertinent question is what redress mechanism is available to patients whose data privacy has been breached?

This article examines the existing legal frameworks in Africa from a continental, regional, and national perspective. The article compares the AU Convention with the EU GDPR and finds that the EU GDPR has a more elaborate redress mechanism that African countries may adopt. Using this template, the article finds that the African continental and

regional frameworks need to be revised. Also, that data protection is focused on the national level. The article finds that even though the selected national frameworks provide a redress mechanism, there is still room for improvement. The article proffered that using a human rights approach might provide an efficient mechanism for patients to seek redress for a data breach. So in answer to question as to whether Africa is ready for the digital space with regards to the healthcare system, given the number of African countries yet to enact a data protection legal framework, this article recommends that African countries may choose to borrow a leaf from the EU GDPR and adopt its elaborate redress mechanisms.