Global Journal of Politics and Law Research
Vol.7, No.3, pp.88-101, April 2019
Published by European Centre for Research Training and Development UK (www.eajournals.org)

IN THE AGE OF TECHNOLOGY: LEGAL PROTECTION FOR PERSONAL HEALTH INFORMATION IN NIGERIA

Dr Bernard Oluwafemi Jemilohun

Faculty of Law, Ekiti State University, Ado-Ekiti, Nigeria

Oluwadara Oluwaseun Ajidasile

Federal Polythechnic, Ile-OlujiOndo State

ABSTRACT*:* *The need to protect the personal health information of individuals has become a global phenomenon. This is based on the duty of confidentiality that healthcare providers owe patients in general of which Nigeria is not an exception. Gradually, doctors and health workers have begun to embrace electronic record keeping of patients' records and the old case note is giving way to electronic forms of record and storage. Thus, personal health information has become another type of electronically stored information that is capable of processing and manipulation by computers. This paper appraises the state of personal health information protection under Nigerian law by looking at the legislative provisions that guarantee protection for personal data especially in the healthcare sector. It examined the constitutional guarantee of the right to privacy, the National Health Act, 2014 and the Nigeria Data Protection Regulations, 2019. A brief attempt was made to look at the legal basis for data protection in the United Kingdom and also a peek into the United States Health Insurance Portability and Accountability Act. The paper observed in a conclusion that the laws appear to be a good start up towards the security of personal health information*

KEY WORDS: Data Protection, Healthcare, Personal Health Information, Confidentiality, Technology.

INTRODUCTION

It has always been the case that doctors and other health workers need to document the medical history of their patients, their drugs, prescriptions and observations.[1] This is largely done by writing what is known as case notes and mostly kept in files where other medical personnel can access the same for continuing treatment especially in cases where more than one doctor or health worker attends to the patient. The health status or condition of such patient becomes a body of information that the doctor or health worker may not have had or had access to if not

[1]Ijeweme Odiawa, (2017) *Electronic Health Records (EHR): the death of the case note as we know it*? https://digitalhealth.com.ng/2017/03/09/electronic-health-records-ehr-the-death-of-the-case-note-as-we-know-it accessed on 06/04/2019

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

for the doctor/patient relationship that comes into being by virtue of the patient's accessing the healthcare facility where the doctor practices.

The common law has always put a doctor under a duty of confidentiality[2] with respect to the health status or condition of his patient even where there is no specific contractual duty to respect the confidence of his patient.[3] The legal principle undergirding this is based on the doctor-patient relationship being characterised as one of a fiduciary nature. It has even been suggested that the scope of the duty covers both information received directly and the ones received indirectly so far as they are received in the doctor's position as the patient's doctor.[4] In the words of Lord Goff, "…a duty of confidence arises when confidential information comes to the knowledge of a person (the confidant) in circumstances where he has notice or is held to have agreed that the information is confidential, with the effect that it would be just in all the circumstances that he should be protected from disclosing the information to others."[5]

And in the words of Lord Riddel, "A doctor being in a fiduciary capacity must preserve his patient's confidence unless relieved from the obligation by some lawful excuse of legal compulsion, the patient's consent, the performance of a moral or social duty or protection of the doctor's interest. A doctor shares with other citizens the duty to assist in the detection and arrest of a person who has committed a serious crime. Everyone recognises the necessity and importance of medical confidence, but we must recognise also that the rules regarding them exist for the welfare of the community and not for the aggrandisement or convenience of a particular class. We must recognise also that they must be modified to meet the inevitable changes that occur in the necessities of various generation"[6]

It is worth noting that this duty of confidentiality is not breached by private discussions with colleagues or other healthcare personnel in the course of treatment of the patient, but this may require the consent of the patient which may be waived by the patient. On the other hand, a doctor may be required by law to make disclosure, in which case, there will be no breach of the duty of confidentiality.

Electronic Record-Keeping

As pointed out above, before the advent of technology, record taking and keeping in the medical sector was largely documentary and as with similar records, they were paper based. Such records could be kept under lock and key and except for intrusions by criminally minded people, unauthorised access to such records was rare. Thus, whilst a doctor may record accurately and in detail, information gotten from patients about patients, such case notes and records may be used in the course of treatment of the patient and kept in the records of the healthcare institution without the fear of such information being taken and used by a third party and thereby causing liability for the doctor or the healthcare institution.

[2] Festus O. Emiri, (2012) *Medical Law and Ethics in Nigeria*, Lagos: Malthouse Press. p. 353
[3] *Attorney-General v. Guardian Newspapers Ltd*. (No 2) [1990] 1 AC 109, [1988]3 All ER 545 There exists a public duty to protect confidential information
[4] Kennedy & Grubb, Medical Law 2nd ed. London: Butterworths 1994 at 639-410
[5] *Supra* Note 2
[6] Lord Riddel, (1929) *Medico-Legal Problem*, London, Lewis & Co Ltd

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

In the age of technology, virtually every form of information and record is capable of being stored electronically. And because of the advances in information communication technology generally, large volumes of information can be transferred deliberately or inadvertently at the click of a button. The possibilities that come with this are numerous. Just as information can be shared with intended recipients for positive and productive uses, the same can be inadvertently shared with the wrong persons and the uses that personal medical information may be put to by a criminally minded person are better imagined than experienced.

However, it is worth noting that electronically recorded information can be more legible than handwritten records and thus are safer from medical errors.[7] They also have the capacity for more durable preservation than paper-based records. Further, electronic health records systems are designed to store data accurately and to capture the state of a patient across time. It eliminates the need to track down a patient's previous paper medical records and assists in ensuring data is accurate and legible. It can reduce risk of data replication on paper as there is only one modifiable file, which means the file is more likely up to date, and decreases risk of lost paperwork.[8]

With information or patients records as mentioned above being stored electronically in healthcare establishments (either because they have large patient records or have chosen to go digital because they understand the benefits that come with an electronic health database system), comes the need to identify the rules governing the protection of such information and preventing the same from abuse in the society. This is more so in the light of the possibility of healthcare providers and practitioners outsourcing their ICT needs and record-creation and electronic storage to non-medical persons. And the fact that medical personnel contract their electronic storage system to outsiders may not exclude them from liability for personal health data security breaches.

The concept of data protection or informational privacy has for quite a while become a matter for global concern. From industry regulations to national legislations and regional conventions and directives, data protection has taken a front burner position. This is made more so by reason of advancements in information communication technology which makes information easily and widely shareable at the click of a button. The possibility of abuse of personal information has also necessitated both criminal and civil legislations in various territories.

Global Perspectives of Privacy Rights

The concept of the protection of privacy rights has shifted from the need to protect private individuals from abuse of privacy by governments to the need to protect personal information from abuse by other private persons including organisations. Edwards posits that the origin of data protection law were primarily to provide protection from state surveillance and data processing with little consideration for threats from the private commercial sector.[9] This view

[7] Institute of Medicine (1999) *To Err is Human: Building a Safer Health System*. The National Academies Press.
[8] Wikipedia
[9] Edwards, L., (2004) "The Problem with Privacy: A Modest Proposal" *IRLCT* 18 (3). Electronic copy available at http://ssrn.com/abstract=1857536

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

is agreed to by Kobrin,[10] who is of the opinion that the history of data protection in Europe is grounded in the attempts of European countries, particularly the Federal Republic of Germany, to curb the threat of the improper use of personal data.[11] This mode of evolution of data protection legislation can be said to be one of the reasons while the European pattern is different from the American approach.

Presently, the right of privacy is embedded in several international declarations and treaties both locally and globally. For example, the Universal Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his privacy, family home or correspondence, nor to attacks upon his honour and reputation. Everyone has the protection of the law against such interference and attacks".[12] In similar vein, the European Convention on Human Rights says: "Everyone has the right to respect for his or her private and family life, home and correspondence. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others"[13]

This right to privacy has been recognised in the constitution of several countries and even where it is not mentioned directly, such as the United States and India,[14] the courts have found the right enshrined in other provisions of the law and have upheld the same. For example, the United States in 1974, in response to the *Watergate* Scandal enacted the Privacy Act wherein the Congress in passing the Act observed that the privacy of the individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal Agencies and that the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information.

The right of privacy seems to have developed into more than one component. According to the Global Internet Liberty Campaign, privacy can be divided into four main areas:[15] (a) information Privacy: which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records; (b) bodily privacy: which concerns the protection of people's physical selves against invasive procedures

[10] Kobrin, S. J., (2004) Safe Harbours are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance *Review of International Studies*, 30, 111-131
[11] See also Roch, M. P., (1996) Filling the Void of Data Protection in the United States: Following the European Example, *Santa Clara Computer and High Tech. L. J.*, 12, 71-96
[12] Article 12 of the UDHR
[13] Article 8 of the ECHR. Compare this with Article 7 of the Charter of the Fundamental Rights of the European Union which is almost the same in wording except that the word 'correspondence in the European Convention is replaced with the word 'communications' in the Charter.
[14] A Marsoof, (2008) The Right to Privacy in the Information Era: A South Asian Perspective 5:3 SCRIPTed retrieved from http://www.law.ed.ac.uk.ahre/scripted/vol5-3/marsoof.asp
[15] Electronic Privacy Information Center (2001) *Privacy and Human Rights 2001: An International Survey of Privacy Laws and Developments* Washington DC, USA

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

such as drug testing and cavity searches; (c) privacy of communications: which covers the security and privacy of mail, telephones, email and other forms of communication; and (d) territorial privacy: which concerns the setting of limits of intrusion into the domestic and other environments such as the workplace or public space.

A major component of the right of privacy and one that appears to have taken the front burner position is data protection. Even though some authors[16] sometimes discuss privacy and data protection as if the two are the same and thus the question has been asked whether privacy and data protection are the same thing but the answer appears to be in the negative.[17] Kuner[18] is of the opinion that 'data protection' and 'privacy' are 'twins but not identical'. He further points out that both under European law and the United States Supreme Court's constitutional interpretation, privacy includes issues that go beyond data protection. In his words, "privacy can thus be seen as a concept which is both broader than, and independent from data protection, though there can be a significant overlap between the two."[19] In a similar vein, Bygrave[20] writes that 'it would be wrong to assume that the concepts of "data protection" and "privacy" are completely synonymous. While closely linked, they are not identical – at least from the European perspective. "Data protection" is typically reserved for a set of norms that serve a broader range of interests than simply privacy protection.' Thus, that data protection stems from the cluster of privacy rights seems to be clear.[21]

Constitutional Protection and Guarantee of Personal Data

One may tend to wonder sometimes why much noise is made about the need for legal safeguards for personal data or personal information. Taking a look at the pre-internet era, Lloyd has this to say about the risks attendant to information gathered without legal safeguards: "Many of the recorded instances of the misuse of information have occurred, not as part of the original design, but as a by-product of the fact that the information is available. The story has been told of how the elaborate population registers maintained by the Dutch authorities prior to the Second World War (no doubt with the best possible motives) were used by the invading

[16] See Kamal, A., (2005) *The Law of Cyberspace – An Invitation to the Table of Negotiations* 1st ed. United Nations Institute for Training and Research, 28-33; Dalal, P., *Data Protection Law in India: A Constitutional Perspective* http://ipmall.info/hostedresources/gin/PDalalDATA-PROTECTION-LAW-IN-INDIA.pdf; Dalal, (2006) Data Protection Law in India: The TRIPS Perspective *Journal of Intellectual Property Rights* 11, 125-131

[17] *Supra* Note 12 above

[18] Kuner, C., (2009) *An International Legal Framework for Data Protection: Issues and Prospects* Computer Law & Security Review 25, 307-317 available at http://ssrn.com/abstract=1443802

[19] *Ibid.*

[20] Bygrave (2010) (2010) *Privacy and Data Protection in an International Perspective*. (Stockholm Institute for Scandinavian Law) Retrieved from http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf See also Bygrave, L. A. (2002) *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, The Hague/London/New York Chapter 7; See also De Hert, P., and Schreuders E., *The Relevance of convention 108' 33, 42, Proceedings of the Council of Europe Conference on Data Protection*, Warsaw, 19-20 November 2001

[21] Bygrave L. A. (2010) *Privacy and Data Protection in an International Perspective*. (Stockholm Institute for Scandinavian Law) Retrieved from http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

Germans to facilitate the deportation of thousands of people.[22] In this case, as in any similar case, it is clear that it is not the information per se that harmed individuals, but rather the use that was made of it. In this sense, information is a tool, but a very flexible tool; and whenever personal information is stored, the subject is to some extent 'a hostage to fortune'. Information which is freely supplied today and which reflects no discredit in the existing social climate may be looked upon very differently should circumstances change.[23]

The Constitution of the Federal Republic of Nigeria, 1999 provides in Chapter 4 for a set of rights that are popularly called Fundamental Human Rights.[24] First among these rights is the right to life. Even though the constitution does not plainly say that people have a right to health, one can say that the denial of a right to health makes some mockery of the right to life. Or what is the essence of the right to life when there is no guarantee of a good health system that can take care of health challenges that may be life-threatening?

With reference to privacy rights, Section 37 of the Constitution of the Federal Republic of Nigeria 1999 expressly recognises the right of privacy. It states that "The privacy of citizens, their homes, correspondence telephone conversations and telegraphic communications is hereby guaranteed and protected". Further, section 34 (1) of the Constitution provides that "Every individual is entitled to respect for the dignity of his person…" One of the indices of the respect for the dignity of an individual is respect for privacy. While it is agreed that informational privacy or data protection is but an aspect of privacy, it does not seem as if the context of privacy protection as enumerated in section 37 of the Nigerian constitution, covers the concept of data protection as discussed in this work. The use of the word 'home' as used in the section may be interpreted to mean that the privacy that is contemplated goes far beyond personal information[25]. It also seems the use of other words like 'correspondence', 'telephone conversations' and telegraphic communications limit the context of privacy protection to communications and personal interactions and not personal information processing.

Interestingly, the second schedule to the Constitution that deals with legislative powers does not mention anything like information communication technology directly. An abstraction or inference may only be made from some clauses that govern matters like posts, telegraphs and telephones;[26] trade and commerce;[27] wireless, broadcasting and television.[28] But it appears that any legislation that may be made on this area lies within the legislative competence of the National Assembly and not that of the states. The fact that cyberspace lies outside the reach of sovereign nations ordinarily, precludes any component state in the Nigerian federation from attempting to legislate on it.

Personal Health Information

[22] Hondius, F. W., (1975) *Emerging Data Protection in Europe* (Amsterdam,)
[23] Lloyd, I. J., (2011) *Information Technology Law* (6th ed.) (Oxford)
[24] There is a special procedure for the enforcement of these right within the corpus of Nigerian procedural legislations.
[25]See Nwauche, E. S., (2007) The Right to Privacy in Nigeria RNLP
[26] Second Schedule Part 1, item 46
[27] Second Schedule Part 1, Item 62
[28] Second Schedule Part 1, item 66

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

Data protection legislation and advocates have created a special class of personal information known as sensitive personal data. Under the United Kingdom Data Protection Act,[29] Personal data is 'sensitive' if it relates to: racial or ethnic origin, political beliefs, religious beliefs, trade union membership, physical or mental health, sex life, criminal offences and court proceedings. Similar to the UKDPA, the GDPR[30] classifies personal data to be sensitive if it relates to: racial or ethnic origin, political beliefs, religious or philosophical beliefs, trade union membership, genetic or biometric data, physical or mental health and sex life or sexual orientation. The major difference is that the GDPR does not categorize data relating to criminal offences and court proceedings as sensitive data.

This class of data is seen as personal and as such should not be processed without stringent controls. The UK Data Protection Act provides that the condition for processing personal data relating to health is met if the processing is necessary for health or social care purposes. The Act goes further to define health or social care purposes to mean the purposes of— (a) preventive or occupational medicine, (b) the assessment of the working capacity of an employee, (c) medical diagnosis, (d) the provision of health care or treatment, (e) the provision of social care, or (f) the management of healthcare systems or services or social care systems or services. Then the conditions and safeguards in Article 9(3) of the GDPR dealing with obligations of secrecy would also apply.

The NITDA Data Protection Regulations (2019) following the line of the above mentioned statutory instruments defines sensitive personal data to mean data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information, but sadly, it fails to make any other reference to the concept of sensitive personal data either by way of outline as to how such data is to be processed, or the necessary safeguards instituted to prevent abuse of such data or in what circumstances the processing of such data would be necessary. The insertion of the phrase "sensitive personal data" within the body of the Guidelines without determining what type of data falls into smirks of the fire brigade approach to legislation and regulation that Nigeria is fond of adopting.

A much better approach is that adopted by the United States Health Insurance Portability and Accountability Act which, with respect to personal health information, gives very clear and explicit definitions. It defines the concept of individually identifiable health information as information that is (a) a subset of health information, including demographic information (b) collected from an individual by the healthcare organisation, and (c) relates to the past, present or future medical health or condition of an individual; the provision of healthcare to an

[29] Section of the 2016 Act

[30] 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 Directive 95/46/EC (General Data Protection Regulation). Article 4(13), (14) and (15) and Article 9 and Recitals (51) to (56) of the GDPR

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

individual; or the past present or future payment for the provision of healthcare to an individual ; and (d) identifies the individual; or (e)with respect to which there is a reasonable basis to believe the information can be used to identify the individual

Legislative Basis for Personal Health Information Protection in Nigeria

(a) The National Health Act.

The National Health Act was enacted in 2014 as an Act to provide a framework for the regulation, development and management of a national health system and set standards for rendering health services in the Federation and for related matters. Prior to the enactment of the Act, there was no federal legislation that attempted to outline the rights of patients (consumers) in the Nigerian healthcare sector, especially with regards to the duty of confidentiality owed by healthcare personnel and workers. In very clear language, the Act stipulates that healthcare workers shall give a user relevant information pertaining to his or her health and forbids the same information being disclosed to other persons except on certain conditions.

The Act makes clear provisions for the protection of personal health information in sections 26 – 29 of the Act. Section 26(1) lays down the duty of confidentiality by providing that "All information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment is confidential." This duty of confidentiality between healthcare providers and patients is an age old one. The import of the foregoing provision is that it is not only doctors that owe this duty, but everyone working in the precincts of a healthcare provider. Subsection (2) of the section goes further to state that "no person may disclose any information contemplated in subsection (1) unless –

(a) The user consents to that disclosure in writing;
(b) A court order or any law requires that disclosure;
(c) In the case of a minor, with the request of a parent or guardian;
(d) In the case of a person who is otherwise unable to grant consent upon the request of a guardian or representative; or
(e) Non-disclosure of the information represents a serious threat to public health.

This is a strong codification of the duty of confidentiality that medical personnel owe the users of healthcare services. Apart from the above-mentioned six grounds, on no other account may personal health information be disclosed to someone who is not a healthcare giver or provider or working in a health establishment. In other words, except the recipient is in the line of duty, personal health information should not be disclosed to him or her.

As a follow up to the preceding subsection, the Act makes provision for other instances of legitimate disclosure in Section 27 which provides that "A health worker or any health care provider that has access to the health records of a user may disclose such personal information to any other person, health care provider or health establishment as is necessary for any legitimate purpose within the ordinary course and scope of his or her duties where such access or disclosure is in the interest of the user".

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

In the view of this present writer, as far as the protection of personal health information is concerned, the most important provision in the Act is Section 29 (1) of the Act which places the duty of protection of health records on the person who is in charge of a health establishment. Such a person is required to set up control measures to prevent unauthorised access to those records and to the storage facility in which, or systems by which records are kept. This clearly delineate where responsibility lies for the protection of electronic as well as manually stored personal health records.

Thus, where the healthcare provider or institution employs a technical person or organisation to handle the conversion of their medical health records from paper based records to electronic format, the responsibility of ensuring the integrity of the records and the prevention of unauthorised access to the records lies with the person in charge of the health establishment and this liability does not distinguish between private and public healthcare systems. Where the records are stored in electronic form from the outset, the person in charge of the health establishment is expected to have put in place appropriate technical safeguards to ensure that data breach is prevented or at the least reduced the possibility to the barest minimum. Where the appropriate person fails, he is liable upon conviction to the payment of a fine or a term of imprisonment.

Subsection (2) creates certain offences with respect to the health records protected under subsection (1). "A person who –

(a) fails to perform a duty imposed on them under subsection (1) of the Act;
(b) falsifies any record by adding to or deleting or changing any information contained in that record;
(c) creates, changes or destroys a record without authority to do so;
(d) fails to create or change a record when properly required to do so;
(e) provides false information with the intent that it be included in a record;
(f) without authority, copies any part of a record;
(g) without authority, connects the personal identification elements of a user's record with any element of that record that concerns the user's condition, treatment or history;
(h) gains unauthorised access to a record or a record-keeping system, including intercepting information being transmitted from one person, or one part of a record-keeping system, to another;
(i) without authority, connects any part of a computer or other electronic system on which records are kept to any –
    (i) other computer or other electronic system; or
    (ii) terminal or other installation connected to or forming part of any other computer or other electronic system; or
(j) without authority, modifies or impairs the operation of any –
    (i) part of the operating system of a computer or other electronic system on which a user's records are kept; or
    (ii) part of the programme used to record, store, retrieve or display information on a computer or other electronic system on which a user's records are kept,

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

commits an offence and is liable on conviction to imprisonment for a period not exceeding two years or to a fine of N250,000.00 or both."

It is encouraging to observe that the language of subsection (2) of Section 29 in creating certain offences in respect to health records, prohibits the connection by any person without authority of personal identification elements of a user's record with any element of that record that concerns the user's condition, treatment or history. The provision further prohibits the gaining of unauthorised access to a record or record keeping system, including the interception of information being transmitted from one person, or one part of a record-keeping system to another. These provisions clearly shows that the Nigerian legislature is beginning to understand the reality and role of computer processed information in this age and the possibilities arising therefrom.

The same attempt to capture computer processed information is shown by the use of the words "any person who without authority, connects any part of a computer or other electronic system on which records are kept to any other computer or other electronic system,[31] or to any terminal or other installation connected to or forming part of any other computer or other electronic system or without authority modifies or impairs the operation of any part of the operating system of a computer or other electronic system on which a user's records are kept, or part of the programme used to record, store, retrieve or display information on a computer or other electronic system on which a user's records are kept". The direct language of the statute recognises the important of personal health information kept or stored or processed by computers and other electronic means and envisages the need to criminalise any abuse or misuse of such information ranging from unauthorised access, to outright damaging or impairing of systems.

The sponsors of this legislation should be commended for taking the bull by the horn by providing for protective measures for personal health information in electronic form. It seems the drafters of this law foresaw that the Cybercrime Act[32] (which was a latter legislation and much broader with the scope of, among other things the protection of privacy rights), would fail to meet up in the area of protection of personal information. The National Health Act clearly and in a robust fashion dedicated certain sections (highlighted above) to the need to protect personal health information in records kept in any form with specific attention to computer-processed and electronic forms.

It is also worthy of note that while the Cybercrime Act fails to clearly prohibit unauthorized access *simpliciter*, it added the unnecessary conditions of accessing for fraudulent purposes and the obtaining of data that are vital to national security. Thus where a party accesses a computer and the data obtained or obtainable are not vital to national security, prosecution under the Cybercrime Act becomes a near impossibility. But the National Health Act tries to capture any type of unauthorised access by making same liable to a fine of N250,000.00 or to imprisonment for a term of two years.

[31] Section 29(2) (i) (1)
[32] The Cybercrime (Prohibition Prevention, Etc) Act 2015

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

The Nigerian Data Protection Guidelines 2019

Though there is no direct legislation for the protection of personal information generally in Nigeria comparable to the United Kingdom Data Protection Act, there appears to be a legal window for the protection of personal data traceable to the constitutional protection for privacy rights. The National Information Technology Development Agency Act is the federal government agency assigned with the responsibility of implementing the National Information Technology Policy. It is worth noting that one of the basic strategies of the National Information Technology Policy is the enactment of a data protection legislation for safeguarding the privacy of national computerized records and electronic documents. By the provisions of the law creating the NITDA, Section 6 empowers the Agency to create a framework for the general operation and regulation of information technology practices, to provide guidelines to establish and maintain information technology infrastructures for all sectors and the government and to develop guidelines for electronic governance, networking and standardization.

It is in furtherance of the above statutory responsibilities that the Agency developed the first Guidelines for Data Protection in 2013 and a subsequent set of guidelines/regulations titled Nigerian Data Protection Regulations 2019. The Guidelines do not appear to have the force of a direct legislation but they are created pursuant to a section of the NITDA Act which is an enactment of the National Assembly. The preamble to the Guidelines state that the NITDA recognizes that many public and private bodies have migrated their respective businesses and other information systems online and that information solutions in both the private and public sectors now drive service delivery in the country through digital systems; and that it is cognizant of emerging data protection regulations within the international community geared towards security of lives and property and fostering the integrity of commerce and industry in the volatile data economy; and that it is conscious of the concerns and contributions of stakeholders on the issue of privacy and protection of personal data and the grave consequences of leaving personal data unregulated.

Under Part 1, Article 1.1 states that the objectives of the Regulations are to:
a) Safeguard the rights of natural persons to data privacy;
b) Foster safe conduct for transactions involving the exchange of Personal Data;
c) Prevent manipulation of Personal Data; and
d) Ensure that Nigerian businesses remain competitive in international trade through the safe-guards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice.

Article 1.2 outlines the scope and provides that:
a) this Regulation applies to all transactions intended for the processing of Personal Data, to the processing of Personal Data notwithstanding the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria;
b) this Regulation applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria;

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

c) this Regulation shall not operate to deny any Nigerian or any natural person the privacy rights he is entitled to under any law, regulation, policy, contract for the time being in force in Nigeria or in any foreign jurisdiction.

The Nigeria Data Protection Regulations in the attempt to safeguard personal information provides that anyone involved in data processing or the control of data shall develop security measures to protect data. Such measures shall include but shall not be limited to, protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organisational policy for handling personal data (and other sensitive or confidential data) protection of emailing systems and continuous capacity building for staff.

The Regulations establish certain governing principles for data processing. Under the instrument, personal data shall be: collected and processed in accordance with specific, legitimate and lawful purpose consented to by the data subject. This means that no healthcare provider shall ask for more than necessary information and the purpose must be consented to by the user of their services. Secondly, personal data shall be adequate, accurate and without prejudice to the dignity of the human person. Thirdly, personal data shall be stored only for the period within which it is reasonably needed. This implies that personal health record may no longer be kept beyond a certain time except there is need to keep the same. Fourthly, personal data shall be secured against all foreseeable hazards and breaches such as theft, cyber-attack, viral attack, dissemination, manipulations of any kind and damage either by rain, fire or exposure to other natural elements.

Further to the above is the attempt by the regulations to create civil liability by providing that anyone who is entrusted with personal data of a data subject (a healthcare provider entrusted with the personal health information of a patient or user) or who is in possession of the personal data owes a duty of care to the data subject. The import of this is that where the duty of care is breached, the injured party may sue for damages. This is because a duty of care gives the other party rights at law. The other side of the provision is that anyone entrusted with personal data or who is in possession of the personal data shall be accountable for his acts and omissions in respect of the processing of the data. This duty of accountability or responsibility is similar to the provisions of the National Health Act,[33] which makes the person entrusted with the records responsible for them.

The Regulations make an attempt to impose punishment on any data controller that fails to comply with the provisions. Where a person who is subject to the Regulations is found to be in breach of the data privacy rights of any data subject, his liability shall depend on whether he is a data controller with more than 10,000 data subjects or less and this shall be in addition to any other criminal liability. The penalty payable ranges from about 2 million naira to about 10 million naira.

[33] Section 29 of the National Health Act.

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

With regards to transfer of personal data to foreign countries, the Regulations impose some stringent conditions but make a very laudable exception and one thinks this fits personal health information that may need to be transferred to a foreign country in certain instances. The Regulations provide that where the requisite decision by the Attorney General of the Federation as to the safeguards in the foreign country is not available, transfer of personal data to a foreign country or an international organisation may take place where the transfer is necessary in order to protect the vital interests of the data subject, or where the data subject is physically or legally incapable of giving consent, provided that the data subject has been made to understand through clear warnings of the principles of data protection that may be violated in the event of transfer to a third country. Thus where a person's health data is to be transferred to another country, the regulations permit it even if the third country does not have appropriate safeguards for protection if the transfer is for the protection of the person's vital interests.

Other Enactments

With respect to people living with HIV/AIDS, section 13(1) of the HIV and AIDS (Anti-Discrimination Act, 2014 provides that: "All persons living with HIV or affected by AIDS shall have the right to protection of data with respect to their health and medical records". Subsection (2) of the section imposes a criminal liability on failure to comply by providing that "A person who fails to comply with the provisions of this section, commits an offence and is liable on conviction to a fine of not less than N500,000.00 for an individual and N1million for an institution or for a term not exceeding two years or to both fine and imprisonment.

Thus, one can say with some measure of certainty that protection for personal health information is guaranteed under the laws of Nigeria. It cannot be over-emphasized that people living with HIV/AIDS should be shielded among other things, from stigmatisation and all manner of discrimination. One sure way of doing this is to ensure that their health and medical records have adequate protection provided by law. The penalty imposed by the above law may serve as a deterrent but there is the need to provide for compensation and damages where a person living with HIV/AIDS has had his health and medical records unduly processed or howsoever abused.

Lessons from other Jurisdictions

As pointed out in the body of this work, the United Kingdom Data Protection Act 2018, in complying with the European General Data Protection Regulation provides for very stringent measures to safeguard the personal information of people and of course, retains the Information Commissioner's Office which is the established institutional framework to ensure that data processors and controllers comply with the provisions of the law and thus afford protection to personal data. In the field of personal health information,

The Health Insurance Portability and Accountability Act 1996 (HIPAA) is a United States statute with which doctors, nurses, hospitals and other healthcare providers have to comply. The HIPAA seeks to ensure that all medical records, medical billing and patient accounts meet certain consistent standards with regard to documentation, handling and privacy. In particular, the HIPAA Privacy Rule provides federal protection for personal health information held by medical entities and gives patients an array of rights with respect to that information.

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)

It is worth noting that while some institutions like schools and school districts may not be covered by the Health Insurance Portability and Accountability Act, the health records of the students that are maintained there are protected by the Family Educational Rights Privacy Act. Nevertheless, the HIPAA may still apply to patient records at a university hospital or to the health records of non-students at a university health clinic.

Conclusion

We have tried to look at the importance of personal health information firstly by looking at the duty of confidentiality that doctors and other healthcare workers owe to patients or users of their health services. We also identified the impact of technology in patients' health records and the migration from the old case notes to electronic records that are recorded by computers and which are processed by computers and subject to serious manipulation both for positive and negative uses.

We attempted to discuss the right of privacy as a globally accepted right which has attracted both regional and territorial legislations and the place of personal data protection as its main offshoot that has necessitated the enactment of data protection legislation both generally and in some cases for some specific types of personal information. One key type is personal health information which is generally seen as worth much protection. Apart from the criminal liabilities that offenders face for contravention of the law, the possibility of an action in damages cannot be excluded even though not directly provided by statute.

It is clear from the foregoing that the personal health information of Nigerians whether processed manually or electronically has some measure of protection today unlike in recent years before the National Health Act was enacted. Also from the provisions of the Nigeria Data Protection Regulations and the other local enactments that were considered, it is clear that Nigeria is seriously addressing the issue of personal data protection and with such legislative provisions the constitutional guarantee of the respect to the privacy of citizens can now be enforced.

One may conclude at this point that personal health information in Nigeria today has legal protection. What remains is how the Nigerian courts will interpret the various legislations when the issues come before the courts. But for now, one can say that personal health information has legal protection in Nigeria.

Print ISSN: ISSN 2053-6321(Print), Online ISSN: ISSN 2053-6593(Online)