Author

David Ekanem
Associate
davidekanem@sskohn.com

# *Evaluation of Telemedicine in Nigeria and Cybersecurity Concerns*

## Introduction

Telemedicine has appeared as a transformative force in global healthcare, offering remote medical consultations and services through digital communication technologies. In 2020, during the pandemic, a lot of countries used telemedicine to combat diseases while physical contact was prohibited. In Nigeria, there are various functional consulting services operated by groups of private doctors using web chats, text messages, specialized apps, video calls, and audio calls. The services include drug prescriptions, patient referrals, patient monitoring, and provision of information about various hospitals. However, the success of telemedicine in Nigeria depends on a comprehensive examination that considers both its benefits and drawbacks, with a particular emphasis on cybersecurity issues.

The regulatory framework surrounding telemedicine in Nigeria is also examined, shedding light on the existing regulations. The article advocates for the development of comprehensive and up-to-date regulations tailored to the evolving telemedicine practice, ensuring a balance between innovation and data protection.

Also, the article proposes strategies and recommendations to enhance data privacy within the telemedicine sphere in Nigeria. It emphasizes the importance of robust cybersecurity measures, regulatory compliance, and public awareness campaigns. By addressing these critical issues, the article seeks to contribute valuable insights to policymakers, healthcare practitioners, and technology developers, fostering a secure and resilient telemedicine practice that aligns with global best practices while catering to Nigeria's healthcare Sector.

## Overview of Telemedicine

Telemedicine, with the prefix *tele*, has its etymological root in Greek which means far or at a distance. Hence the merging of the words tele and medicine means medicine over a distance. The World Health Organization (WHO) defined Telemedicine as the delivery of health care services at a distance using

electronic means for ailment diagnosis, prevention, and treatment of illnesses.[1] Telemedicine, broadly defined as the remote delivery of healthcare services using telecommunications technology, encompasses a wide range of applications, including teleconsultations, telemonitoring, and tele-education.[2]

With telemedicine, a patient can know how to get treatment receive a diagnosis, and receive a prescription, from the comfort of his/her home. Telemedicine originally started with the use of telephones but has now expanded to include apps, video software, video conferencing, etc.[3]

A practical example of telemedicine is where a patient sends photos to her dermatologist for evaluation and communicates with him through text. Some telemedicine platforms require a form of quiz to be taken to avail the healthcare personnel a better understanding of the situation and it is then followed by prescriptions from the dermatologist based on the evaluation.[4]

One of the most significant advantages of telemedicine is its ability to ease timely access to healthcare services, particularly in remote or rural areas where healthcare facilities are scarce. Through teleconsultations, patients can connect with healthcare providers virtually, receive medical advice, and even obtain prescriptions without the need for physical visits to healthcare facilities. This not only saves time and travel costs but also ensures continuity of care, especially for patients with chronic conditions.[5]

Moreover, telemedicine enables healthcare providers to reach a broader patient population, transcending geographical barriers and expanding their reach beyond traditional healthcare settings. With the proliferation of smartphones and internet connectivity, telemedicine platforms offer unprecedented convenience, allowing patients to access healthcare services from the comfort of their homes or workplaces. This accessibility is particularly beneficial for individuals with mobility issues, busy schedules, or limited access to transportation.

---

[1] M Serper, ML Volk, 'Current and Future Applications of Telemedicine to Optimize the Delivery of Care in Chronic Liver Disease' 2018 Feb 16 (2): 157-16 Clin Gastroenterol Hepatol <https://www.ncbi.nlm.nih.gov/pubmed/29389489> accessed 11 April 2024

[2] J Smith, Dividing E-Health, Telehealth and Telemedicine' (Electronic Health Reporter, 20 March 2020) <https://electronichealthreporter.com/dividing-e-health-telehealth-and-telemedicine/> accessed 11 April 2024

[3] G Roberts-Grey, 'What is Telemedicine and how does it work?' (*GoodRx*, 12 October 2020) <https://www.goodrx.com/blog/what-istelemedicine/#:~:text=Since%20the%201950s%2C%20healthcare%20providers,in%20a%20variety%20of%20ways.> accessed 11 April 2024

[4] M Maheu and others; *E-Health, Telehealth, and Telemedicine A Guide to Start-Up and Success* (United States, Jossey-Bass, 2001)

[5] M Serper, ML Volk, 'Current and Future Applications of Telemedicine to Optimize the Delivery of Care in Chronic Liver Disease' 2018 Feb 16 (2): 157-16 Clin Gastroenterol Hepatol

Furthermore, telemedicine plays a crucial role in enhancing healthcare delivery efficiency and reducing healthcare costs. By minimizing the need for in-person consultations and hospital visits, telemedicine helps alleviate the burden on healthcare facilities, streamline healthcare workflows, and optimize resource utilization. Additionally, remote patient monitoring technologies enable continuous monitoring of vital signs and health parameters, allowing healthcare providers to intervene proactively and prevent medical emergencies, thereby reducing hospital readmissions and healthcare expenditures.

*Types of Telemedicine*

1. **Store and Forward Telemedicine**: This is commonly used in specialties like dermatology and otolaryngology. It involves collecting clinical information, storing it securely in a cloud-based platform, and then sending it electronically to another site for expert opinion.[6] An example includes sending images of a skin condition to a dermatologist for diagnosis and treatment. This method is less reliant on internet connectivity but does not allow for direct patient examination.
2. **Real-time Telemedicine**: This involves live consultations between doctors and patients, replacing the need for in-person visits and offering immediate results. It typically utilizes video calls and requires high bandwidth and constant internet connectivity.[7]
3. **Remote patient monitoring**: This entails continuously monitoring a patient's physiological data, such as heart rate and oxygen levels, through medical technology. This approach is often used for elderly individuals, those with special needs, and neonates to track their health remotely.

## Telemedicine in Nigeria

Telemedicine in Nigeria has gotten a larger acceptance due to the 2020 COVID-19 pandemic, which has led to Nigerians seeking access to health care without having to visit the hospital and risk contracting disease while in transit or at the facility.

It all started in 2006 when a pilot project was initiated by the National eGovernment Strategies Ltd to introduce telecardiology utilizing video conferencing and digital equipment. Following this, in 2007, the National Space Research and Development Agency (NASRDA), in collaboration with the

[6] S Gogia, Fundamentals of Telemedicine and Telehealth (London, Academic Press, 2020)
[7] O'Brien, 'The Definitive Guide to Telemedicine: History, Benefits, Implementation and Everything Else' (RingCentral, 20 August 2020) <https://www.ringcentral.co.uk/blog/what-is-telemedicine/#ring-uk> accessed 15 April 2024

Federal Ministry of Health, launched a telemedicine pilot project via NIGCOMSAT-1, a geostationary communication satellite. This initiative aimed to enhance emergency healthcare delivery, telemonitoring, intensive healthcare, and cross-border teleconsultation services, particularly benefiting rural communities.[8] Notably, this facility has also played a role in mobile coronavirus testing.[9] This project was launched in two teaching hospitals and six federal medical centres spanning the country's six geopolitical zones. The selected teaching hospitals were the University College Hospital in Ibadan and the University Teaching Hospital in Maiduguri. Federal medical centers involved in the project were in Owo, Gombe, Makurdi, Yenagoa, Birnin Kebbi, and Owerri. Alongside public institutions, private entities such as Lagoon Hospital in Lagos and Igbinedion University Teaching Hospital in Benin also embraced telemedicine technology.[10]

Additionally, in 2010, a telecommunications service provider introduced a service allowing customers to consult health personnel over the phone, albeit at a costly rate of N100 per minute, discouraging widespread use.[11] Subsequently, in the same year, Suburban West Africa, an Indian telecommunications provider, implemented a telemedicine project in Nigeria, connecting university-based medical experts at the National Hospital in Abuja with the National Sickle Cell Foundation in Lagos via teleconferencing technology.[12]

Similarly, the Lagos state government has made significant strides in telemedicine adoption, exemplified by the implementation of the e-health project in 2009. Initially launched as an interactive Hospital Management Information System (HMIS), this project aims to leverage ICT to enhance healthcare accessibility, quality, and service delivery volume.[13] Notably, it facilitates teleconsultation services between primary healthcare centres, general hospitals, and federal hospitals.

---

[8] A Felix, 'On National e-Healthcare Delivery Through Nigcomsat-1' (2014) 3 Issue 1 IJERT <https://www.ijert.org/research/on-national-e-healthcare-delivery-through-nigcomsat-1-IJERTV3IS10620.pdf> accessed 15 April 2024

[9] Space in Africa, 'Nigerian Space Agency Launches Telemedicine Facility to Support Covid-19 Testing in Nigeria' (Space in Africa, 9 April 2020) <https://africanews.space/nigerian-space-agency-launches-telemedicinefacility-to-support-covid-19-testing-in-nigeria/> accessed 15 April 2024

[10] K Ukaoha, 'Prospects and challenges of telemedicine in Nigeria' (2012) 3(1) 65 Journal of Medicine and Biomedical Sciences - <https://www.researchgate.net/publication/272877000_Prospects_and_challenges_of_telemedicine_in_Nigeria/citations> accessed 16 April 2024

[11] Ibid.

[12] T Fatunde, 'NIGERIA: Telemedicine arrives at Lagos' (University World News, 17 January 2010) <https://www.universityworldnews.com/post.php?story=20100114190633688>

[13] A Balogun, 'E-Health (Telemedicine and Healthcare in Lagos State, Nigeria' <https://www.ha.org.hk/haconvention/hac2016/proceedings/downloads/IHF2.2.pdf>

Currently, there are several companies that have adopted the use of Telemedicine in Nigeria. They include: Mobihealth International, iWello, Tremendoc, mDoc, 1Dokita Healthcare Ltd, and others.

## Laws Regulating Telemedicine in Nigeria

Currently, there is no legislation regulating telemedicine in Nigeria. However, it is pertinent to look at existing laws and guidelines on the practice of telemedicine.

i. **The Nigeria Data Protection Act of 2023 (NDPA)**
The NDPA serves as the primary legislation governing the safeguarding of personal data belonging to Nigerian citizens. It establishes a legal framework outlining rules and criteria for the gathering, handling, retention, and transmission of personal information within Nigeria. Applicable to all entities responsible for managing or utilizing personal data within Nigerian borders, including healthcare providers involved in telemedicine, this Act delineates essential standards and procedures to ensure data protection and privacy.

ii. **The 1999 Constitution of the Federal Republic of Nigeria (CFRN)**
By virtue of the provision of Section 37 of the CFRN which focuses on the protection of the privacy of citizens, homes, telephone conversations and communications, it places obligations on health professionals using telemedicine to ensure that medical records and health information of patients are protected.

iii. **The National Information Technology Development Agency (NITDA) Act 2007**
The NITDA Act of 2007 is instrumental in governing and advancing telemedicine services within Nigeria. It establishes a legal foundation for the development of ICT systems that facilitate telemedicine, setting standards and regulations for their implementation and operation. Recognizing the significance of ICT in healthcare delivery, the Act emphasizes the necessity of regulating ICT systems supporting telemedicine services. Section 6 specifically mandates NITDA to formulate guidelines for deploying IT systems across various sectors, including healthcare.

iv. **Code of Medical Ethics 2008**
A unique legal basis for telemedicine is provided by Section 22 of the Code of Medical Ethics. It mandates medical practitioners to exercise caution, emphasizing confidentiality, appropriate equipment use, patient referral, consultant professionalism, and specialist registration status. Additionally, it requires practitioners to secure personal information transmitted electronically

and during data storage. However, the Code lacks comprehensive coverage, notably omitting standards of care, privacy, informed consent, confidentiality, data security, and permissible treatments in telemedicine.

v. **National Health Act 2014**
Section 29 of the National Health Act requires health institutions to implement preventive measures against unauthorized access to patients' health records and storage systems. Failure to comply may result in imprisonment for up to two years and/or a fine of N250,000.

vi. **Medical and Dental Practitioners Act (MDPA) 2004**
The MDPA regulates the medical and dental profession, prescribing punitive measures for misconduct. It outlines registration and licensing requirements for medical doctors and establishes the Medical and Dental Council responsible for setting professional standards. However, it is suggested that the Act be amended to include provisions for the training and licensing of telemedicine practitioners, ensuring they possess requisite skills and understand telemedicine's standard of care. Additionally, incorporating telemedicine education into medical school curricula is recommended.

## Cybersecurity Concerns in Telemedicine

While telemedicine offers numerous benefits, it also presents inherent challenges, particularly concerning data privacy and security. Telemedicine involves the transmission, storage, and processing of sensitive medical information, including patients' personal health records, diagnostic images, and treatment plans. Ensuring the confidentiality, integrity, and availability of this data is essential to maintaining patient trust and compliance with regulatory requirements.

In Nigeria, where data privacy laws are still evolving, telemedicine providers face unique challenges in safeguarding patient data. Section 44 of the Code of Medical Ethics stipulates that medical practitioners are bound to keep privileged information received from patients confidential, with disclosure permitted only with the patient's explicit consent, a duty that persists even after the patient's demise. Additionally, Section 27 of the National Health Act allows healthcare providers to disclose patient information to other parties or providers for legislative purposes within their professional scope. One of the primary concerns is the risk of unauthorized access, interception, or disclosure of medical information during data transmission over the Internet or mobile networks as a result of weak or lacking firewalls, unsecured networks, unencrypted information, weak authentication protocols, etc.

**Third-party risks**

The nature of telemedicine involves interactions with various third parties, such as telemedicine apps or websites, which may share sensitive data like location and contacts. There is a risk of interception of medical information during transmission through telemedical links. Furthermore, non-medical personnel involved in healthcare delivery, like IT staff and administrative support, pose a risk of unauthorized access to health data. Additionally, browsing websites for healthcare information may lead to the tracking and storing of personal data for other purposes, necessitating options for users to control data tracking. Without robust encryption protocols and secure communication channels, patient data may be vulnerable to interception by malicious actors, compromising patient privacy and confidentiality.

To mitigate these risks, telemedicine providers must implement robust security measures, including data encryption, organizational policies for handling confidential data, firewalls, and secure emailing systems. Furthermore, protocols should be established to verify the identities of both patients and providers. The challenge lies in regulating the disclosure of personal information to third parties, as demonstrated by a 2017 class-action lawsuit against MDLive, alleging unauthorized sharing of patient health information with a third-party provider. MDLive defended its actions by stating that consumers are informed in its privacy policy of potential disclosure to contracted third parties.[14]

**Data Sovereignty and Jurisdictional Challenges**

The storage and processing of patient data on telemedicine platforms raise concerns about data sovereignty and jurisdictional issues. Many telemedicine platforms are hosted on cloud servers located outside Nigeria, raising questions about the jurisdictional authority and legal protections governing the storage and processing of Nigerian patients' data. In the absence of clear regulatory frameworks and international data transfer agreements, patients' data may be subject to foreign laws and regulations, potentially undermining their privacy rights and legal recourse.

**Medical devices and wearable security**

Additionally, the proliferation of mobile health (mHealth) applications and wearable devices aggravates data privacy concerns, as these technologies collect vast amounts of personal health data, including biometric information,

[14] J Comstock, 'MDLive faces class action suit over alleged data privacy breach' (Mobihealthnews, 25 April 2017) <https://www.mobihealthnews.com/content/mdlive-faces-class-action-suit-over-alleged-data-privacybreach> accessed 17 April 2024

activity levels, and geolocation data.[15] The integration of these data sources with telemedicine platforms raises ethical and regulatory questions about informed consent, data ownership, and data sharing practices. Without adequate safeguards and transparency measures, patients may unknowingly consent to the collection and sharing of their health data, exposing them to privacy risks and potential exploitation by third parties.

**Unpatched or outdated software used by consumers**

Telemedicine involves the use of software applications and platforms to provide healthcare services remotely. These software applications, if not regularly updated or patched, can become vulnerable to cyberattacks. Cybercriminals often exploit known vulnerabilities in unpatched software to gain unauthorized access to systems and data. This is because many consumers lack the technical knowledge to properly manage software updates and patches on their devices.

## Conclusion/Recommendations

Telemedicine holds immense promise for transforming healthcare delivery in Nigeria, offering unprecedented access, convenience, and efficiency in healthcare services. However, ensuring the privacy and security of patient data is paramount to building trust, protecting patient rights, and fostering the sustainable growth of telemedicine practices. By implementing robust regulatory frameworks, ethical guidelines, and cybersecurity measures, Nigeria can harness the potential of telemedicine while safeguarding patient privacy and advancing healthcare for all.

This work recommends as follows:

1. There is a need to explore the integration of emerging technologies such as blockchain, the Internet of Things (IoT), and artificial intelligence (AI) to enhance the protection of patient data in telemedicine practices.

2. Telemedicine providers should appoint a proficient Data Protection Officer. This appointed individual will serve as a focal point for all matters related to data privacy, diligently overseeing the handling, storage, and transfer of sensitive patient information.

3. Telemedicine providers should collaborate with cybersecurity organizations to gain insights into implementing effective data protection measures and addressing cyber threats.

[15] Providers and Business Leaders Beware: Telemedicine Security & Privacy Risks' (Virtru, 12 November 2020) <https://www.virtru.com/blog/telemedicine-privacy-security/>

4. Healthcare providers should establish comprehensive policies, procedures, and protocols to ensure optimal protection of patient data against cyber breaches, considering factors like multifactor authentication, data encryption, antivirus software, and software updates.

5. Organizations offering telemedicine services must develop and enforce policies to safeguard information confidentiality.

6. Regulatory bodies should define the responsibilities of technology platforms, such as websites and mobile apps, offering telemedicine services to patients. Clarity should be provided on the appropriateness of using Artificial Intelligence for patient advisories and treatment prescriptions.

7. Government-led awareness and sensitization campaigns are crucial to disseminate information about telemedicine's benefits and opportunities. This initiative will help increase public understanding and acceptance of telemedicine services.

8. There is a need for comprehensive regulation governing telemedicine practices. Legislators should ensure that such regulations account for the unique characteristics of Nigerian society and the healthcare landscape. It is essential to develop regulations that are tailored to local needs and challenges rather than simply transplanting foreign laws.

9. Healthcare providers and telemedicine platform developers need to work together to ensure that software updates and patches are applied promptly. This could involve providing clear instructions to consumers on how to update software, or even automating the update process where possible.