NIGERIA HEALTH ICT PHASE 2 FIELD ASSESSMENT FINDINGS
Table of Contents

Acknowledgements ................................................................. 4
List of Acronyms and Abbreviations ........................................... 5
Executive Summary ................................................................. 6
Overview of Laws Relevant to Patient Privacy and Data Security ........... 8
  CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA ................... 8
  NATIONAL HEALTH ACT .......................................................... 8
  HEALTH RECORDS OFFICERS ACT ......................................... 9
  DANGEROUS DRUG ACT AND NATIONAL DRUG
  FORMULARY AND ESSENTIAL DRUG LIST ACT .......................... 9
  THE CODE OF MEDICAL ETHICS ........................................... 9
  OTHER RELEVANT LAWS & REGULATIONS .................................. 9
  PATIENT DATA PROTECTION UNDER RELEVANT LAWS ................. 11
  DATA CAPTURE OR RECORDING ........................................... 11
  PERSONNEL RESPONSIBLE FOR OBTAINING OR CAPTURING DATA ....... 12
  ACCESS TO PATIENT INFORMATION ...................................... 13
  USE OF PATIENT INFORMATION ........................................... 13
  STORAGE OF PATIENT INFORMATION ..................................... 14
  DATA TRANSFER ............................................................... 14
  SECURITY OF PATIENT INFORMATION .................................... 15
  THIRD PARTY RESPONSIBILITIES ........................................ 16
  ENFORCEMENT AND SANCTIONS ......................................... 17
  GAPS IN THE PROTECTION OF PATIENT INFORMATION ..................... 18
Recommendations ................................................................. 19
Conclusion ................................................................ 19
List of Reviewed Resources ..................................................... 20
Acknowledgements

This Guide to Health ICT privacy and security laws document has been developed and produced by United Nations Foundation as an output of the Information Communications Technology for Saving One Million Lives (ICT4SOML) initiative midwifed through the visionary leadership provided by the Honourable Minister of Health and Honourable Minister of Communication Technology with funding support from Norwegian Government.

Gratitude is due the following individuals: Dr. Patricia Mechael, Jonathan Payne, Carolyn Florey, Olasupo Oyedepo, Ime Asangansi, Emeka Chukwu from the ICT4SOML initiative.

We would also like to express our gratitude to Technology Advisors, LLP, ICT Lawyers & Consultants (Basil Udotai and Ndubisi Okonta) for their work that culminated in this guide. We remain indebted to all others who have contributed to this work but have been omitted in this acknowledgement.
List of Acronyms and Abbreviations

CA  Cybercrime (Prohibition, Prevention, etc.) Act
DDA  Dangerous Drug Act
GMPC  General Multi-purpose Identify Cards
HROA  Health Record Officers (Registration, etc.) Act
ICT  Information and communication technology
ICT4SOML  Information Communications Technology for saving One Million Lives
MDCN  Medical and Dental Council of Nigeria
NCA  Nigerian Communication Act
NCC  Nigerian Communications Commission
NDFEDLA  National Drug Formulary and Essential Drug List Act
NHA  National Health Act
NHISP  Nigeria Health Information System Policy 2015
NIMC Act  National Identity Management Commission Act
NIN  National Identification Number
NITDA Act  National Information Technology Development Agency Act
NITDA  National Information Technology Development Agency
RTS  Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations
SOML  Saving One Million Lives
WHO  World Health Organization
Executive Summary

In 2012, the Nigerian government launched the Saving One Million Lives (SOML) initiative to prevent the deaths of one million pregnant women, new mothers, newborns, and children under five by 2015.\(^1\) The use of information and communication technology (ICT) is a key strategy of SOML, prioritized by the government to help save a million lives and deliver universal health coverage.

The use of ICT in the delivery of health services is generally referred to as eHealth, and increasingly as digital health, is widespread. In all cases where eHealth services have been deployed, a recurrent issue has been the safeguarding of patient information or data. Some countries have enacted overarching data protection regimes that apply to all sectors including the health sector, while others have enacted sector-specific regimes. The general objectives of these data protection laws include prescribing conditions for the lawful processing of data, providing for data quality, conferring certain rights to data subjects such as the right of access to data, imposing restrictions for the disclosure of data, imposing the obligation to report data breaches, prescribing judicial remedies, liability and sanctions, and the conditions for the transfer of personal data to third parties and across borders.

Nigeria does not have an overarching personal data protection framework, rather, various sector-specific laws including certain professional codes of ethics and industry practices that govern the processing of personal information. Although the various laws provide in general for the confidentiality of personal information and requires in most cases, consent before the disclosure of personal information, they do not confer rights on data subjects such as the right of access to the data or the right to object to the processing of data.

Nigeria’s laws differ in robustness. The laws that apply to the communications sector, for instance, contain specific provisions on data protection while data protection does not feature prominently under the laws governing the health sector. Arguably, the architects of the national health system focused on the policy objective of universal health coverage and have yet to address issues such as lawful processing of patient information.

Gaps in the health sector laws notwithstanding, the provisions in non-health sector legislation as well as contractual obligations may serve to close the gaps until a more permanent solution can be put in place.

This paper reviews the current legislation, policy and regulations that apply to the processing of patient information in Nigeria and makes recommendations as to how gaps in existing legislation can and should be addressed. It builds on the work undertaken by TrustLaw Connect on behalf of the mHealth Alliance to review national and regional approaches to patient privacy in an increasingly mobile environment.\(^2\) A critical next step identified through this review process is the development of specific provisions for the explicit protection and processing of personal health information.

---

1. Every year, pneumonia, diarrhea, and malaria claim the lives of about 596,000 children in Nigeria. According to a demographic and health survey, only about a third of women give birth in medical facilities. Unsafe pregnancy, birth, and postnatal care are among the biggest killers in Nigeria. It is estimated that more than 30,000 Nigerian women die each year due to complications from pregnancy and delivery. [http://voices.mckinseyonsociety.com/a-health-care-vision-for-nigeria/#sthash.DmgZ3wKx.dpuf](http://voices.mckinseyonsociety.com/a-health-care-vision-for-nigeria/#sthash.DmgZ3wKx.dpuf) (accessed on 11 September 2015)

Overview of Laws Relevant to Patient Privacy and Data Security

The legal framework that governs the health sector consists of policies, statutes and rules of professional conduct. The following is an overview of key legislation that is applicable directly or indirectly to patient privacy and the secure capture, processing, storage, and transfer of personal health information.

CONSTITUTION OF THE FEDERAL REPUBLIC OF NIGERIA

Nigeria’s supreme law—the Constitution of the Federal Republic of Nigeria—guarantees the right to privacy to every Nigerian citizen. This right to privacy extends to the individual’s home, correspondence, telephone conversations and telegraphic communications. In the event of conflict between the Constitution and any other law, the Constitution prevails and the other law shall to the extent of the inconsistency be void.

NATIONAL HEALTH ACT

In the context of the laws that apply to the health sector, the recently enacted National Health Act (NHA) is the primary legislation that regulates the provision of health services. The NHA provides a framework for the regulation, development and management of a national health system and sets standards for rendering health services in Nigeria.

The NHA is arguably the first law that provides for the rights and obligations of users and healthcare personnel. It requires the person in charge of a health establishment to keep the health records of every user of health services, attaches confidentiality to a user’s information, imposes restrictions on the disclosure of a user’s information, and requires the person in charge of health establishments to set up control measures for preventing unauthorised access to information. Users have a right to be informed of their state of health and necessary treatment. There is no corresponding right for users to be informed of how their data are being processed or would be processed.

HEALTH RECORDS OFFICERS ACT

The Health Record Officers (Registration, etc.) Act (HROA) establishes a Board to oversee the profession of health record management. It requires health records officers to be

---

3. Policies are formulated at the national level by the Federal Ministry of Health and at the State level, by the State Ministries of Health. (Nigeria is a federal republic, made up of 36 states and a Federal Capital Territory).

4. Statutes are enacted by the legislature usually in the form of Acts. An Act is a law duly passed by the National Assembly, to which the President of the Federal Republic of Nigeria had assented. It is binding and represents the law until amended or repealed.

5. Please see section 1(3) of the Constitution of the Federal Republic of Nigeria 1999 (as amended)

6. User is defined in the NHA to mean the person receiving treatment in a health establishment, including receiving blood or blood products, or using a health service, and if the person receiving treatment or using a health service is:

(a) below the majority age, “user” includes the person’s parent or guardian or another person authorised by law to act on the first mentioned person’s behalf; or incapable of taking decisions, “user” includes the person’s spouse or, in the

(b) absence of such spouse, the person’s parent, grandparent, adult child, brother, sister, or another

(c) person authorised by law to act on the first mentioned person’s behalf.

7. Health establishment is defined in the NHA to mean the whole or part of a public or private institution, facility, building or place, whether for profit or not, that is operate or designed to provide inpatient or outpatient treatment, diagnostic or therapeutic interventions, nursing, rehabilitative, palliative, convalescent, preventative or other health service.
registered and prescribing the conditions for registration. Although not specifically applicable to patient data, it contains a definition for “health record” unlike the NHA, which requires the creation of “health record” but does not define “health record”.

**DANGEROUS DRUG ACT AND NATIONAL DRUG FORMULARY AND ESSENTIAL DRUG LIST ACT**

Helpful guidance on what may count as “patient or user information” is provided by the Dangerous Drug Act (DDA) and the National Drug Formulary and Essential Drug List Act (NDFEDLA).

**THE CODE OF MEDICAL ETHICS**

The Code of Medical Ethics (Code) issued by the Medical and Dental Council of Nigeria pursuant to the Medical and Dental Practitioners’ Act, applies to all medical and dental practitioners. It confers “absolute confidentiality” on all a physician knows about his or her patient even after the patient has died; attaches confidentiality to all communications between the patient and the medical or dental practitioner made in the course of treatment, except where disclosure is compelled by law or overriding common good or with the consent of the patient.

**OTHER RELEVANT LAWS & REGULATIONS**

Other laws, which may apply to the processing of patient information, include the Cybercrimes (Prohibition, Prevention, etc) Act (CA), the Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations (RTS), the National Identity Management Commission Act (NIMC Act), the National Communications Act (NCA), and the National Information Technology Development Agency Act (NITDA Act).

**Cybercrimes (Prohibition, Prevention, etc) Act**

The CA provides a unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. It also ensures the protection of critical national information infrastructure, and promotes cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

**Nigerian Communications Commission Regulations**

The RTS provides for the establishment and maintenance of a central database for all corporate, private and commercial subscribers to Mobile Telephone Services in Nigeria. The Central Database is domiciled within the Nigerian Communications Commission and provides a platform for the central processing and storage of subscriber information. The Central Database is the property of the Government of Nigeria. The RTS contains specific provisions on data protection and confidentiality, confers on licensees the right to use subscriber information; imposes conditions for lawful processing of subscriber information and vests in the subscriber, a right to view his or her personal information as well as the right to request updates or amendments to the information.

---

8. The Regulation also apply to subscribers of foreign licensees who are roaming on the network of a licensee in Nigeria. Provided that subscribers of foreign licensees are registered in their home jurisdiction and there exists necessary arrangements between the Nigerian Regulator and the relevant regulatory authority which allows the Nigerian Regulator access such subscriber information, the subscriber need not register their information in Nigeria.
9. Licensee is defined in the RTS to mean a provider of mobile Telephone Services that utilises a subscription medium in the Federal Republic of Nigeria.
10. Section 9 of the RTS.
National Identity Management Commission Act

The NIMC Act provides for the establishment of a national identity database (Database)11 and a National Identity Management Commission (Commission or NIMC) charged inter alia with the maintenance of the national identity database, the registration of individuals, the issuance of general multipurpose identity cards and ensuring the preservation, protection, sanctity and security (including cyber security) of any information or data collected, obtained, maintained or stored in respect of the Database.

The Commission is required to assign a unique National Identification Number (NIN) and issue General Multi-purpose Identity Cards (GMPC) to registrable persons.12 According to the Commission's website, their mandate is to "provide an assured identity system in Nigeria through the concept of enrol once and be identified for life".13

The Commission is also required to specify a date (by means of regulations) from which every registered individual would be required to present their identification number for specified transactions.14 There is, on the Commission's website, a draft form of its regulation on the mandatory use of the NIN.15 Paragraph 2.1 of the draft regulation states that as of July 1, 2015, any government agency/institution, bank, insurance company and all other institutions offering services and/or are involved in transactions requiring an individual's identity as contained in section 27 of the Act, and transacts without using or requiring the use of the NIN is in violation of the Act.16

In addition, the Commission is tasked with integrating and harmonizing existing identification databases in government agencies.17

---

11. The National Identity Database shall contain registered information or data relating to citizens of Nigeria and non-Nigerian citizens who are registrable persons. See section 14 of the NIMC Act.
12. Registrable persons include: (i) any person who is a citizen of Nigeria, (ii) any person, whether or not s/he is a citizen of Nigeria who is lawfully and permanently resident in Nigeria and (iii) any non-citizen of Nigeria who is lawfully resident in Nigeria for a period of two years or more.
14. Section 27(1) of the NIMC Act lists the transactions for which an identification number is to be presented. This includes the opening of individual and or personal bank accounts, purchase of insurance policies, such transactions specified under the Contributory Health Insurance Scheme, transactions that have social security implications, relevant government services and any other transaction which the Commission may so prescribe and list in the Federal Government Gazette. Conducting any of the specified transactions without a NIN is an offence punishable by either a fine or imprisonment (see Section 29 of the NIMC Act).
15. The draft regulation can be accessed through this link: http://www.nimc.gov.ng/sites/default/files/MANDATORY%20USE%20OF%20NIN%20Draft_0.pdf
17. According to press reports, the Federal Government, by a Circular with reference number: Ref. Na. 59B03NL/87 dated 28 May 2014, mandated all government Ministries, Departments and Agencies ("MDAs") involved in all forms of biometric data capture to complete their registrations (required under various Acts) and hand over to the NIMC by December 31 2014.

The government organisations which collect biometric data include the National Population Commission (NPC), the National Identity Management Commission (NIMC), the Federal Road Safety Commission (FRSC) and the Independent National Electoral Commission (INEC), Central Bank of Nigeria (CBN), Nigerian Immigration Service (NIS), as well as the suspended Nigerian Police Biometrics Central Motor Registry (PoliceBCMR), among others.

It appears that the above deadline was not met as President Buhari is reported to have directed government agencies to harmonise the collection and usage of biometric data, (see article by Kunle Azeez of the New Telegraph on harmonising citizens' biometric databases: http://newtelegraphonline.com/harmonising-citizens-biometric-data-bases/ Accessed on 6 October 2015.

Press reports on NIMC’s website highlights the steps taken by NIMC towards the harmonising of biometric data and lists the Federal Road Safety Commission (FRSC), National Health Insurance Scheme (NHIS), Ministry of Agriculture (for the enrolment of farmers) and others as the collaborating agencies (http://www.nimc.gov.ng/?q=nimc-and-inec-comply-presidential-directive-harmonisation-biometric-data-set-jointtechnical). Accessed on 6 October 2015.
Nigerian Communications Act (NCA)

The NCA provides a regulatory framework for the Nigerian communications industry. The NCA applies with respect to third party responsibilities as telecommunications service providers are regulated by the Nigerian Communications Commission (NCC) under this Act.

National Information Technology Development Agency Act

The NITDA Act created the National Information Technology Development Agency (NITDA) to promote the use of information technology in Nigeria through regulatory policies, guidelines, standards, and incentives. Pursuant to its powers under the NITDA Act, NITDA developed national guidelines on data protection, which is still in draft.

What follows is a review of how the above-mentioned laws apply to the capture, recording, access, use, storage, transfer, and security of personal information in the health sector. The enforceability of these laws and sanctions for breach or infraction are considered, so are the rules, or the lack thereof, relating to the transfer of data to third parties including cross-border data transfer.

The term “user” and “patient” are used synonymously in the discussions that follow.

PATIENT DATA PROTECTION UNDER RELEVANT LAWS

Patient information or health data is not specifically defined under any of the laws that apply to the health sector. The NHA, however, makes reference to all information relating to the patient’s health status, treatment or stay in any health establishment. The RTS defines personal information to mean the full names (including mother’s maiden name), gender, date of birth, residential address, nationality, state of origin, occupation and such other personal information and contact details of subscribers specified in the registration specifications.

The NIMC Act distinguishes between “personal information” and “identification information” and defines both terms. Personal information includes an individual’s full name, other names by which the individual is or had been known, date of birth, place of birth, gender, the address of the individual’s principal place of residence in Nigeria and the address of any additional places of residence of the individual in Nigeria. Identification information includes a photograph of the individual’s head and shoulders, the individual’s signature, the individual’s fingerprints and other biometric information about the individual.

Although biometric information is not defined under the NIMC Act, it is defined in the RTS as referring to fingerprints and facial image of a subscriber in accordance with the Registration Specifications (as may be amended from time to time) provided by the Commission for the registration of subscribers.

DATA CAPTURE OR RECORDING

As there is no definition of patient information in health sector-specific legislations, it is difficult to say with a degree of certainty from the point of view of the law what information is required from patients.

---

18. Sections 6, 17 and 18 of the NITDA Act.
19. NITDA’s draft National Guidelines on Data Protection is not considered in this paper on account of it being a draft.
20. Section 26 (1) of the NHA.
21. Section 1. Registration specifications is also defined in section 1 as the Data Dictionary, Guidelines on Fingerprint Quality, specifications for Digital Image Standards and Quality, the XML Schema, Transmission protocol and the Technical interface specifications and such other specifications and amendments thereto that may be made or issued by the Commission, from time to time, to guide the registration of subscribers and the interaction of Licenses’ or Independent Registration Agents’ databases with the Central Database.
22. The Nigerian Communications Commission
The NHA mandates every health establishment to keep a health record for each patient.\textsuperscript{23} The Minister of Health may specify the content of the health record by regulation.\textsuperscript{24} For the time being, the contents of health record, however, may be intuited from the nature of information, which the NHA requires to be kept confidential. Section 26(1) of the NHA provides that all information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment is confidential.

The HROA defines “health record” as a specialized branch of health management, which embraces all technical and clerical procedures associated with management of patients from primary healthcare to tertiary levels of care. Although useful for the purposes of understanding what the profession of a health record officer is, the definition is by and large not useful for determining what information would be taken from a patient requiring health services.

The DDA requires licensed medical practitioners to keep records of patients administered drugs classified as dangerous drugs.\textsuperscript{25} The NDFEDLA provides for specific patient information to be recorded as a condition for prescription, namely: name, sex, address, age, the name of the drug or prescription, frequency and duration of administration, and date of prescription.\textsuperscript{26}

PERSONNEL RESPONSIBLE FOR OBTAINING OR CAPTURING DATA

In general, the NHA prescribes obligations for healthcare personnel. Healthcare personnel are defined in the NHA as healthcare providers and health workers. Healthcare provider means a person providing health services.\textsuperscript{27} Health worker means any person who is involved in the provision of health services to a user, but does not include a healthcare provider.\textsuperscript{28}

Apart from general provisions requiring that healthcare providers give users relevant information pertaining to their health and treatment and that the person in charge of a health establishment should ensure that health records are created and available for every user of health services, the NHA is silent as to who is authorised to capture or obtain information.

The HROA requires that health records officers\textsuperscript{29} should register with the Health Records Registration Board of Nigeria. The conditions for registration include, among others, that the individual has attended a course of training approved by the Board,\textsuperscript{30} the individual holds a certificate of experience, is of good character and has paid the prescribed fees. Again, the provisions of the HROA do not relate to the context of data capturing or recording being considered here. It relates more to the management of records, similar to library science.

In conclusion, it is not clear whose duty it is to capture data or information under current legislation. A more general answer would be to say that the obligation rests with healthcare personnel (defined in the NHA to mean healthcare providers and health workers).

As to whether consent is required before collecting information from users, there are no provisions requiring users to give consent prior to providing their data.

\textsuperscript{23} Section 25 of the National Health Act 2014
\textsuperscript{24} Section 59 of the NHA prescribes that the Minister of Health, in consultation with the National Council, may make regulations with regard to any other matter which is reasonably necessary or expedient to prescribe in the implementation of the Act.
\textsuperscript{25} Section 18 of the DDA.
\textsuperscript{26} Section 11 of the NDFEDLA.
\textsuperscript{27} Section 64 of the NHA.
\textsuperscript{28} Section 64 of the NHA.
\textsuperscript{29} Health records officer is not defined in the HROA.
\textsuperscript{30} The accepted minimum qualification for registration include the following: Diploma of the Health Records Officers’ Registration Board of Nigeria, any equivalent qualification, Degree, Higher national Diploma or Diploma in Health Studies plus Diploma in Medical Records and United Kingdom Certificate in Medical records plus Diploma in Health Statistics.
ACCESS TO PATIENT INFORMATION

There are three scenarios under the NHA whereby user information can be accessed. The first relates to the disclosure of the user information. Health workers or any healthcare provider that has access to the health records of a user may disclose such personal information to any other person, healthcare 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.31

The second is where access is needed for the purposes of treatment. In this case, the user’s consent has to be obtained. The NHA does not specify how the consent or authorization is to be obtained.32

The third scenario is for purposes of study, teaching or research. The healthcare provider is required to obtain authorization from the user, head of the health establishment concerned and the relevant health research ethics committee.33 Where the study, teaching or research will not reflect or obtain information, which identifies a user, the healthcare provider does not need to obtain the specified authorizations.

Patient health records can be accessed without authorisation where such access is in the interest of defence, public safety, public order, or public morality. This derives from section 45(1) of the Constitution of the Federal Republic of Nigeria which states the right of privacy guaranteed under the Constitution shall not invalidate any law that is reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality or public health or for the purpose of protecting the rights and freedom of other persons.

The RTS states that subscriber information contained in the Central Database shall be held on a strictly confidential basis and no person or entity shall be allowed access to any subscriber.

USE OF PATIENT INFORMATION

Patient information may be used for treatment, study, research or teaching. Where used for treatment, the patient’s authorization needs to be sought and where used for study, research or teaching, authorization has to be obtained from the patient, the head of the health establishment and the relevant health research ethics committee. In each case, the NHA does not state how the authorization should be sought.

Given the limited scope for using patient information under the NHA, “use” has been defined in this paper to include the confidentiality obligation attaching to patient information. Patient information, refers to, all information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment is confidential.34

A health worker or healthcare provider may disclose patient information where they judge it to be in the interests of the patient. Otherwise, no disclosure should be made unless these conditions are met:

- the user consents to the disclosure in writing;
- a court order or any law requires that disclosure be made;
- in the case of a minor at the request of a parent or guardian;

31. Section 27 of the NHA.
32. Section 28(1) of the NHA.
33. Section 28 (1) of the NHA. Section 34 of the National Health Act prescribes that every institution, health agency and health establishment at which health research is conducted, shall establish or have access to a health research ethics committee, which is registered with the National Ethics Committee.
34. Section 26 of the National Health Act.
• in the case of a person who is otherwise unable to grant consent upon the request of a
guardian or representative; and/or

• where non-disclosure of the information represents a serious threat to public health.

The RTS requires mobile technology service providers (“licensees”) to retain and use its
subscribers’ information on its network in accordance with the Consumer Code of Practice
for Telecommunications Services (“Consumer Code”) and any other instrument issued from
time to time by the Commission.35 A licensee shall only use personal information for their
operations and in accordance with the provisions of the Consumer Code and other Instru-
ments or Act regulating personal information.36

STORAGE OF PATIENT INFORMATION

There are no specific obligations in the NHA relating to the storage of patient information. The
obligation to keep the health records of patients prescribed under the NHA states that such
records should be created and available at that health establishment (emphasis added).37

The term “available at that health establishment” gives rise to interpretative uncertainty.
It is unclear whether it means that the records are to be physically located at all times at
the health establishment so that, for instance, the health establishment’s servers are to be
located at the health establishment or whether the fact that the health records are accessible
electronically satisfies the availability requirement. This uncertainty makes it unclear whether
health records could be stored using cloud-based services.

The RTS prohibits the retention of subscribers’ biometrics and requires licensees to retain
subscribers’ information on its network. It does not specify how long the records should be
kept. Similarly, the NHA is silent on the length of time health records are to be kept.

The Cybercrimes Act (CA) requires service providers to keep all traffic data and subscriber
information as may be prescribed by the relevant authority, responsible for the regulation
of communications services in Nigeria for a period of two years. The Act defines “service
provider” to mean:

i. any public or private entity that provides to users of its services the ability to
communicate by means of a computer system, electronic communication devices,
mobile networks, and

ii. any other entity that processes or stores computer data on behalf of such communica-
tion service or users of such service.

DATA TRANSFER

There are no provisions relating to data transfer in the laws that apply to the health sector.
It is, again, subject to interpretation whether the provision in the NHA which allows a health
worker or healthcare provider to disclose patient information to any other person, health-
care provider or health establishment as is necessary for any legitimate purpose (emphasis
added) within the ordinary course and scope of his or her duties where such access or
disclosure is in the interest of the user (emphasis added) might be used as basis for the
transfer of patient information within and outside of Nigeria. At face value, and given that
Nigerians engage in medical tourism or the possibility of medical emergency and need for
medical attention in locations other than a patient’s regular hospital, a healthcare worker or
healthcare provider may transfer patient information to persons or hospitals outside Nigeria
so long as it is for a legitimate purpose and in the interest of the patient.

35. Section 7 of the RTS.
36. Section 9(5) of the RTS.
37. Section 25 of the NHA.
However, the RTS prescribes that no subscriber information shall be transferred outside the Federal Republic of Nigeria without the prior written consent of the Nigerian Communications Commission.38 Licensees shall not release personal information of a subscriber to any third party without obtaining the prior written consent of the subscriber.39

SECURITY OF PATIENT INFORMATION

The NHA requires a person in charge of the health establishment who is in possession of a user’s health records (emphasis added) to set up control measures to prevent unauthorised access to those records and to the storage facility in which, or system by which, records are kept.40 Requiring the person in charge of a health establishment to be in possession of the health records creates uncertainty. It is not clear whether reference to possession here is to actual possession or constructive possession, or both.

Pursuant to the CA, certain computer systems, networks, computer programs, computer data or traffic data vital to the country, whose incapacity or destruction of or interference with such system would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of these matters, may be designated Critical National Information Infrastructure.

If the President were to so designate computer programs, computer data, systems or traffic data used in the health sector, more stringent security measures would apply. In the case of such designation, the President, by means of an Order, may prescribe:

• minimum standards, guidelines, rules or procedures for the protection or preservation of critical information infrastructure;
• general management of critical information infrastructure;
• access to, transfer and control of data in any critical information infrastructure;
• infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any designated critical national information infrastructure;
• storage or archiving of data or information designated as critical national information infrastructure;
• recovery plans in the event of disaster, breach or loss of the critical national infrastructure or any part of it; and
• any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure.41

The RTS requires licensees, independent registration agents, subscriber registration solution providers and the Nigerian Communications Commission to take reasonable precautions in accordance with international practices to preserve the integrity and prevent any corruption, loss or unauthorised disclosure of subscriber information obtained pursuant to the RTS and take steps to restrict unauthorized use of the Subscriber Information by their employees who may be involved in the capturing or processing of such subscriber information.42

38. Section 10(4) of the RTS.
39. Section 10(3) of the RTS.
40. Section 29(1) of the NHA.
41. Section 3 of the Cybercrimes (Prohibition) Act.
42. Section 9(4) of the RTS.
Breach Of Security Under The National Health Act

Section 29(2) of the National Health Act provides that any person who:

(a.) fails to perform a duty imposed on them under subsection (1);

(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 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:

(i.) any other computer or other electronic system; or

(ii.) any 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-

(k.) any part of the operating system of a computer or other electronic system on which a user’s records are kept; or

(l.) any 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:

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.

THIRD PARTY RESPONSIBILITIES

Although the NHA does not contain specific provisions on third party responsibilities, it nevertheless uses language suggestive of third party culpability. It is arguable that section 29(2) of the NHA (see box one) may apply to third parties owing to its use of the words “any person”.43

Technology service providers procured to provide services to health establishments may be subject to certain provisions of the CA and the NCA which impose certain duties on the service providers and prescribes sanctions where those duties are breached. For example, communications service providers are mandated to procure a licence from the Nigerian

---

43. There is the point of view that absent express provisions in the NHA imposing responsibilities or duties on third parties under the NHA, it is difficult to see how any liability would attach to third parties.
Communications Commission (NCC).\textsuperscript{44} They are also required to use their best endeavours to prevent the network facilities that they own or provide from being used in relation to the commission of any offence\textsuperscript{45} and to ensure the capability of their network to allow authorized interception by law enforcement.\textsuperscript{46}

The CA contains similar duty on cooperating with law enforcement agencies. It requires service providers to disclose information requested by any law enforcement agency or otherwise render assistance howsoever in any inquiry or proceeding under the Act.\textsuperscript{47} It also lays down specific instances where a service provider is required to provide assistance at the request of law enforcement agencies.\textsuperscript{48} There is a provision in the CA which may apply to third parties simply as it states that “any person” who may carry out specified acts, thereby committing an offence and is convicted, will be liable to imprisonment or the payment of a fine.\textsuperscript{49}

**ENFORCEMENT AND SANCTIONS**

All breach of security under the NHA is punishable by imprisonment for a period not exceeding two years or to a fine of N250,000.00 or both. See Box One for the offences under the NHA.

Professional misconduct and unethical behaviours are enforced through Tribunals or Disciplinary Committees. For instance, a medical doctor falsely claimed to have 20 years of surgical experience at a hospital in Nigeria and then accepting a position at St. Luke’s in Kilkenny was found guilty of professional misconduct and recommended to be censured. His name will remain on the medical register.\textsuperscript{50}

In 2011, the Registrar and Chief Executive Officer of the Medical and Dental Council of Nigeria (MDCN), Dr. Abdulkunini Ibrahim, disclosed that a total of 50 doctors in Nigeria were sanctioned and two were removed from practice due to professional misconduct. To ensure compliance, the Registrar disclosed that the Council works hand in hand with the Law Enforcement Agencies; the Director of Medical Services in the State where the doctor is based, as well as the Commissioners for Health and of Police.\textsuperscript{51}

The CA contains extensive provisions covering a wide range of offences, which would apply to any person who commits offences against systems designated critical national infrastructure. The offences include system interference,\textsuperscript{52} intercepting electronic messages,\textsuperscript{53} computer related forgery,\textsuperscript{54} unauthorized modification of computer systems, and network data and system interference.\textsuperscript{55} The penalties are more severe, ranging from imprisonment from two years to 14 years and substantial fines.

The RTS stipulates that licensees, independent registration agents and subscriber registration solution providers shall not under any circumstance retain, duplicate, deal in or make copies of any subscriber information or store any copies of the subscriber information for any purpose other than as stipulated in the RTS or in an Act of the National Assembly.\textsuperscript{56} Entities, including licensees, independent registration agents or subscriber registration solution providers who retain, duplicate or deal with Subscriber’s information in contraven-
tion of any provisions of the RTS are liable to a penalty of N200,000.00 per subscription medium.\textsuperscript{57} Where the entity is found to have used a subscriber’s information in any business, commercial or other transactions, such entity is liable to a stricter penalty of N1,000,000.00 per subscription medium.\textsuperscript{58}

As there is no requirement for notification of data breaches under the health sector laws and the non-health sector laws, it was difficult to find instances of data breaches. Given that individuals have very limited right of action in relation to their information and no compensatory entitlement under the health sector laws or the non-health sector law, it contributes to the paucity of information in this area.

**GAPS IN THE PROTECTION OF PATIENT INFORMATION**

The protection of patient information suffers from a number of deficiencies in the laws that apply to the health sector. The provisions in the NHA relating to patient information are vaguely worded, giving rise to uncertainties in relation to:

- the definition of patient information including what constitutes “health record”;
- the entities obligated to comply with data processing requirements;
- the conditions for the lawful processing of data, for example, the procedure for obtaining consent from the patient before the disclosure of their information is not clear;
- the lack of provisions on data quality;
- the lack of provisions on actual consent by patients before information is obtained;
- the lack of notification requirements;
- the lack of provisions on ownership of patient data
- the lack of provisions on how long patient data is to be retained;
- the non-vesting of information rights in patients, for example, patients do not have right of access to their data; and
- the lack of provisions for third party responsibilities and cross-border transfer of data.

\textsuperscript{57} Section 21(1) of the RTS.
\textsuperscript{58} Section 21(2) of the RTS.
Recommendations

Addressing the deficiencies in the laws applicable to the protection of patient information requires both near- and long-term actions. In the short term, contractual mechanisms should be used to ensure the protection of patient information. This means that health establishments should incorporate provisions on data protection in contracts with service providers.59

In the longer term, the Minister of Health may wish to exercise powers under the NHA to make regulations on patient data protection. Such regulations may borrow from the RTS, which already contains data protection provisions. The regulations should, at a minimum, accord the following rights to users: the right to access data including the right to request changes to the data, the right to control the use of their data, the right to receive notification of data security breaches and the right to compensation where breaches occur.

Conclusion

If Nigeria is to meet its objective of using digital health services to reach the targets set forth by the SOML Initiative and to help enable the achievement of Universal Health Coverage, it is important that it establishes legal frameworks, to facilitate the lawful processing of patient information. Current laws applicable to the health sector do not contain robust safeguards for the processing of user information. The laws that apply to the communications sector contain data protection provisions, which may be borrowed by the health sector. Contractual mechanisms may be used in the interim to safeguard patient data pending the enactment of appropriate data protection laws in the health sector.

59. With respect to third party suppliers, there is the view that absent legislation covering protocols with third parties, the person responsible for collecting the data remains criminally liable for any breaches as contractual responsibility does not beget criminal liability.

The International Standards Organisation’s ISO 27001 which includes a requirement (S6.2.3: Addressing security in third party agreements) may be a useful guide (https://www.iia.org.uk/resources/it-auditing-and-cyber-security/data-security-in-third-party-agreements/).
List of Reviewed Resources

Constitution of the Federal Republic of Nigeria

Dangerous Drug Act

Medical and Dental Practitioners Act
http://www.nassnig.org/document/download/1068

National Archives Act
http://www.nassnig.org/document/download/210

National Drug Formulary and Essential Drug List Act

National Health Act
(currently unavailable online)

National Identity Management Commission Act

National Information Technology Development Agency Act

National Planning Commission Act

National Population Commission Act

Nigerian Communication Commission Act

Optometrist and Dispensing Opticians (Registration) Act

Orthopedic Hospital Management Board Act

Pharmacist Council of Nigeria Act
http://www.nassnig.org/document/download/1126

Psychiatric Hospitals Management Board Act
http://www.nassnig.org/document/download/708

Quarantine Act

Revised National Health Policy of 2004

National Policies on integrated Disease and Surveillance and Response

National Strategic Health Development Plan (NSHDP) 2010-2015

Health Metrics Network, Framework and Standards for country health information Systems
http://www.who.int/healthmetrics/documents/hmn_framework200803.pdf

National Information Systems and Network Security Standards & Guidelines