International Comparative Legal Guides

Digital Health 2020

A practical cross-border insight into digital health law

First Edition

Featuring contributions from:

Advokatfirma DLA Piper KB
Astolfi e Associati, Studio Legale
Baker McKenzie
Biopharmalex
Bird & Bird LLP
Cliffe Dekker Hofmeyr
D'Light Law Group
GVA Law Office
Hammad & Al-Mehdar Law Firm
Herbst Kinsky Rechtsanwälte GmbH
Hoet Pelaez Castillo & Duque
Kemp Little LLP
Kyriakides Georgopoulos Law Firm
LEĜA
LexOrbis
Llinks Law Offices
Machado Meyer Advogados
Mason Hayes & Curran
McDermott Will & Emery LLP
OLIVARES
Polsinelli PC
Quinz
Gilat, Bareket & Co., Reinhold Cohn Group
Shook, Hardy & Bacon L.L.P.
The Center for Healthcare Economics and Policy, FTI Consulting
TripleOKLaw LLP Advocates
VISCHER

ICLG.com

ISBN 978-1-83918-027-9
ISSN 2633-7533

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Group Publisher
Rory Smith

Associate Publisher
James Strode

Senior Editors
Suzie Levy
Rachel Williams

Sub Editor
Lucie Jackson

Creative Director
Fraser Allan

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Digital Health 2020

First Edition

Contributing Editor:
William A. Tanenbaum
Polsinelli PC

Expert Chapters

Q&A Chapters

Kenya


John M. Ohaga


Stephen Mallowah


Catherine Kariuki


Janet Othero

TripleOKLaw LLP Advocates

1 Digital Health and Health Care IT

1.1 What is the general definition of "digital health" in your jurisdiction?

In Kenya, digital health is synonymously used with the term **eHealth** which finds its place in legislation, i.e. the Health Act of 2017, and which is defined as "the combined use of electronic communications and information technology in the health sector including telemedicine".

1.2 What are the key emerging technologies in this area?

The key emerging technologies in digital health are:

Telehealth: The use of telecommunications and virtual technology to deliver healthcare outside of traditional healthcare facilities.

Telemedicine: The remote delivery of healthcare services over telecommunication infrastructure e.g. video conferencing. The Kenyan government in May 2015 launched a first phase of a national telemedicine initiative for the poor and the marginalised as one of the programmes that will help to tackle non-communicable diseases.

Mobile health (**mHealth**): Involves delivering medical services using mobile technologies. In 2013, Kenya's Mobile Post Exposure Prophylaxis (**mPEP**) initiative was developed through a public-private partnership initiative with mHealth Kenya and the Centre for Disease Control and Prevention Foundation (**CDC**).

Integrated Hospital Management Information System (**HMIS**): Is an element of health informatics that focuses mainly on the administrational needs of hospitals.

1.3 What are the core legal issues in health care IT?

The following are the core issues that affect healthcare IT:

- **Protection of data regarding the health status of an individual by the Data Protection Act**: The health status of an individual falls squarely within two classes of data as envisioned by the Data Protection Act, 2019 (**DPA**). The first is the definition of "sensitive personal data" which has been defined as data revealing the natural person's health status, genetic data of the data subject amongst other components. The second is "health data" which is data related to the state of physical or mental health of the data subject.

  The DPA provides guidance regarding the processing of personal data relating to health. Notably, personal data relating to the health of a data subject may only be processed by or under the responsibility of a healthcare provider; or by a person subject to the obligation of professional secrecy under any law.
- **The duties of the data controller and data processor under the DPA**: Section 18 of the DPA, states that bodies designated as data controllers and data processors must register with the Office of the Data Commissioner. The DPA imposes several obligations on processors and controllers. Including registration with the data commissioner, duties corresponding to data subjects' rights, etc.
- **Profiling and automated processing of health data**: Section 35 of the DPA states that every data subject has a right not to be subject to a decision based solely on automated processing, including profiling which produces legal effects or significantly affects the data subject. This binds healthcare IT providers as they contract with data subjects.
- **The prioritisation of data regarding HIV Patients as outlined under the HIV/AIDS Prevention and Control Act, 2006**: The Act necessitates technology providers who intend to store and analyse data regarding HIV patients to accordingly create robust digital frameworks which use encryption and pseudonymisation techniques to further protect the identities of such data subjects.
- **Prohibited disclosure of information in respect of HIV/AIDS Patients under the HIV and AIDS Prevention and Control Act, 2006**: Under Section 22 of the Act, persons in possession of any information regarding the result of a HIV test or any related assessments to any other person are expressly prohibited from disclosing that information, except through numerous exemptions identified therein.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The Constitution of Kenya, 2010

Access to healthcare is a fundamental right and freedom enshrined under Article 43 (1) (a) of the Constitution providing in part that "every person has the right to the highest attainable standard of health, which includes the right to healthcare services…". The integration of digital healthcare into the health sector contributes towards achieving this standard. Article 31 also guarantees the right to privacy for all citizens in relation to their personal information.

Health Act, 2017
This Act aims to regulate health products and health technologies. Section 104 of the Act provides that within three years from the operation of the Act, the Cabinet Secretary responsible for healthcare shall ensure the enactment of legislation that provides for the collection and use of personal health information, management of disclosure of personal health information, protection of privacy, health service delivery through M-Health, E-learning and telemedicine, E-waste disposal and health tourism.

In addition, Sections 103–105 of the Health Act protects and regulates the use of eHealth in the collection, retrieval, processing, storage, use and disclosure of personal health information.

Public Health Officers (Training, Registration and Licensing), 2013
This Act provides for the training, registration and licensing of public health officers and public health technicians.

Mental Health Act
This Act amended and consolidated the law relating to the care of persons suffering from mental disorders, or mental sub-normality with a mental disorder, for the custody of these persons, management of their properties, management and control of a mental hospital and for custodial purposes.

HIV and AIDS Prevention and Control Act 2006
This Act is designed to provide measures for the prevention, management and control of HIV and AIDS, to provide for the protection and promotion of public health and for the appropriate treatment, counselling, support and care of persons infected or at risk of HIV/AIDS.

2.2 What other regulatory schemes apply to digital health and health care IT?

The other regulatory schemes that apply are:

Health Records and Information Managers Act, 2016
The Act provides for the training, registration and licensing of the health records and information managers. It provides for the establishment, powers and functions of the Health Records and Information Managers Board.

Kenya Information and Communication Act, 2009
The Act provides for the establishment of the Communications Authority of Kenya whose mandate is to license and regulate postal, information and communication services in accordance with the Act.

Access to Information Act, 2016
The Act gives effect to Article 35(1) of the Constitution which states that "Every citizen has the right of access to: (a) information held by the State; and (b) information held by another person and required for the exercise or protection of any right or fundamental freedom". This enables individuals to access their medical records that are held in any medical institution.

Data Protection Act
Section 46 of the Act addresses personal data relating to health and provides that personal data relating to health of a data subject may only be processed: (a) by or under the responsibility of a healthcare provider; or (b) by a person subject to the obligation of professional secrecy under any law.

2.3 What regulatory schemes apply to consumer devices in particular?

The following laws govern the standards and quality of consumer devices in Kenya:

Consumer Protection Act, 2012
The Act provides for the protection of the consumers and prevents unfair trade practices in consumer transactions. Section 5 of the Act provides for the supplier of goods and services warranting that they are of a reasonable merchantable quality. The same is provided for under the Sale of Goods Act Section 16.

Standards Act
The Act promotes and provides the standardisation of the specification of commodities.

2.4 What are the principal regulatory authorities? What is the scope of their respective jurisdictions?

The following lists the principal regulatory authorities:

The Ministry of Health
Section 15 of the Health Act mandates the Ministry of Health to formulate health policy and regulation, provide national referral health facilities, capacity building and provide technical assistance to counties.

Kenya Bureau of Standards
It is established under Section 3 of the Standards Act and is mandated to inspect imports based on standards required by the Act.

The Consumer Protection Committee
The Committee is established under Section 89 of the Consumer Protection Act 2012 and part of its function is to include formulating policies relating to the Act in the interest of consumers, promotion or participation in consumer education and providing advice to consumers on their rights and responsibilities regarding the law.

Kenya Medical Supplies Authority (KEMSA)
This is a state corporation under the Ministry of Health established under the KEMSA Act 2013 whose mandate includes to procure, warehouse and distribute drugs and medical supplies for prescribed public health programmes, the national strategic stock reserve, prescribed essential health packages and national referral hospitals.

2.5 What are the key areas of enforcement when it comes to digital health and health care IT?

The following are the key areas of enforcement in digital health and healthcare IT:

1. Patient management in the case of patients with chronic diseases where the specific interface to be used will need to be built around patients and their need for effectiveness.
2. Data collection of patient details and reporting on their progress.
3. Administration/management of different healthcare.
4. Stock and supplies management in hospitals.
5. Service delivery (vaccines, family planning, maternal and childcare, HIV treatment and support).
6. Clinical decision support and alerts.

2.6 What regulations apply to Software as a Medical Device and its approval for clinical use?

The following regulations apply to Software as a Medical Device and its approval for clinical use:

1. **The Pharmacy and Poisons Act, Cap 244 (2002) and the Guidelines on Submission of Documentation for Registration of Medical Devices**
   The Kenya Pharmacy and Poisons Board supervises medical device regulation. Under the guidelines, a medical device means among others, **software** or any other similar or related article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific defined purposes.
2. **The KEBS Guidelines for Inspection of Imported Medical Devices, Food Supplements, Medical Cosmetics, Herbal Products and Other Borderline Products** provides that importers have to apply for Pre-Export Verification of Conformity as the first step of initiating importation of any medical devices in order to obtain Certificates of Conformity from KEBS.
3. **Global Harmonisation Task Force for Medical Devices Guidance Documents**
   This task force encourages a convergence in standards and regulatory practices related to the safety, performance and quality of medical devices. It provides publications of harmonised guidance documents for basic regulatory practices.

3 Digital Health Technologies

3.1 What are the core issues that apply to the following digital health technologies?

- **Telehealth**
  Licensure: The legal requirements for licensure and other requirements based on geolocation can prove to be a hurdle for telehealth providers in relation to patient data collection, patient data storage and mandatory tests during the provisioning of healthcare services.
  Payments ecosystem: Since telehealth cuts across multiple geolocations, areas that have adopted online payment methods and mobile money appeal to telehealth providers.
  Inadequate regulation: The digital health space is mostly unregulated. The convergence of information technology with healthcare requires regulation that contemplates both instances, which is yet to be enacted in the Kenyan legal space.
  The recently enacted Data Protection Act, 2019 addresses data subjects' privacy and as such any data controller or processor is expected to be compliant.
- **Robotics**
  Ethical concerns regarding robotics are a key issue. Questions arise as to how the innovation was achieved, the practice of use and types of robotics used, whether collaborative or embedded.
- **Wearables**
  Its challenges cut across those of telehealth and do it yourself (DIY) healthcare practices. A key issue is unsolicited diagnosis which is only justified when, in the case of using a mobile application, it is from a regulated and licensed healthcare institution or a third party that has partnered with such an entity.
- **Virtual Assistants (e.g. Alexa)**
  The main issue regarding Virtual Assistants is how the collection and processing of data is done. These factors are mostly guided by the rights of the data subject as provided for in the Data Protection Act, 2019. Another key issue is lack of certification for healthcare diagnosis.
- **Mobile Apps**
  Key issues regarding mobile applications are ideally centred on Intellectual Property rights granted to the developers of the product. Additional concerns include: guarantee of data privacy; consumer protection issues revolving around consumer terms and conditions; limited internet connectivity and poor mobile phone market penetration rates.
- **Software as a Medical Device**
  A key issue is the user's trust of the software which hampers its acceptance in the healthcare ecosystem. Additionally, stifling regulatory requirements are a hurdle to the full implementation of software in offering healthcare solutions. Data privacy laws regard a patient's health data as a special category of data that has to be handled in a special way and this does not leave a lot of wiggle room for innovative technologies.
- **AI-as-a-Service**
  Unsolicited diagnosis is an issue that cannot be ignored, as well as collection of personally identifiable information which can easily lead to profiling that is regulated under the Data Protection Act.
- **IoT and Connected Devices**
  The challenges associated with the application of these include: human device interaction; interoperability of various IoT devices; and data sharing with healthcare providers and other third parties. There are a lot of grey areas that need to be addressed by the law.
- **Natural Language Processing**
  Issues unique to this include but are not limited to: bias on accents; lack of adequate regulation; and lack of certification for healthcare diagnosis.

3.2 What are the key issues for digital platform providers?

Data Protection: Digital platform providers who process personal information are required to be compliant with Article 31 of the Constitution which guarantees privacy for all citizens in relation to their personal information. The DPA (2019) also provides in detail requirements to be satisfied by all data controllers and processors before processing any personal information relating to Kenyan residents.

Cyber security: The Data Protection Act imposes some cyber security requirements on data controllers and processors of personal information. Notably, Kenya has domesticated the Budapest Convention on Cybercrime in the form of the Computer Misuse and Cybercrimes Act.

4 Data Use

4.1 What are the key issues to consider for use of personal data?

The use of personal data is primarily governed under the provisions of the DPA which heavily mirrors the GDPR (The General Data Protection Regulation 2016/679).

When processing personal data, data controllers and processors ought to ensure that: personal data is processed in accordance with the data subject's right to privacy; it is processed in a lawful and transparent manner; collected for an explicit purpose that is specific and legitimate; adequate, relevant and limited to

the necessary data; accurate and up-to-date with the availability of correction without delay; stored for no longer than required for the intended purposes; and is portable outside Kenya, but only upon consent and proof of adequate safeguards.

4.2 How do such considerations change depending on the nature of the entities involved?

The prevailing right that accrues in processing a data subject's personal information is consent. Data controllers and processors have a duty to notify and inform the data subject on aspects regarding the processing of personal data. However, exceptions to consent exists for the purposes of: legal compliance; public interest; or statutory tasks.

In addition, exercise of rights of data subjects may vary depending on the circumstance of the subject, i.e. where the data subject is a minor and where the data subject has a mental incapacity. In both instances, consent has to be sought from the parent/guardian/administrator.

4.3 Which key regulatory requirements apply?

The use of personal data is primarily governed under the provisions of the Data Protection Act. The DPA gives effect to Article 31 (c) and (d) of the Constitution of Kenya that guarantees the privacy of every person, including the guarantee that they do not have information relating to their family or private affairs unnecessarily required or revealed and not to have the privacy of their communications infringed on.

4.4 Do the regulations define the scope of data use?

Amongst the principles set out in the Act is that the data processor and controller must limit the use of the data to the specific purpose for collecting such information.

A data subject has rights which includes the right to be informed of the use to which their personal data is being put.

4.5 What are the key contractual considerations?

Contracts relating to the collection and processing of data ought to be compliant with the DPA to avoid non-compliance and subsequent penalties. Organisations must consider whether they fall under the category of controller or processor to cater for the responsibilities and relevant liability terms in their contracts. Controllers ought to ensure that their processors sign data processing agreements and that they guarantee certain technical measures are in place in accordance with the DPA. Data residency and data base rights are key terms that should be included in the contracts. Intellectual property rights should also be addressed. Parties that integrate with others should satisfactorily address the issue of exit in case of a termination of the relationship so that the transition is not disruptive to the business and data subject rights are not breached in any way. The data subject onboarding process has to factor in the principles of the Data Protection Act which includes transparency, adequate information and scope of processing the data, as well as the express consent of the customer.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

Some key issues to consider are: the rights of a data subject; the category of the data in question, e.g. special categories; obligations relating to transfer of data out of Kenya; express consent of the data subject; consumer protection issues; and any prescribed data sharing code by the relevant authority.

5.2 How do such considerations change depending on the nature of the entities involved?

In certain circumstances, data controllers or processors are required by law to share certain personal data with e.g., regulators or authorities.

5.3 Which key regulatory requirements apply when it comes to sharing data?

Parts VI and VII of the Data Protection Act will apply when regulating the sharing of data. These relate to the transfer of personal data and exemptions extended to the transfer.

6 Intellectual Property

6.1 What is the scope of patent protection?

Patents in Kenya provide government-granted exclusionary rights for an "invention". Kenya has specific legislation governing patent protection in the form of The Kenya Industrial Property Act of 2001 (**KIPI**). A registered patent is protected for a period of 20 years.

It takes approximately four years to complete the process of registration. The Act expressly prohibits patenting of plant varieties as provided for in the Seeds and Plant Varieties and inventions contrary to public order, morality, public health and safety, principles of humanity and environmental conservation.

6.2 What is the scope of copyright protection?

Copyright protection in Kenya extends to work that is of an original character and has been reduced in material form. Literary, musical, artistic and audio-visual works, sound recordings and broadcasts are all eligible for copyright protection. The Copyright Amendment Act of 2019 amended the Copyright Act of 2001 (**Act**) widened the range of protected subject matter under the Act. The protection period for copyright works is dependent on the category of type.

6.3 What is the scope of trade secret protection?

Currently, Kenya does not have a statute dedicated to trade secrets provided for under Intellectual Property-specific legislation. Enforcement of trade secrets is mostly achieved by common law and equity remedies as well as remedies available for breach of contract.

However, Kenya is a signatory to the Agreement on Trade-Related Aspects of Intellectual Property Rights (**TRIPS Agreement**). The TRIPS Agreement contains, among others, provisions on the protection of trade secrets against their unlawful acquisition, use or disclosure by third parties.

6.4 What are the typical results on academic technology transfer rules?

Technology transfer rules in Kenya are guided by The Science, Technology and Innovation Act of 2013 and corresponding rules to the Act. The Act has made it mandatory for universities and research institutions to have IP policies and technology transfer rules. In order to harmonise the various conflicting interests of stakeholders and achieve broad-based objectives, an intellectual property management policy for universities and research and design institutions should address certain issues listed in the Act.

6.5 What is the scope of intellectual property protection for Software as a Medical Device?

Protection of Software is generally covered by Copyright, Trademark and to some extent, Patents. Copyright protects the various components of a software such as source code, object code and text. Protection, however, does not extend to the underlying idea embodied in the copyrighted software, or to the medium or device used to express the software. Under Kenyan law, registration is not a prerequisite for copyright protection as protection accrues once work that is subject to copyright is reduced to material and permanent form. However, registration is still recommended as it constitutes *prima facie* evidence of copyright ownership. Copyright law currently provides the most convenient available means of encouraging software development because protection is easily obtained and at a minimal cost.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

The Ministry of Health launched the Kenya Health Data Collaborative in May 2016, a mid-term review of the Kenya Health Sector Strategic Plan, a series of data analytics capacity building workshops, and workshops across 33 counties to strengthen civil registration and vital statistics (**CRVS**) have all been successfully completed with the support of HDC partners.

Parties should always be aware of issues relating to data privacy, consumer protection, intellectual property, confidentiality, etc., throughout the contracting process especially where it involves integrating systems to facilitate data flows between the parties.

7.2 What considerations apply in agreements between health care and non-health care companies?

Parties must be careful that they define the scope of their services as narrowly as possible to ensure they do not carry an inordinate amount of legal risk while ensuring compliance. Obligations of each party should be clearly outlined in the contract. Terms relating to audit rights, database rights, IT rights, termination, service level agreements, commercials, etc., must be clearly outlined.

8 AI and Machine Learning

8.1 What is the role of machine learning in digital health?

Machine learning plays a pivotal role in research into genetics, diseases and medicine. With the advanced speed of machine learning research can be fast tracked and optimised for better results.

Machine learning has also improved the process of diagnosis. It can play a key role in the early detection of key symptoms as well as an overall improvement in the speed, quality and accuracy of diagnosis.

8.2 How is training data licensed?

Research data is often released and with this, such data (training and/or research) is required to be licensed prior to the release. There are various forms of licensing in this case. However, they all share some key elements such as an arbitration requirement, a copyleft requirement and/or intent of non-commercial (unless required to be commercial, then the licensor must be paid) parties involved and the domain of the data used (public or private data) will determine how a licence is drawn up as well as the desire to commercialise at a point or not to commercialise.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning without active human involvement in the software development?

The rights can be owned by either party involved in the development and use or a combination of the various stakeholders. An agreement should clarify who owns the particular rights. For instance, the provider of the algorithm can own a portion of the IP and another portion can be owned by the party that provides the knowledge base used to teach the AI, such as a medical institute. The ownership structure could be risk-oriented (sharing the risks involved in any wrong done by the software) or commercially-oriented.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Considerations are geared towards finding the cost of collecting, storing and operating on the data. Publicly accessible data cannot be commercialised. Data with personally identifiable information (**PII**) must be anonymised to protect the identity of the data subjects. Data that is considered to be a knowledge base built over time by the party granting access to the data may be commercialised, provided they own all rights to the data.

9 Liability

9.1 What theories of liability apply to adverse outcomes in digital health?

The realm of digital health is vast, and it transcends everything from a simple Fitbit, m-Health, digital access to medical practitioners and storage of medical records. Accordingly, adverse outcomes also transcend from unpermitted disclosure of a data subject's medical information, to giving treatment in reliance to

inaccurate/erroneous medical data. It is crucial to note that the jurisprudence emanating from the courts with respect to digital health is still growing as the concept of digital health is also still growing, although at an exponential speed having been incorporated into the country's long-term strategic health plans.

As a general rule, the theory that applies to digital health offences is that of negligence. In Kenya, protection of health rights and digital health for that matter take a multi-statutory approach. Take a case of unpermitted disclosure, for example. Under Section 11 of the Health Act, read together with Sections 32 and 46 of the Data Protection Act as well as the medical Practitioners and Dentists Act, medical information is generally confidential unless the data subject consents to the release or in the event of other considerations such as public interest or there being a court order. Article 31(c) of the Constitution speaks to privacy and provides that personal information should not be unnecessarily revealed. Whilst the privacy of medical records enjoys this legal protection, the right to privacy is not an absolute right and it may be limited when necessary. The obligation is, however, on the data controller or processor, as the custodian of such data, to ensure that this data remains private. Under Section 32 of the Data Protection Act, where there is consent, the burden is on the data process to demonstrate so. The data controller/processor has a duty to protect the data subjects' data and where there is a breach, the courts must assess the circumstances under which such data was released and hence, breach of that duty of care.

The Court for instance in *David Lawrence Kigera Gichuki v Aga Khan University Hospital [2014] eKLR* found justification in the release of medical records and held:

i. that a medical practitioner or medical facility is under an obligation not to release confidential information about a patient without the patient's knowledge or consent;
ii. that there are, however, circumstances in which the medical practitioner or institution may be required to release such information for valid governmental and public interest reasons; and
iii. that a medical practitioner or institution may be required by law or a court order to release information about a patient without the patient's consent.

On the flipside, the Court in *Kenya Plantation and Agricultural Workers Union v James Finlay (K) Limited [2013] eKLR* found fault in the release of medical information:

"This issue is of particular concern to the court because under Sub-Article 31(c) of the Constitution, every person has the right to privacy which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed. In the opinion of the court, such right includes the right to have information such as official records, photographs, correspondence, diaries and **medical records** kept private and confidential. It is the further opinion of the court that in the instant case, the respondent in discharge of the duty to uphold medical professional ethics of its medical staff as prescribed in the Rules is obligated to take positive steps to prevent intrusions into the privacy of its hospital's patients."

Similarly, in cases where treatment has been administered based on erroneous records, there will have been a duty of care and the Court will assess, on a case-by-case basis whether there was a breach on such duty. Accordingly, any inimical consequence is tested on a case-by-case basis to establish whether there was negligence as absolute/strict liability is not applicable.

9.2 What cross-border considerations are there?

The Data Protection Act envisions situations where personal data may be transferred outside Kenya and prohibits it. Section 25(h) of the Data Protection Act prohibits the transfer of personal data with a proviso to where there has been consent or proof of data protection safeguards.

The cross-border transfer of data has room for improvement. The DPA, new as it is, also leaves room for such improvement under Section 74, which states that the data commissioner may develop sector-specific guidelines for areas such as health. This will cover situations such as hospitals that buy storage from service providers who are not in Kenya in as much as the custodian of the data is the medical facility in Kenya.

10 General

10.1 What are the key issues in Cloud-based services for digital health?

Data Sovereignty: The location of the data centre should be considered since some sectors such as healthcare information are considered to process sensitive special categories of personal data (in line with the DPA) and thus, the cloud provider should be able to impose rights relating to the data regardless of where it is hosted.

Cyber-threats: The cloud provider has the obligation to provide adequate safeguards that guard against cyber threats in accordance with the Kenya Information Act and the Computer Misuse and Cybercrimes Act.

Cloud infrastructure type: Cloud providers can consider several options such as: infrastructure as a service (**IAAS**); platform as a service (**PAAS**); and software as a service (**SAAS**). Each of these options has its own responsibilities to the cloud provider and digital healthcare provider.

10.2 What are the key issues that non-health care companies should consider before entering today's digital health care market?

Some of the key issues that non-healthcare companies should consider are:

- Applicable laws and regulation to assess the compliance requirements.
- Government Policy.
- Any applicable market standards.
- Consumer protection issues to mitigate reputation risk.
- Peculiarity of the market to assess if its facilitative or prohibitive.

10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital health care ventures?

- Licensing models: Firms can exploit available intellectual property-based commercialisation tools such as licensing and franchising.
- Competition regulation: The Competition Act, 2010 is the law that regulates competition in Kenya. It prohibits restrictive trade practice, controlling mergers and acquisitions and concentration of economic power, aims to protect consumers and the public at large from unfair and misleading market.
- Taxation: The Income Tax Act and subsidiary rules guide taxation of different industries.
- Existing laws and regulations that govern such transactions.

John M. Ohaga is the Managing Partner at TripleOKLaw LLP Advocates and is celebrated as a formidable leader in the firm and the public space as a legal practitioner. His career spans more than 26 years during which he has been involved in numerous complex litigation matters as well as high-value domestic and international arbitration cases. John is acknowledged as an expert practitioner in several areas of law such as administrative law, banking and finance, constitutional law, employment and labour law, public procurement and sports law. He advises numerous blue-chip companies listed on the Nairobi Stock Exchange, many private companies, and some of Kenya's largest state corporations. He sits on the boards of several companies and public tribunals including as Chairman of the Kenyan Sports Disputes Tribunal and the Appeals Committee of the Advertising Standards Board.

TripleOKLaw LLP Advocates
ACK Garden House, 1st Ngong' Avenue
Nairobi
Kenya

Tel: +254 709 830 100
Email: johaga@tripleoklaw.com
URL: www.tripleoklaw.com

Stephen Mallowah is a partner in the Commercial and Corporate Law Department and heads a couple of specialised practice areas in the firm. He has demonstrated expertise in several specialised areas of law, including capital markets and financial services, structured and project finance, energy, mining, oil and gas. He further provides advice to clients on regulatory compliance, public policy and legislative engagement. Steve is constantly pushing the knowledge boundary in emerging areas of practice. This is evidenced by the fact that he is one of the pioneering lawyers in Kenya in the area of Public Private Partnerships and has advised both the public and private side on large PPP projects that successfully achieved commercial and financial close. Steve also heads the firm's new Climate Change and Sustainability Practice.

TripleOKLaw LLP Advocates
ACK Garden House, 1st Ngong' Avenue
Nairobi
Kenya

Tel: +254 709 830 100
Email: smallowah@tripleoklaw.com
URL: www.tripleoklaw.com

Catherine Kariuki is a Deputy Managing partner heading the Technology, Media and Telecommunications (**TMT**) Practice and is a strong advocate for innovation in the legal space. Her work provides advisory on general commercial work, fintech-related transactions, data protection, cyber security-support in digital forensics work, privacy, ownership and governance, consumer protection, intellectual property and mobile payments. Catherine's strength in transactional work and regulatory compliance has enabled her to work seamlessly with several domestic and multi-national companies towards regulatory compliance and business processes and strategy support. Catherine is internationally recognised as a recommended lawyer for Commercial, Corporate and Mergers and Acquisitions and is a frequent speaker at digital disruption and fintech conferences and symposiums.

TripleOKLaw LLP Advocates
ACK Garden House, 1st Ngong' Avenue
Nairobi
Kenya

Tel: +254 709 830 100
Email: ckariuki@tripleoklaw.com
URL: www.tripleoklaw.com

Janet Othero is a partner and one of the brains behind our cutting-edge practice in telecommunications regulations and technology in the financial sector. She has experience in contract negotiations, regulatory due diligence and general legal advisory, having worked with several leading financial institutions. With her understanding of digital disruption, Janet continuously advises clients on the legal implications arising from cyber security to cyber resilience and handling the interrelated impact. She has also gained expertise in Fintech, Regtech, payment systems and data privacy governance. She is internationally recognised as a next generation lawyer for her work in Banking, Finance and Capital Markets and is a regularly featured speaker at conferences and symposiums on digital disruption and Fintech symposiums.

TripleOKLaw LLP Advocates
ACK Garden House, 1st Ngong' Avenue
Nairobi
Kenya

Tel: +254 709 830 100
Email: jothero@tripleoklaw.com
URL: www.tripleoklaw.com

TripleOKLaw LLP is a full-service law firm founded in Kenya in 2002. The firm is renowned for its innovative and professional legal services in the local and international space.

A strong background in corporate and commercial law practice coupled with robust technology-based internal systems inspired a well-informed and practised Telecommunications, Media and Technology team. The innovative practice area advises clients on regulatory compliance, data protection and policies, digital forensics and more aspects affecting clients in the telecommunications, fin-tech, payments and technology industries.

The firms commercial work supports our clients' various needs in legal advisory services on mergers & acquisitions, legal due diligence, joint ventures, corporate restructurings, public private partnerships, corporate governance, regulatory compliance, company secretarial services and commercial contracting.

www.tripleoklaw.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group