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

South Africa

Christoff Pienaar

Nikita Kekana

Cliffe Dekker Hofmeyr

1 Digital Health and Health Care IT

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

The Department of Health in South Africa has published the National Digital Health Strategy for South Africa 2019–2024 ("**SA Health Strategy**"). In terms of the SA Health Strategy, digital health is defined as the use of information and communications technology for health to do things such as treat patients, pursue research, educate students, track disease and monitor public health.

1.2 What are the key emerging technologies in this area?

One key trend in South Africa is the use of 3D printers in the medical sector. For instance, at the Steve Biko Academic Hospital, doctors completed the world's first middle ear transplant using 3D-printed middle ear bones.

The use of robotics is also being introduced to surgery within South Africa. Africa's first full knee replacement operation using a robotic arm-assisted surgery system was conducted in South Africa. More and more physicians are getting qualified to perform robotic surgeries.

The South African National Blood Service has developed its own drones for the transportation of blood.

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

The core legal issues in healthcare IT in South Africa are data protection, ownership of the digital health technology (especially copyright issues concerning big data and artificial intelligence), regulation (particularly the health and safety in using digital health technology) and dispute resolution.

With the advancement of technology, data including big data is now being analysed and used to develop medical technologies and services. So, there is an increased focus on data protection and regulating the processing of personal information.

With the development of many different types of technology, the determination of usage rights, licensing rights and ownership of such technology is critical.

There is pressure to keep up with the developmental trends in the digital health sector and regulate this sector in a way that protects the safety of patients without stifling innovation.

There is also a need to resolve disputes in this sector swiftly and efficiently so as not to jeopardise access to the technology but at the same time uphold fair judicial process and the rule of law.

2 Regulatory

2.1 What are the core health care regulatory schemes?

The core pieces of legislation applicable in the health sector are the National Health Act 61 of 2003, the Medicines and Related Substances Act 101 of 1965, the Medicines and Related Substances Amendment Act, 14 of 2015 and the Health Professions Act No. 56 of 1974.

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

The Protection of Personal Information Act 4 of 2013 is the core legislation dealing with data protection in South Africa and is key to the digital health sector. The Information Regulator is the responsible regulatory authority.

2.3 What regulatory schemes apply to consumer devices in particular?

The Consumer Protection Act 68 of 2008 ("**CPA**") and aspects of the Electronic Transactions and Communications Act 25 of 2002 are the main pieces of legislation that apply to consumers and consumer devices. The CPA has the following regulatory bodies: the National Consumer Commission; Consumer Goods and Services Ombud; and National Consumer Tribunal, who all help enforce consumer protection, consumer rights and resolve disputes in South Africa.

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

There are the following principal regulatory authorities:

The South African Nursing Council ("**SANC**") who are responsible for establishing, improving and controlling the nursing practice in South Africa and standardising nursing education and training.

The Healthcare Professions of South Africa ("**HPCSA**") which is mandated to promote health within South Africa, determine the standards of professional education and training, and set and maintain standards of ethical and professional practice of healthcare professionals in South Africa.

The South African Pharmacy Council which is an independent, self-funded, statutory body mandated in terms of the Pharmacy Act, 1974 (Act 53 of 1974) that regulates the pharmacy

profession in South Africa and is authorised to register pharmacy professionals and pharmacies, control pharmaceutical education, and ensure good pharmacy practice.

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

The provision, manufacturing and wholesaling of medical substances and medical devices is carefully legislated and overseen by the South African Health Products Regulatory Authority. Medical practitioners, including those that may operate online, need to be properly qualified and registered with the Healthcare Professions of South Africa.

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

The core legislation that applies is the Medicines and Related Substances Act, 1965 (Act 101 of 1965) and the GN 1515 of 9 December 2016 – regulations relating to Medical Devices and *In Vitro* Diagnostic Medical Devices (IVDS). A person wishing to manufacture, import, export, distribute or wholesale software as a medical device needs to obtain the requisite licensing and authorisations from the Medicines Control Council.

3 Digital Health Technologies

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

For all of the digital technologies, data protection, including security and prevention of unauthorised disclosure or access, is a fundamental issue that needs to be considered.

- **Telehealth**
  When providing telehealth solutions, companies need to ensure that information is communicated clearly and concisely so that any advice given is not misconstrued. South Africa has 11 official languages, so part of this requirement also includes communicating to end-users where possible in their own language. There also needs to be the necessary disclaimers to limit liability of the telehealth provider in relation to any suggestion given on the app.
- **Robotics**
  The ownership of both the software and hardware of the robot is an issue that needs to be considered. The safety features and limitations of the robot, particularly those used in surgery, need to be determined to avoid the issue of medical negligence claims brought against the relevant medical practitioner.
- **Wearables**
  For wearables, an issue that arises is the lack of transparency and clear communication on what data is being harvested from data subjects and the purpose for which this data is processed. Making even deidentified personal information available, such as the running routes used, could jeopardise the safety of data subjects and make them targets of criminal activity and theft if their ordinary running routes are deserted. Another issue is the possible hacking of wearables and this having severe adverse negative effects. For instance, if a wearable is used to distribute medication into a data subject and this device is hacked, it could be used to cause an overdose of medication in that person.
- **Virtual Assistants (e.g. Alexa)**
  An important aspect of healthcare is the human interaction aspect, so the issue is ensuring that virtual assistants are appropriately programmed to provide appropriate and sympathetic responses and also apply machine learning so that with each interaction, the software gets better.
- **Mobile Apps**
  Important issues for mobile apps include developing an app that is fit for purpose and ensuring that it is appropriately maintained and where necessary, upgraded. The storage and location of the mobile app's software is also an important aspect.
- **Software as a Medical Device**
  An important aspect is that the medical practitioner utilising the device is properly trained to operate the device as they would face medical negligence claims if the software was not used properly and injured a patient. Another issue is determining the licensing/ownership rights in the device.
- **AI-as-a-Service**
  The important issues to consider here are the parameters of the AI licence and also agreeing to liability exposure should the AI device cause personal injury.
- **IoT and Connected Devices**
  Anything that is connected to the internet is vulnerable to hacking so the issues are ensuring that the technology is properly protected against malware, viruses and hacking and that the technology is easily and regularly updated. It is also important to ensure that connected devices are compatible with each other and remain so even when each device is updated. This is especially important in the medical industry where devices could be needed for life-saving measures. For instance, one device may be monitoring the quantity of a particular medication currently in stock and the other device may be triggered and be responsible for ordering more medication when the stock levels reach a certain level.
- **Natural Language Processing**
  An important issue to consider with these technologies is that they are only useful if they receive enough training data and are able to further develop through machine learning to fulfil their function. When these technologies are used as chatbots, they need to be able to offer natural responses, as an important aspect of medical treatment is currently the human interaction and patients feeling heard and listened to.

3.2 What are the key issues for digital platform providers?

Digital platform providers should be aware of at least the general categories of data and software that will be used on these platforms, the level of security needed and how often this needs to be updated to limit its exposure to hackers and other unauthorised disclosure.

4 Data Use

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

When using personal data in the digital health space, two key issues include the consideration and adherence to the regulatory requirements, laid out by the Protection of Personal Information

Act 4 of 2013 ("**POPI**"), and the importance of protecting the confidentiality of the data and securing it from data breaches as health data is generally very sensitive in nature and disclosure of such data can cause very severe reputational damage, as well as having legal ramifications.

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

For the most part, it is subject matter, i.e. the type of personal information used rather than the entities, that should be considered when processing personal data in the digital health sector.

However, POPI does distinguish between responsible parties and operators.

A responsible party is the person that determines how personal information is processed and an operator is the person who processes the personal information on behalf of the responsible party.

If an entity is considered a responsible party, then POPI directly applies to that entity and non-compliance of POPI can result in fees and penalties; where as if an entity is an operator then, provided that such entity does not exceed its contractual mandate with the responsible party, POPI only applies indirectly to it and the operator's exposure is limited to what it has agreed to in its contractual mandate with the responsible party.

4.3 Which key regulatory requirements apply?

POPI is the primary data protection legislation in South Africa. Whilst POPI has been promulgated into law, its substantive provisions are not yet in effect. The President of South Africa needs to determine the full commencement date of POPI but, as an information regulator has been appointed and draft regulations drafted, this is likely to be imminent.

Personal information is essentially any information that can be used to identify a person. A data subject is the person to whom the personal information relates.

In terms of POPI, personal information about a person's health or sex life and ethnic origin is considered special personal information and the processing of special personal information is prohibited unless one of the listed exceptions applies, such as where the data subject consents to the processing.

It is vital therefore in the digital health sector for businesses to focus on obtaining the consent of data subjects when they process special personal information.

Another important issue that digital health businesses ought to consider when processing personal information is that the use of the personal information must be for a specific purpose and the general rule is that personal information should be obtained directly from the data subject.

4.4 Do the regulations define the scope of data use?

The use of personal data must only be for a specific purpose that is adequate, relevant and the processing of such data must not be excessive. Furthermore, the use of the data must be lawful and be used in a reasonable manner that does not infringe the privacy of the data subject.

4.5 What are the key contractual considerations?

When contracting, it is important to identify who is the responsible party and who is an operator under POPI, where and how the data will be stored and whether or not the personal data is being transferred outside of South Africa. A responsible party must ensure that its suppliers who would be operators under POPI are contractually bound to comply with the principles and requirements of POPI.

When contracting with data subjects the purpose for which the personal information is used must be clearly stated and where consent is relied upon for the processing of the personal information, this must be expressed in specific and unequivocal terms by the data subjects.

5 Data Sharing

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

The identity of the person which the personal data shares is of critical importance and whether or not the personal data has been deidentified is a key consideration when sharing personal data.

Generally, if regulatory, court of law or the data subject themselves request personal data then the personal data may be shared. Furthermore, if personal data has been deidentified to an extent that the personal data cannot be reidentified, then that personal data can be freely shared unless protected by a confidentiality clause.

Deidentification and the sharing of the general findings and analytics of big data sets is often critical in the medical health space as it enables entities to commercialise data within its possession and make public importance research results.

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

Under POPI, it is the responsible party who determines the nature and extent of processing personal information, thus it is this party who can determine within the bounds of the law who to share the data with. An operator is mandated to process personal information on behalf of the responsible party, so this entity cannot determine who to share personal information with.

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

Under POPI, a responsible party is required to keep personal information confidential. This means that, generally, data containing personal information cannot be shared with third parties.

Moreover, under POPI, the sharing of personal information would in most instances amount to further processing which is only possible if it is in accordance with or compatible with the purpose for which it was collected. This would typically not be the case when the data is shared, especially where the data is sold to a third party for advertising purposes.

Importantly, in the digital health sector, a significant portion of the data is personal information about a patient's health or sex life. As mentioned in our response to question 4.3, the general rule is that the processing of this type of data (which includes the sharing of data) is prohibited unless an exception applies, such as the data subject consenting to the data sharing.

Another instance where health or sexual life personal information could be shared is within a healthcare facility or between medical practitioners where this processing (sharing) is necessary for the proper treatment and care of the data subject. By

way of example, paramedics could share with a surgeon, about to perform emergency robotic surgery, details about the patient's current medical conditions.

It is worth noting that anonymised data where the personal information has been completely deidentified, can generally be shared with others, unless it is protected by a confidentiality agreement or similar undertaking.

6 Intellectual Property

6.1 What is the scope of patent protection?

In South Africa a patent is an exclusive right granted for an invention, which is a product or a process that provides a new way of doing something or offers a new technical solution to a problem. Patents can last up to 20 years under South African Law.

South African Law provides protection for patents registered with the Companies and Intellectual Property Commission ("**CIPC**") and South Africa is also a party state to the Patent Cooperation Treaty ("**PCT**") which is an agreement for international co-operation in the field of patents.

6.2 What is the scope of copyright protection?

Copyright in South Africa is regulated by the Copyright Act 98 of 1978 ("**Copyright Act**") and automatically subsists in original works, eligible for protection, created by a qualified person or which are first published in South Africa or another country to which protection is extended. The Copyright Act contains a clear description of the various works that are capable of copyright protection. These various works include literary works, cinematographic films, musical and artistic works and computer programs. Certain exclusive rights are vested in the owner of the copyrightable work, including the right to reproduce, publish or make an adaptation of the work in question. Persons can co-own a copyrighted work.

6.3 What is the scope of trade secret protection?

Trade secrets are not protected in terms of legislation but under the common law as long as they are kept secret and confidential and not disclosed to the public. It is possible to interdict a person from disclosing such secrets.

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

In South Africa there is the Intellectual Property Rights from Publicly Financed Research and Development Act 51 of 2008 ("**IPR Act**"). Under the IPR Act, if intellectual property is created with public funds then the public university or research institution involved in the development or commission of the intellectual property shall own the intellectual property no matter what is agreed between the parties.

The IPR Act also enables these institutions to receive subsidies and funding from public funds. The IPR Act also restricts what public institutions can do with its intellectual property. For instance, the intellectual property cannot be assigned without following the guidelines given by the National Intellectual Property Management Office ("**NIPMO**") and also notifying the NIPMO.

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

Software as a Medical Device would be granted protection as a computer program under the Copyright Act 98 of 1978 ("**Copyright Act**"). An owner of the Software as a Medical Device has the exclusive right to use, copy, license and dispose of the device.

7 Commercial Agreements

7.1 What considerations apply to collaborative improvements?

It is important to establish and agree beforehand what the ownership structure in the improvements shall be and also what each party's exposure and liability is under the collaboration.

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

It is crucial to consider what type of data is being processed under the agreement and whether personal information is processed, and if personal information is processed, then adequate data protection clauses must be included. It is also critical to determine each party's exposure and liability, particularly to third parties like data subjects if the data is unlawfully accessed.

Both entities must also ensure that the other party has the requisite expertise and authorisations to fulfil their obligations. For instance, if a hospital partners with a software developer to jointly create and own an app that provides post-hospital advice to outgoing patients then it is important that the hospital ensures that the software developer has the capabilities to develop the app and provide the necessary security safeguards. The software developer would want to ensure that the hospital is appropriately registered, the advice that is provided on the app has been properly vetted by registered and qualified medical professionals and any personal information shared is only shared where the patient has consent to the data being processed and used on the app.

8 AI and Machine Learning

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

Machine learning is playing an increasingly important role in digital health as it is a useful tool to constantly improve digital health solutions. For instance, in robotic surgery, machine learning can be used to ensure that the robots used learn from each surgery performed, thereby making them more effective and safer with every surgery.

One of South Africa's medical insurance providers uses AI chatbots to engage with customers on its website and help customers find the information that they need on the website. Customers can provide feedback on whether or not the information provided was useful/relevant. By utilising machine learning, these chatbots can learn which responses are appropriate for which queries based upon the customers' response, thereby improving customer satisfaction and becoming more useful to the insurer.

8.2 How is training data licensed?

Techopedia.com defines that, "the training data is an initial set of data used to help a program understand how to apply technologies like neural networks to learn and produce sophisticated results".

In South Africa, there are a few ways in which training data is acquired. If possible, data in the public domain or already in developer's possession is used to develop the program, or a developer may offer to develop software for a client or clients and then use the clients' data as training data to build and improve the computer program.

It is also possible to "license" the training data by asking for individuals to provide it voluntarily or for some kind of compensation, although this approach is in our view less frequently used.

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

Algorithms are categorised as a "computer program" under the Copyright Act.

The general rule is that ownership of original work shall vest in the author, or in the case of joint authorship, in the co-authors of the work. It is therefore critical to identify who the author is. In respect of a computer program, the author is the person who exercised control over the making of the computer program. Where the work is created in the course and scope of employment (whether under a contract of service or apprenticeship), the employer will hold the copyright. Where a computer program has been commissioned, the person commissioning the work would be the author.

Where this algorithm is thereafter further improved by machine learning without active human involvement, then the owner of the algorithm would remain the person who initially exercised control over the making of the algorithm as only natural and juristic persons such as companies can acquire ownership rights and not machines.

Furthermore, even if the algorithm is improved and altered to a large extent without further human involvement that it is no longer considered the original but an adaption of the algorithm, the adaptions are also under copyright law and are considered to be owned by the author.

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

The most important considerations are how the licensor will be paid or otherwise compensated and agreeing who will own the analysis of the data. The source of the data is also important as, if the data contains personal information, then it is also important that the data subjects whose personal information is being processed have consented to its use in machine learning or there is another legal justification for processing this data.

9 Liability

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

Under South African law, parties are typically liable for the legal consequences that arise out of their negligence or fault.

In limited circumstances, parties may also be held strictly liable. A common example of this is vicarious liability where an employer shall be held liable for its employees' delicts (torts) that are performed within the course and scope of their employment. A common instance where strict liability will apply is in contracts involving consumers. Where a client is a natural person or small juristic person, they may also be able to hold both the service provider and developer of digital health technology liable under the Consumer Protection Act where such technology is unsafe, defective or of poor quality. This is because the producer, importer, distributor and retailer are all deemed to include an implied warranty of quality under the Consumer Protection Act. The Consumer Protection Act also contains a similar right to quality services for a consumer.

9.2 What cross-border considerations are there?

Under South African law, an entity may not export capital including intellectual property outside of South Africa without first obtaining approval from the Financial Surveillance Department of the South African Reserve Bank ("**SARB**") or an authorised dealer, where SARB has delegated its power to authorise the export of capital to that authorised dealer.

This means that if an entity has invented a digital health app/software or other asset in South Africa and wishes to expand into other countries, sell or licence the software to a foreign entity, it can only do so if it obtains the authority of SARB under the Exchange Control Regulations.

10 General

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

Medical data of data subjects is considered special personal information under POPIA, thus the processing of medical data, including storage on the cloud, is only allowed in limited circumstances such as where the data subjects have consented to such data processing.

Furthermore, often cloud-based providers' servers are located outside of South Africa, thus it is critical for the cross-border transfer to be lawful under POPIA.

A cloud provider is considered a service provider of a digital health entity thus, it is important for there to be proper agreements in place that protect the digital health entity's data and guarantees the security and confidentiality of medical data of any data subjects.

Furthermore, because of the sensitive nature of patient-linked digital health data, to avoid data breaches and irreparable reputational damage, it is critical for entities in this sector to partner with reputable cloud service providers when providing cloud-based health services.

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

Non-healthcare companies need to properly analyse compliance and regulation issues as this is a regulated sector and so, in many instances, licences and other authorisations are required to conduct their business. These companies also need to acknowledge that there are already a few big players from hospital groups to medical insurers in the medical industry that are driving

innovation in order to maintain their market share and remain relevant. This means that before entering the market, it is critical for new entrants to properly identify gaps in the market and develop a customer-centric brand identity.

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

It is critical for venture capital and private equity firms to conduct comprehensive due diligence to determine whether the digital health ventures' intellectual property rights are properly protected and that the ventures actually own the digital healthcare technology that they are utilising and developing. Depending on the nature of the venture, it is also important to ensure that the entity is properly licensed and has the necessary authorisations to conduct its business.

Christoff Pienaar is a Director and the National Head of Technology, Media & Telecommunications at Cliffe Dekker Hofmeyr. He advises on commercial, information technology and intellectual property law. He specialises in information technology and commercial matters and has particular expertise in payment systems, technology outsourcing, business process outsourcing, systems integration, hardware acquisitions and maintenance, IT consultancy services, managed services, disaster recovery services, software development and software licensing and support transactions. Christoff also advises on general commercial and intellectual property issues across a diverse range of industry sectors, especially financial services.

Cliffe Dekker Hofmeyr
11 Buitengracht Street
Cape Town
South Africa

Tel: +27 21 481 6300
Email: christoff.pienaar@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Nikita Kekana is an Associate in Cliffe Dekker Hofmeyr's Technology, Media & Telecommunications practice. Nikita specialises in commercial, information technology, intellectual property and data protection law. Nikita also has a keen interest in artificial intelligence, machine learning and big data.

Cliffe Dekker Hofmeyr
11 Buitengracht Street
Cape Town
South Africa

Tel: +27 21 481 6300
Email: nikita.kekana@cdhlegal.com
URL: www.cliffedekkerhofmeyr.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