ORARO & COMPANY
ADVOCATES
An Affiliate Member of AB & DAVID AFRICA

ODPC ISSUES GUIDANCE NOTE ON THE PROCESSING OF HEALTH DATA

JANUARY 2024

ODPC Issues Guidance Note on the Processing of Health Data

The health sector is one of the largest consumers of personal data due to the large volumes of data obtained and processed during a typical medical cycle, including registration, diagnosis, storage, analysis and transfer of data. The use of technology in processing of heath data has increased, with new and innovative methods of rendering health services through online means such as e-health and m-health heralding a new dawn in the health sector. Whereas the use of technology in healthcare no doubt carries with it significant benefits for the sector such as faster processes and increased efficiencies, it also raises serious privacy concerns such as the potential misuse of personal and health data, breach of patients' privacy, lack of transparency around data processing, amongst others. The use of technology further poses risks relating to cybersecurity, with more and more health institutions and service providers becoming prone to cyberattacks. As such, the importance of data protection and privacy compliance with respect to the healthcare sector cannot be emphasised and the Guidance Note issued by the Office of the Data Protection Commissioner (ODPC Guidance Note) on the processing of Health Data could not have come at a timelier period.

Who does the ODPC Guidance Note apply to?

The ODPC Guidance Note applies to all persons providing healthcare services, ranging from hospitals, clinics and other healthcare institutions to individuals using technology in the provision of healthcare services. Other stakeholders include public health agencies, health insurance companies, pharmaceutical companies, medical research institutions, government agencies, and non-governmental organizations. The ODPC Guidance Note is intended to provide healthcare institutions with a clear understanding of their duties and obligations under the Data Protection Act, 2019 (the DPA or the Act).

How do the principles of data protection apply to the health sector?

The principles of data protection provided under the DPA are applicable to all forms of processing of personal data, including processing of health data, as set out below:

a) Lawfulness, fairness and transparency – Processing health-related data is only legitimate if such processing is undertaken for lawful, fair and transparent reasons such as medical diagnosis and treatment, for purposes of legal obligations, or purposes of a contract with a healthcare professional.

b) Purpose limitation – This principle requires that all health-related data should only be collected or processed for the reasons provided for and not be used for any other purpose inconsistent with those identified, for instance, to provide medical treatment, research, health insurance, public health purposes or health awareness and wellbeing programs.

c) Data minimization – This principle requires that a healthcare provider should only collect or process what is necessary for a specific purpose, or to the extent necessary to achieve the medical care objectives. For instance, in the provision of medical treatment, they must only collect personal data that is necessary for the diagnosis, treatment, and monitoring of a patient's health, and no more. As such, it would, for example, be improper for one to enquire into the patient's financial information, which has no bearing on the patient's health.

d) Accuracy – This principle requires that all personal data should be accurate, up-to-date, and complete. This means that all health sector stakeholders should take reasonable steps to ensure that the personal data or health-related data collected is accurate and provide for a manner to correct any inaccuracies, including taking immediate steps to remove or delete any inaccuracies once discovered.

e) Storage limitation – This principle requires that all personal data, including health-related data, should not be stored for longer than is necessary to accomplish the purposes for which it was collected. In line with this principle, the relevant stakeholders

ODPC Issues Guidance Note on the Processing of Health Data

in the health sector should have appropriate mechanisms in place to ensure that personal and health-related data are not stored indefinitely and only stored for as long as they are required to achieve the intended purposes.

f) Integrity and confidentiality – Under this principle, stakeholders in the health sector are required to maintain the confidentiality of health data collected and ensure that health data is stored and transmitted securely. This includes implementing appropriate technical and organizational measures to protect against unauthorized access, disclosure, alteration, or destruction of personal data.

g) Accountability – This principle refers to the responsibility of stakeholders in the health sector to ensure compliance with relevant laws and regulations related to the processing of health data. Such compliance measures such as policies and procedures should be reviewed and updated regularly.

What are the lawful bases of processing personal data in the health sector?

A healthcare provider or stakeholder is required to have a lawful basis for processing personal data and health data. Such lawful basis must be carefully determined before undertaking the processing activity and must ensure all requirements for such processing are met e.g. ensuring the security of the data is safeguarded throughout the processing. Some lawful bases for processing personal and health data include:

a) Consent – One of the main bases for undertaking any processing activity is obtaining clear and informed consent for the specific processing activity to be undertaken. The consent must be freely given, informed, specific, and unambiguous. It is also important distinguish consent for data processing purposes with 'medical consent' which is a specialised form of consent required where patients agree to undergo medical treatment, surgery, or participate in clinical research. Medical consent related to the body autonomy of the patient as to whether they agree to undergo a specific medical procedure or treatment and does not necessarily grant the right to share or store medical data for other purposes.

b) Performance of a contract – Healthcare providers and stakeholders may process personal data to fulfil a contractual obligation or for purposes of pre-contractual relationships. For instance, where some medical check-ups may be required before entering into a contract with an individual.

c) Compliance with a legal obligation – Stakeholders in the health sector may rely on legal obligation as a lawful basis to process personal data and ensure the protection of the data in accordance with the data protection laws. For instance, regulatory bodies in the health sector may require processing some of the personal data held by a healthcare provider in carrying out their duties.

d) Protection of the vital interests of a data subject – An example of a vital interest with respect to healthcare could be a medical emergency of a data subject, which would provide a basis to process the data.

e) Legitimate interests pursued by the healthcare Providers – In this instance, healthcare providers and stakeholders must ensure that the processing activities are necessary for the legitimate interest pursued, such as managing and administering healthcare services. However, the legitimate interests of the healthcare provider should not outweigh or override the individual rights and freedoms of data subjects.

f) Public interest – In line with this, stakeholders in the health sector may process personal data to safeguard the public interest while ensuring that such processing is done in a way that respects individuals' rights and freedoms and that appropriate measures are in place to protect the security and confidentiality of personal data. An example of this is processing personal data for the purposes of tracking the spread of infectious diseases, to help identify outbreaks and contain their spread.

ODPC Issues Guidance Note on the Processing of Health Data

g) Historical, statistical, journalistic, literature and art or scientific research – This may be conducted by stakeholders in the health sector for various purposes such as:

   a. Scientific research – the processing of personal data for scientific research is necessary for public interest in advancing knowledge and understanding of health and diseases.

   b. Historical research – this is necessary for preserving and studying historical events and their impact on the society.

   c. Statistical research – health care providers can carry out statistical research using health data for purposes of monitoring trends in disease incidences and the prevalence to predict and control any outbreaks.

What are the compliance obligations for participants in the health sector?

Some of the compliance obligations that would be required of persons in the healthcare sector include:

a) Registration with the ODPC – All entities in the healthcare sector are required to undertake mandatory registration with the ODPC as a data controller or processor.

b) Privacy by design or default – This requires the incorporation of data privacy and security measures into the products, services and systems to ensure compliance (privacy by design), as well as requiring that one's systems and procedures are established in line with data protection principles from the outset (by default). This is particularly important in the health sector where health data which is categorized as sensitive personal data, is processed.

c) Data storage – This is in line with the storage limitation principle whereby, once the purpose for which the data was collected has been fulfilled, it should either be erased, anonymized, or pseudonymized to make sure it's not kept for longer than it needs to be. This prevents misuse of personal data and safeguards the privacy rights of individuals, as personal data that is no longer needed is less likely to be accessed or revealed without consent.

d) Data Protection Impact Assessment (DPIA) – A DPIA is a useful tool to help data controllers and/or data processors comply with data privacy laws and is mandatory where processing is "likely to result in a high risk to the rights and freedoms of data subjects". Where it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out.

e) Notification and communication of breach – Upon unauthorised access of data, stakeholders within the health sector are required to report such breach with the ODPC without delay within seventy-two (72) hours of becoming aware of the breach. In addition, they are also required to communicate to the affected data subjects in writing within a reasonable period.

f) Engagement of data processors – Due to the various services in the health sector provided by third parties, it is important for health facilities to engage data processors that have experience in handling health data and are compliant with all relevant laws and regulations related to data protection and confidentiality. This will help to ensure that health data is handled securely and ethically, and that patient privacy is protected.

g) Data sharing – healthcare providers and stakeholders may be required to share health data with relevant stakeholders, such as government agencies, researchers and other healthcare institutions, so to improve health outcomes for the population. Such data sharing must be done in accordance with the principles of confidentiality, privacy, and informed consent.

h) Data transfer – Any transfer of personal data to a third party must ensure that the appropriate safeguards are in place, the transfer is a necessity, or has the consent of the data subject. Particularly with respect to health data, such personal data is required to be stored and

ODPC Issues Guidance Note on the Processing of Health Data

processed in Kenya, except in limited circumstances such as where the data subject has given explicit consent to the transfer or where there is an adequate level of protection in the receiving country.

i) Duty to notify – In line with the principle of transparency, a data controller or processor in the health sector is obligated to notify data subjects of their rights, provide them with information about the purpose of data collection, disclose any third parties who may receive the data and the safeguards adopted, describe the technical and organizational security measures, and outline the consequences if data subjects fail to provide all or part of the requested data. Such information may be contained in a data protection policy, which should be made available to data subjects.

Disclaimer

This alert is for informational purposes only and should not be taken to be or construed as a legal opinion. If you have any queries or need clarifications, please do not hesitate to contact John Mbaluto, FCIArb, Deputy Managing Partner, (john@oraro.co.ke) and Morris Muriu Mbugua, Senior Associate, (morris@oraro.co.ke) or your usual contact at our firm, for legal advice.

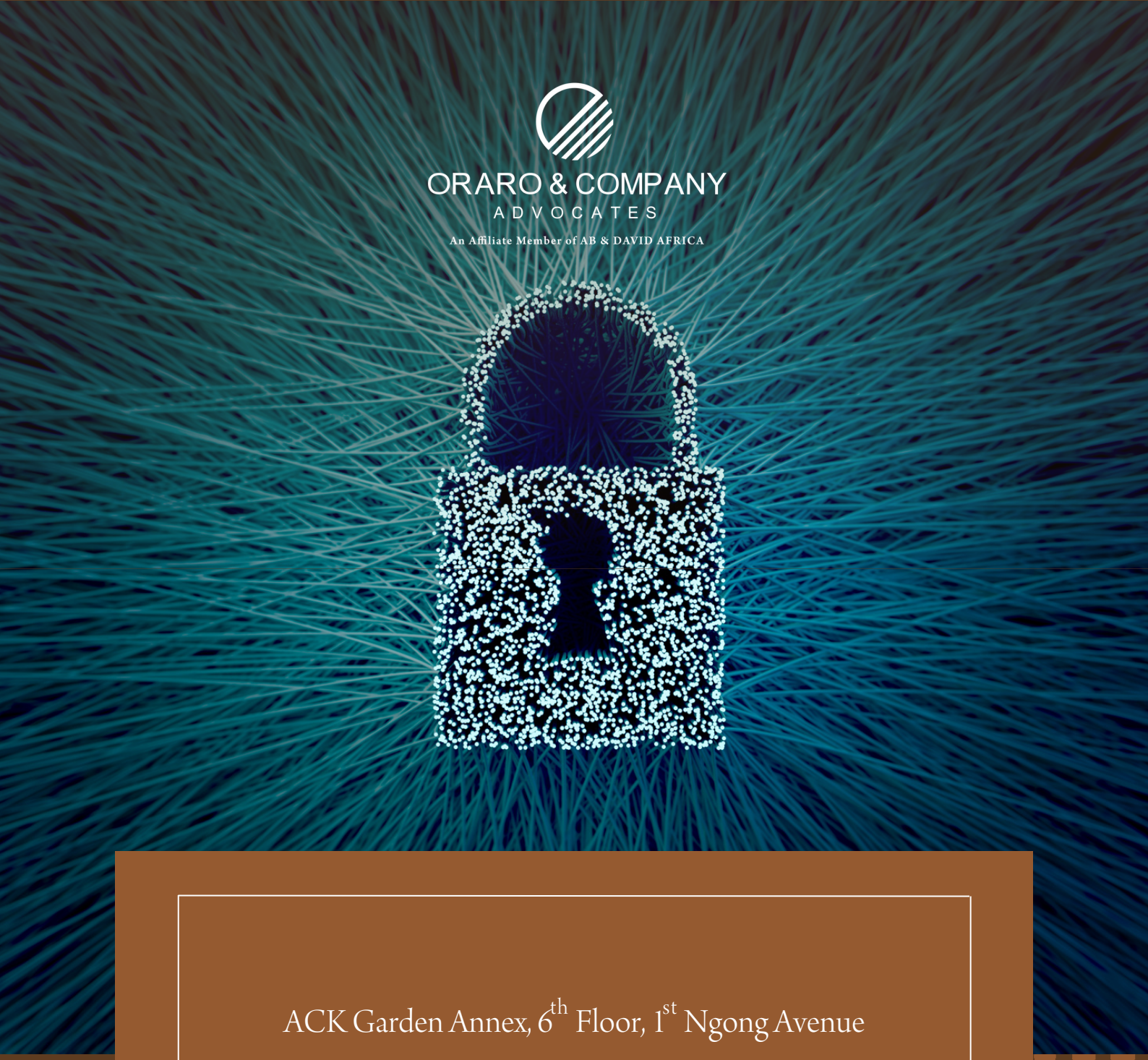
John Mbaluto, FCIArb

Deputy Managing Partner

Morris Muriu Mbugua

Senior Associate

ORARO & COMPANY
ADVOCATES
An Affiliate Member of AB & DAVID AFRICA



ACK Garden Annex, 6th Floor, 1st Ngong Avenue
P. O. Box 51236-00200, Nairobi, Kenya.
T: +254 709 250 000
E: legal@oraro.co.ke

Oraro & Company Advocates