23 JUNE 2021

HEALTHCARE & PHARMACEUTICALS **ALERT**

IN THIS ISSUE >

The digitisation of healthcare: Privacy and data protection considerations

In recent years and accelerated by the COVID-19 pandemic, the number of digital health businesses or virtual health offerings has significantly increased globally and in South Africa. The digitalisation of healthcare poses interesting legal questions. Digital health businesses should consider, amongst other things, the privacy and data protection legal paradigm applicable to their businesses, including the Protection of Personal Information Act 4 of 2013 (POPIA).

CDH
CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA

The digitisation of healthcare: Privacy and data protection considerations

By its very nature, digital health businesses will process health data which is regarded as *"special personal information"* in terms of POPIA. The processing of special personal information is highly regulated in POPIA.

In recent years and accelerated by the COVID-19 pandemic, the number of digital health businesses or virtual health offerings has significantly increased globally and in South Africa. The digitalisation of healthcare poses interesting legal questions. Digital health businesses should consider, amongst other things, the privacy and data protection legal paradigm applicable to their businesses, including the Protection of Personal Information Act 4 of 2013 (POPIA).

What is "digital health"?

Although there is no legislative definition of *"digital health"*, the Department of Health (DoH) has adopted the World Health Organisation's definition as set out in the DoH's National Digital Health Strategy document: *"The field of knowledge and practice associated with any aspect of adopting digital technologies to improve health, from inception to operation"*. *"Digital health"* is therefore understood to be an umbrella term which incorporates, amongst other things, e-health, telemedicine, and telehealth (to name a few).

Processing special personal information

By its very nature, digital health businesses will process health data which is regarded as *"special personal information"* in terms of POPIA. The processing of special personal information is highly regulated in POPIA.

The point of departure is that a responsible party may not process the special personal information of a data subject i.e., there is a general prohibition against such processing, unless it falls within the scope of authorisation provided under sections 26 – 33 of POPIA. Although there are other potentially relevant legal bases to process special personal information health information may be processed by a responsible party with the consent of a data subject. Consent, under POPIA, means *"any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information"*. The five key elements to be addressed in obtaining consent are that consent must be:

- **freely given** – the data subject must not be pressured into giving consent or suffer any detriment if they refuse;
- **specific** – the data subject must be asked to consent to individual types of data processing with full information as to what their personal information will be used for;
- **informed** – the data subject must be told what they are consenting to;
- **unambiguous** – the language must be clear and simple; and
- **clear affirmative action** – the data subject must expressly consent by doing or saying something.

The digitisation of healthcare: Privacy and data protection considerations...*continued*

Due to the sensitive nature of health information, digital health businesses must ensure that such information is secure.

This consent must be obtained when the responsible party (digital health business) processes the data subject's personal information or as soon as possible thereafter. For example, where one downloads an app such consent should be obtained upfront and prior to the collection of any special personal information.

Data security

Due to the sensitive nature of health information, digital health businesses must ensure that such information is secure.

POPIA requires that a responsible party secures the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent (a) loss of, damage to or unauthorised destruction of personal information; and (b) unlawful access to or processing of personal information. In order to give effect to this, the responsible party must take reasonable measures to (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; (b) establish and maintain appropriate safeguards against the risks identified; (c) regularly verify that the safeguards are effectively implemented; and (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

A digital health business must also have regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of the healthcare industry or professional rules and regulations.

Data Sharing and Transferring

POPIA requires that data subjects must be made aware and should agree to their special personal information being shared with third parties. If health information is shared with a third party or hosted outside of South Africa, consideration must be given to section 72 of POPIA, which amongst other things, requires that the data subject consents to sharing their information and that the responsible parties take appropriate measures to ensure that the third party has measures in place to secure the integrity of the data. Digital health businesses must also apply for prior authorisation from the Information Regulator should the transfer of special personal information (health information) be to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72.

Conclusion

Data subjects must be confident that their rights to privacy and confidentiality are respected and upheld, and that the information they share with digital health business is kept safe and secure. This is why it is crucial that providers of digital health consider privacy and data protection concerns before deploying a digital heath platform to customers. Non-compliance with the data protection obligation imposed by POPIA could attract severe liabilities including financial penalties.

Christoff Pienaar, Lee Shacksnovis and Thando Hadebe

OUR TEAM

For more information about our Healthcare & Pharmaceuticals sector and services in South Africa and Kenya, please contact:

Susan Meyer
Sector Head
Healthcare & Pharmaceuticals
Director
Competition
T +27 (0)21 481 6469
E susan.meyer@cdhlegal.com

Etta Chang
Director
Corporate & Commercial
T +27 (0)11 562 1432
E etta.chang@cdhlegal.com

Mashudu Mphafudi
Director
Finance & Banking
T +27 (0)11 562 1093
E mashudu.mphafudi@cdhlegal.com

Sammy Ndolo
Managing Partner | Kenya
T +254 731 086 649
+254 204 409 918
+254 710 560 114
E sammy.ndolo@cdhlegal.com

Tim Fletcher
National Practice Head
Director
Dispute Resolution
T +27 (0)11 562 1061
E tim.fletcher@cdhlegal.com

Christoff Pienaar
National Practice Head
Director
Technology Media & Telecommunications
T +27 (0)21 481 6350
E christoff.pienaar@cdhlegal.com

Emil Brincker
National Practice Head
Director
T +27 (0)11 562 1063
E emil.brincker@cdhlegal.com

Lara Granville
Director
Competition
T +27 (0)11 562 1720
E lara.granville@cdhlegal.com

Lucinde Rhoodie
Director
Dispute Resolution
T +27 (0)21 405 6080
E lucinde.rhoodie@cdhlegal.com

André de Lange
Director
Corporate & Commercial
T +27 (0)21 405 6165
E andre.delange@cdhlegal.com

Quintin Honey
Director
Corporate & Commercial
T +27 (0)11 562 1166
E quintin.honey@cdhlegal.com

Roxanna Valayathum
Director
Corporate & Commercial
T +27 (0)11 562 1122
E roxanna.valayathum@cdhlegal.com

Imraan Mahomed
Director
Employment Law
T +27 (0)11 562 1459
E imraan.mahomed@cdhlegal.com

Njeri Wagacha
Partner | Kenya
T +254 731 086 649
T +254 204 409 918
T +254 710 560 114
E njeri.wagacha@cdhlegal.com

BBBEE STATUS: LEVEL TWO CONTRIBUTOR
Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

JOHANNESBURG
1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa. Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

CAPE TOWN
11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com

NAIROBI
CVS Plaza, Lenana Road, Nairobi, Kenya. PO Box 22602-00505, Nairobi, Kenya.
T +254 731 086 649 | +254 204 409 918 | +254 710 560 114 E cdhkenya@cdhlegal.com

STELLENBOSCH
14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com

CLIFFE DEKKER HOFMEYR

INCORPORATING
KIETI LAW LLP, KENYA