OFFICE OF THE DATA PROTECTION COMMISSIONER

GUIDANCE NOTE ON THE PROCESSING OF HEALTH DATA

DECEMBER 2023

TABLE OF CONTENTS

DEFINITION

"Act" or "DPA" means the Data Protection Act, No 24. of 2019.

"Confidentiality" is the degree to which access and disclosure of given information is limited to authorized entities (e.g., users) and for intended purposes only thereby preventing access by or disclosure to unauthorized entities (users).

"Data Commissioner" means the person appointed pursuant to section 6 of the Act.

"Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of Processing of Personal Data.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

"Data Subject" means an identified or identifiable natural person who is the subject of Personal Data.

"Entity" or **"Entities"** means a natural (individual) or legal person, public authority, agency or other body that processes (handles) Personal Data.

"Health data" means data related to the state of physical or mental health of the data subject and includes records regarding the past, the present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services.

"Sensitive personal data" is data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

"Client" or "Patient" is a recipient of professional healthcare services.

"Healthcare service provider" is an individual or an institution that provides preventive, curative, promotional, or rehabilitative healthcare services in a systematic way.

"mHealth" Health services, interventions, and/or programs accessed, delivered or availed through the use of mobile phone and other wireless technologies and devices.

"eHealth" is the secure use of information and communications technologies in support of health and health-related fields, including healthcare services, health surveillance, health literature, and health education, knowledge, and research.

"e-Prescription" This is electronic writing and sending of prescriptions instead of using handwritten or faxed notes or calling in prescriptions.

"Longitudinal Health Record" is a single complete patient record that combines data from a variety of sources throughout the healthcare system.

"Office" means the Office of the Data Protection Commissioner as established in section 5 of the Act.

"Privacy" is the right of individuals to be free from unauthorized intrusion, surveillance, and publicity. it is the ability to control access to personal information and activities.

"Confidentiality" is the degree to which access and disclosure of given information is limited to authorized entities (e.g., users) and for intended purposes only thereby preventing access by or disclosure to unauthorized entities (users).

"Machine-readable" is data in a format that can be processed by a computer.

THE OFFICE

The Office of the Data Protection Commissioner (Office) is a government agency established to protect the privacy and security of personal data in our increasingly digital world. It has the responsibility of enforcing data protection laws and policies to safeguard the privacy, dignity, and fundamental rights of individuals. The Office is mandated to oversee the implementation and enforcement of the Data Protection Act, 2019, which regulates the processing of personal data of persons located in Kenya by both private and public sector organisations.

The Office plays a vital role in ensuring that individuals have control over their personal data and that organisations respect their privacy rights. The office's work involves monitoring and enforcing compliance with data protection regulations, investigating data breaches, and imposing sanctions on entities that violate data protection laws. In addition, the Office is responsible for raising public awareness about data protection issues and educating individuals and organisations on how to protect personal data. With the growing importance of data protection in our digital age, the Office of the data protection commissioner is a critical institution in maintaining trust and confidence in our data-driven society.

The Office of the Data Commissioner is uniquely positioned to facilitate both the government and private sector entities in achieving Government's strategic goals under the "Bottom Up Economic Transformation Agenda" and, in particular, its digital superhighway initiative. As the digital landscape expands, the need for robust data protection mechanisms becomes paramount. The Office, with its mandate to oversee, regulate, and ensure lawful data processing, plays a pivotal role in this transformation. Kenya remains at the cutting edge of digital transformation while maintaining stringent data protection standards. The Office of the Data Commissioner serves as a key stakeholder and regulator in guiding the nation's digital superhighway journey by ensuring that as we advance technologically, the rights and privacy of individuals remain safeguarded.

2. INTRODUCTION

2.1. BACKGROUND

The health sector is one of the largest users of personal data in Kenya, as it collects, stores, and analyzes vast amounts of personal data during registration, diagnosis, storage, analysis, and transfer. The use of technology such as e-health and m-health are revolutionizing the way healthcare data is transferred, stored, and accessed. These technologies are improving care coordination, enhancing patient outcomes, and enabling healthcare providers to provide more personalized and effective care. Some of the key stakeholders in the health sector include the data subjects (patients/clients), hospitals & clinics, laboratories, donors & partners, health workers, community health volunteers, pharmaceutical services, health insurance providers, health research and training institutions, and professional health bodies.

The adoption of technologies such as Health Management Information System (HMIS), eHealth, mHealth, medical imaging devices (X-rays, CT scans, MRI scans & ultra-sounds), wearable devices (such as fitness trackers, blood pressure monitors & heart rate monitors), e-Prescription and robotic surgery in the health sector has grown significantly in recent years, from basic to advanced levels. Other technologies; include Community Health Information System (CHIS), District Health Information System (DHIS2), Laboratory Information System (LIS), Logistics Management Information System (LMIS), Pharmaceutical Information System (PIS), Electronic Medical Records (EMR) and Electronic Health Records (EHR). However, this transition to digital applications has come with its own set of privacy concerns. They are increasingly becoming a target for cyberattacks, accidental leakage, and misuse putting the privacy of collected and stored health data at risk. As records continue to take the place of face-to-face encounters in the society, there needs to be some recompense to give the individual the kind of control over the collection, use, and disclosure of information about them that their face-to-face encounters normally entail.

Therefore, besides the legal and ethical concerns, the framework of Data protection in the health sector in Kenya has become increasingly important. The right to privacy is enshrined in the Kenyan Constitution, as expounded under the Data Protection Act, 2019, which provides the required legal framework to all individuals and organizations that process personal data, including healthcare institutions.

Healthcare providers in Kenya are required to comply with the Data Protection Act when processing personal data. This includes ensuring that data is processed on reliance on a proper lawful basis from individuals before collecting their data, ensuring that data is accurate and upto-date, and protecting data from unauthorized access, use, and disclosure. This guidance note aims to provide healthcare institutions and the respective stakeholders with a comprehensive overview of their obligations when processing personal data and practical steps to ensure compliance with the law.

2.2. PRIVACY CONCERNS

The nature of processing data in the health sector raises significant privacy concerns, including the potential misuse of personal and health data, patients' privacy and dignity, lack of transparency around data processing, and the risk of bias and discrimination in the processing of health data. A need has thus arisen for the health sector to take steps to ensure that personal data related to the provision of personal health are processed in a fair and

transparent manner, with appropriate data protection measures in place to safeguard personal data against unauthorized access, disclosure, or loss.

The adoption of technologies is increasingly becoming a target for cyberattacks, putting the privacy of collected and stored health data at risk. Another critical privacy concern is how vendors use the personal data to which they have access. Untrustworthy vendors can collect and reuse personal data in ways that healthcare institutions and stakeholders (donors, data subjects, and their legal guardians) may be unaware of, such as using data for advertising purposes or packaging and selling data to third parties. The use of health data for profiling and predictive analysis can have serious long-term effects and raises significant privacy concerns.

Cloud-based solutions present their own set of risks, such as non-efficient encryption algorithms or inherent security risks when all assets are hosted online. The most significant issue with cloud- based solutions is the minimal control over data and cloud system setup. The terms and conditions are determined by cloud service providers, and healthcare institutions as data controllers have very little power. Surveillance technology adopted by most healthcare institutions as a safety instrument, and the pervasive use of surveillance technology (including CCTV and AI-driven tools to track patients' behavior online) can result in serious harm.

While the above list of challenges is illustrative, it is not exhaustive, and the health sector must remain vigilant and proactive in addressing privacy concerns.

According to various research conducted in regard to data protection in the health sector, it is noted the health sector has enacted laws and policies that require and recognize data protection when health data is processed. While these identified laws and policies address distinct issues and acknowledge certain data protection principles, they are, in specific instances, inconsistent with the Data Protection Act. As a result, it is necessary to amend these laws and policies to ensure full compliance with the DPA and address the privacy concern mentioned above.

According to several research studies[1], the privacy policies of various healthcare providers have been reviewed, however, the majority of institutions have not posted any privacy notices on their websites or made them available to the public. Those who have attempted to create the policies and notifications are too general or don't give the data subject enough information about the specific aims of data processing and their rights.

2.3. SCOPE AND PURPOSE

The scope of this guidance note is to provide healthcare institutions with a clear understanding of their obligations under data protection law. The guidance note aims to cover various aspects of data protection, including the collection, use, retention, disclosure, and disposal of personal data in the health sector. The note will apply to all healthcare institutions operating in Kenya, including hospitals & clinics, laboratories, pharmaceutical services, health insurance providers, health research and training institutions, and professional health bodies.

Further, the scope of the guidance note extends to the processing of digital health processing platforms such as Health Management Information System (HMIS), eHealth, and mHealth applications that comply with the same rigorous data protection standards as manual records in traditional in-person health service provision. It will also cover electronic health records such as eHealth and mHealth systems that healthcare institutions engage in and use. It will

emphasize the importance of due diligence in selecting and using electronic health systems and records that meet data protection standards.

The note may include separate sections tailored to different healthcare institutions and players in the industry, such as hospitals & clinics, laboratories, pharmaceutical services, health insurance providers, and health research and training institutions, respectively. It will also consider the specific data protection challenges and issues relevant to each type of institution. It will provide clear and practical guidance on various data protection principles, including the legitimacy and lawful basis for processing personal data, fair processing, data retention, security, automated decision-making, profiling, and the use of biometric data.

Lastly, it will include checklists to help healthcare institutions understand the requirements and check their compliance with relevant legal requirements, including guidance on the creation of privacy notices, which must stipulate the rights of data subjects and how they can be exercised. Each healthcare institution will be required to create an individual privacy notice covering the processing activities specific to their institutions. While certain sections of this guidance note may be applicable, regular compliance audits conducted may be necessary to provide tailored guidance and recommendations.

3. LEGISLATIVE FRAMEWORK

The legal framework for data protection in the health sector is aimed at protecting personal data and ensuring that it is processed, stored, and shared in a manner that is lawful, fair, and transparent.

The health sector in Kenya is regulated by laws and policies that require and recognize data protection principles when health data is processed. The existing laws and policies regulating health information/data all came into force prior to the enactment of the DPA.

In addition, this legislative framework demonstrates how health data is perceived in the adoption of new technology in the health sector and gives insight as to the extent to which data protection has been considered in the implementation and use of new technologies that process health data. The laws include:

The Constitution of Kenya 2010 – The constitution recognizes the right to privacy including, the right not to have a citizen's personal information in relation to their family or private affairs, unnecessarily required or revealed.

Data Protection Act, 2019 - The Act defines "Health data" as data related to the state of physical or mental health of the data subject and includes records regarding the past, present, or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services.

Further, under the Act, health data is considered sensitive personal data, and additional safeguards should be put in place to protect this information.

Section 26: Individuals have the right to access their health data and request corrections to any inaccurate information. They also have the right to request that their health data be deleted in certain circumstances.

4. APPLICATION OF DATA PROTECTION PRINCIPLES

4.1. LAWFULNESS, FAIRNESS, AND TRANSPARENCY

As established, the health sector encompasses several stakeholders such as hospitals, clinics, public health agencies, health insurance companies, pharmaceutical companies, medical research institutions, Government agencies, and Non-governmental Organizations. As these entities collect and handle personal data for various purposes, data protection principles play a significant role in the safeguarding of any personal data obtained and shared by these organizations.

Healthcare institutions in the health sector must process personal data in a lawful, fair, and transparent manner.

Processing health-related data is only legitimate if a data controller or processor meets specific criteria. These include reasons like medical diagnosis and treatment, public health considerations, and legal obligations among others, all of which must be conducted within the bounds of law. Consent from the data subject is also a valid basis for processing, provided it is explicit, specific, and easily revocable. Additionally, health-related data may be processed for the purpose of a contract with a healthcare professional or if the data subject has manifestly made the data public. Importantly, the data should only be handled by or under the responsibility of a healthcare provider or a person subject to professional secrecy under any law.

Further specifying who can process this sensitive data, section 46(1) states that personal data related to health may only be processed either by a healthcare provider or by someone obligated to maintain professional secrecy as dictated by law. The condition in subsection (1) is considered met if the processing is necessary for public interest in the area of public health or if carried out by another individual who owes a duty of confidentiality under any law. Across all these instances, it is mandatory to establish appropriate safeguards to ensure data security and the respect for individual rights.

For instance, when a health practitioner is collecting the personal data of a patient, the proper lawful purpose, which may include performance of a contract or consent, must be identified in order to process patient personal information. To secure transparency, data protection policies or notices should be issued by the healthcare institution. The privacy notices should include:

a) The categories of data processed
b) The purpose(s) for which the information will be processed
c) Information on how personal data will be collected
d) Details on how data will be kept up-to-date
e) Details on how confidential waste will be disposed of
f) Details on the use of security systems, such as computer passwords and firewalls
g) Where necessary, how personal data is encrypted when held electronically
h) Who is considered a trusted third party
i) Procedures for what to do if personal data is lost or stolen
j) Rules for sharing or transferring data outside of the healthcare institution
k) Rights regarding personal data
l) Contacts of the DPO (if applicable)

The privacy notices should be included in the registration of patients and employment process in healthcare institutions. An acknowledgment of the privacy notice should also be available at the bottom of any documents issued by the healthcare institution.

Example 1:

The relationship between a healthcare provider and their patients is in some cases based on a contractual agreement. If the personal information is collected for any purpose including the provision of medical services, the data subject should be well informed to promote transparency in the processing of the data promoting a fair and lawful approach to data collection and processing.

Example 2:

If Mr. Patient visits a healthcare facility for a medical checkup and the healthcare provider decides to use the data for clinical research collection and processing was expressly stated to be collected and processed for medical checkup, the healthcare provider will be liable for breach of the Act as processing of the data would be unlawful in that regard.

4.2. PURPOSE LIMITATION

The purpose limitation principle in the health sector means that personal data should only be collected and processed for specific and legal purposes and should not be used for any other purpose inconsistent with the identified legal purposes/basis. Some examples of how the purpose limitation principle is applied in the health sector are:

a) **Medical treatment**: Healthcare providers collect personal data from patients, such as medical history and test results, to provide medical treatment. This data should only be used for the purpose of diagnosing, treating, and monitoring the patient's health.
b) **Research**: Personal data may be collected for research purposes, such as clinical trials and epidemiological studies. The data collected should only be used for research purposes and not for any other purpose.
c) **Public health**: Public health agencies collect personal data to monitor and control disease outbreaks, such as COVID-19. This data should only be used for public health purposes and not for any other purpose.
d) **Health insurance**: Health insurance companies collect personal data to determine eligibility for coverage and to process claims. This data should only be used for insurance purposes and not for any other purpose.
e) **Health awareness**: Personal data may be collected for health awareness purposes, such as in wellness programs. The data collected should only be used for the specific health awareness program and not for any other purpose.

Example 1:

A healthcare provider collects personal data from a patient during a medical consultation. The data collected includes the patient's medical history, current symptoms, and test results. The healthcare provider only uses this data to diagnose, treat, and monitor the patient's health. The data shall not be shared with any third party without the patient's consent, and it should not be used for any other purpose, such as marketing or medical research, without the patient's explicit consent.

NB: The Data Protection Act provides that sensitive personal data shall not be processed for the purposes of direct marketing.

4.3. DATA MINIMIZATION

The data minimization principle in the health sector refers to the idea that personal data should be limited to what is necessary for a specific purpose, and should not be collected, used, or retained beyond that purpose. This means collecting only the minimum amount of data required to achieve the health purpose for which it is being collected.

The data minimization principle is found in the Kenya National eHealth policy as a security requirement for m-health services.

The healthcare provider must only process personal data to the extent necessary to achieve the medical care objectives.

Some examples of how the data minimization principle is applied in the health sector:

Medical treatment: Healthcare providers must only collect personal data that is necessary for the diagnosis, treatment, and monitoring of a patient's health.

Example 1:

Mr. Patient visits Afya bora Hospital to get medical treatment, the hospital must only collect personal data that is necessary for the diagnosis, treatment, and monitoring of a patient's health. The hospital must not collect any additional personal data that is not necessary for providing medical care, such as information about the patient's financial status or political beliefs.

a) **Research**: Personal data collected for research purposes should be limited to what is necessary for the specific research project. For example, if a research study is investigating the effectiveness of a new medication, the personal data collected should only include the relevant medical history and test results of the participants.
b) **Public health**: Personal data collected by public health agencies should be limited to what is necessary to monitor and control disease outbreaks or other public health issues. For example, during a COVID-19 outbreak, public health agencies may collect personal data related to COVID-19 testing and contact tracing, but they would not collect data related to unrelated health conditions.
c) **Health insurance**: Health insurance companies should only collect personal data that is necessary to determine eligibility for coverage and to process claims.
d) **Health Awareness**: Personal data may be collected for health promotion purposes, such as in wellness programs. The data collected should only be used for the specific health awareness program and not for any other purpose.

Example 1:

An NGO is implementing a screening program for a specific disease in a community where there are high rates of the disease. The program aims to identify individuals who may have the disease and provide them with appropriate care and treatment. To conduct the screening, the NGO needs to collect personal data from the participants, such as their name, age, contact information, and medical history. However, to adhere to data protection principles, the NGO should only collect the minimum amount of data required for the specific screening program.

4.4. ACCURACY

This principle refers to the idea that personal data should be accurate, up-to-date, and complete. This means that all health sector stakeholders should take reasonable steps to ensure that personal data is accurate and that any inaccuracies are corrected as soon as possible. Some examples of how the principle of accuracy is applied in the health sector are:

a) Medical records: Healthcare providers should ensure that medical records are accurate and up-to-date. This includes updating the records with new information as it becomes available, such as changes in a patient's medical history, allergies, or medications.
b) Test results: Healthcare providers should ensure that test results are accurate and correctly attributed to the patient. This includes verifying the identity of the patient and ensuring that the test results are correctly labeled and recorded in the patient's medical record.
c) Prescriptions: Healthcare providers should ensure that prescriptions are accurate and appropriate for the patient's condition. This includes verifying the patient's medical history, allergies, and current medications, and ensuring that the dosage and frequency of the prescription are correct.
d) Health research: Researchers should ensure that personal data used for research purposes is accurate and complete. This includes verifying the accuracy of medical records and test results used in the research and ensuring that the personal data is properly de-identified to protect the privacy of the individuals.
e) Health insurance: Health insurance companies should ensure that personal data used for determining coverage and processing claims is accurate and up-to-date. This includes verifying the patient's medical history, treatment, and medication information, and ensuring that the personal data is properly secured and protected.

Example 1:

Afya Bora Hospital collects personal data from patients at various points throughout their medical journey depending on the purpose of data collection. Afya Bora ensures that the personal data collected is accurate and up-to-date by verifying the patient's medical history and asking follow-up questions to confirm the information provided. It also ensures that the personal data is properly recorded in the patient's medical record and updates the record as necessary to ensure accuracy. In the event of any change in the patient's details earlier provided, Afya Bora updates the patient's medical record promptly to ensure that the record remains accurate and complete.

4.5. STORAGE LIMITATION

This principle requires that personal data should not be kept for longer than is necessary for the purposes for which it was collected.

All stakeholders in the health sector must have the right policies and processes in place to guarantee that personal data is safely stored and only preserved for as long as necessary in order to put the storage limitation principle into practice. In accordance with data protection legislation, the policies should have defined retention durations. The Act neither stipulates nor defines any particular retention times; therefore, entities processing personal data in the health sector must justify a stated retention time and should not preserve any personal data on a 'just-in-case' basis. Furthermore, where health data is to be retained for an unlimited amount of time, data retention regulations should provide realistic time frames for pseudonymization and anonymization. Entities in the health sector must make a justified decision about how long patient file data should be kept after a patient has received treatment or has passed away if there is no industry guidance on suitable retention periods for health data. The retention of data must be justified and should not last indefinitely.

Example 1:

A healthcare provider collects personal data from a patient during a medical consultation. The healthcare provider has developed a retention policy where it maintains patient medical records for non-returning patients or of deceased patients for a period of seven years.

The healthcare provider securely stores the personal data and following the expiration of seven years, safely destroyed the personal data or anonymizes the data. Further, the healthcare provider reviews its policies from time to time to ensure that they are in line with existing legal or regulatory requirements for data retention in the health sector.

4.6. INTEGRITY AND CONFIDENTIALITY

Confidentiality and data security are critical principles in the health sector, given the sensitivity of personal health information. This principle requires that personal data must be processed in a manner that ensures its security, including protection against unauthorized or unlawful processing against accidental loss, destruction, or damage.

Therefore, all technical procedures used to gather, process, store, use, or distribute data should make use of strong security safeguards, for which threshold standards must be established. This may involve data encryption, security keys, two-factor authentication, and password requirements. Facilities for data processing and storage must be secure in accordance with both international and national standards. Moreover, all health stakeholders should conduct periodic data security audits**.**

Some **key aspects of confidentiality and data security in the health sector** are:

a) **Confidentiality**: Healthcare providers are required to maintain the confidentiality of personal health information. This includes ensuring that only authorized individuals have access to the information and that the information is not disclosed or shared without the patient's consent except where required under a court order. ***Example: Section 11 of the Health Act No 21 of 2017 provides for informed consent of the patient for research and policy planning purposes.***

b) **Data security**: Healthcare providers are also required to ensure that personal health information 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.

c) **Training and awareness**: Healthcare providers and their employees should be trained and made aware of their responsibilities to protect the confidentiality and security of personal health information. This includes understanding the legal and ethical obligations, as well as the risks and consequences of unauthorized disclosure or data breaches.

d) **Risk assessment**: Healthcare providers should conduct regular risk assessments to identify potential vulnerabilities in their systems and processes, and to implement appropriate safeguards to mitigate those risks.

Example 1:

A hospital may store patient records in a secure location and limit access to authorized personnel only. The hospital should also have appropriate technical and organizational measures in place to protect the personal data from unauthorized access, loss or theft, and back up the data regularly to prevent loss. The hospital can also implement password protected systems to secure records among others. Examples of physical security measures are securing physical records in locked cabinets or rooms and implementing security measures such as video surveillance or security guards, to prevent unauthorized access to facilities.

Example 2:

To uphold the principle of confidentiality, healthcare providers should ensure that they develop, train and implement effective data handling procedures. This is important to prevent data breaches that could result due to the unauthorized access or disclosure of personal health data. For instance, a healthcare provider may face sanctions for breaching data privacy if a patient report being inappropriately contacted by their member of staff after treatment.

4.7. ACCOUNTABILITY

Accountability involves taking proactive steps to protect personal data.

The accountability principle in the health sector refers to the responsibility of healthcare institutions and stakeholders to ensure compliance with relevant laws and regulations related to the collection, use, and disclosure of personal health information.

Stakeholders in the health sector should have policies and procedures in place to govern the collection, use, and disclosure of personal health information. These policies and procedures should be reviewed and updated regularly to ensure compliance with changing legal and regulatory requirements.

Example 1:

When data breaches occur, Healthcare institutions are required to notify the individuals affected as well as report the breach to the appropriate regulators. Information on the nature of the breach, what data may have been exposed, and specific actions taken to prevent a similar breach in the future should be provided. Independent oversight mechanisms must review every significant breach.

Example 2:

To uphold the principle of accountability, a healthcare provider is required to establish a Data Processing Agreement that clearly outlines the responsibilities of any vendors they have contracted. This agreement ensures that the vendors are aware of their obligations and equally safeguard the personal data in their possession. Also taking cognizant that they will be held accountable for any breach of personal data that may occur.

5. LAWFUL BASIS OF PROCESSING

Regardless of the purpose of processing personal data, such processing is assumably not permitted unless the health care provider has a valid lawful basis to do so. There are a number of lawful bases that exist for processing personal data. No single basis is better or more important than the others. The lawful basis which is most appropriate to use will depend on the purpose of the processing and the relationship with the individual.

The lawful basis must be determined prior to the processing and must be properly documented, as per processing activity. It is also important to note that the processing activity shall only rely on one legal basis for processing at a time.

For health service providers, given the sensitivity of the information that they process, prior to commencing processing personal data, they must carefully assess which lawful basis is appropriate for a given processing activity and ensure that all relevant requirements are met. In detail, the lawful basis is as follows.

5.1. CONSENT

This is a lawful basis where the data subject has given clear informed consent for the processing of personal data for a specific purpose.

Consent must be freely given, informed, specific, and unambiguous. It must be a statement or clear affirmative action signifying agreement to the processing, and the person has the right to withdraw their consent at any time. Entities in the health sector have the duty to keep a verifiable record of the consent, especially for treatment.

Free consent: consent of the data subject must represent the free expression of an intentional choice. The existence of free consent is only valid if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion, or significant negative consequences if he/she does not consent.

Informed consent: The data subject must have sufficient information before exercising his or her choice. Informed consent will usually comprise a precise and easily understandable description of the subject matter requiring consent.

Specific consent: For consent to be valid, it must also be specific to the processing purpose, which must be described clearly, and in unambiguous terms. This goes hand-in-hand with the quality of information given about the purpose of the consent.

***Unambiguous consent*:** All consent must be given in an unambiguous way. This means that there should be no reasonable doubt that the data subject wanted to express his or her agreement to allow the processing of his or her data. For instance, inactivity from a data subject does not indicate unambiguous consent.

It is important to note that there is consent required for provision of health services which is different from the consent required for processing personal data in the health sector. In the health sector, pursuant to section of Health Act, 2017, no specified health service may be provided to a patient without the patient's informed consent unless

a) the patient is unable to give informed consent and such consent is given by a person mandated by the patient in writing to grant consent on his/her behalf or authorised to give such consent in terms of any law or court order;
b) the patient is unable to give consent and no person is mandated or authorized to give such consent but the consent is given by the next of kin;
c) the provision of health service is authorised by an applicable law or court order
d) the patient is treated in an emergency situation;
e) failure to provide the health service will result in a serious risk to public health or any delay in the provision of the service may result in the death or irreversible damage to the health of the patient.

Medical consent and consent under data protection Act serve different purposes and are governed by different legal frameworks, although both are forms of explicit permission from an individual.

Medical Consent: This is a specialized form of consent required in healthcare settings, where patients agree to undergo medical treatment, surgery, or participate in clinical research. Medical consent is generally focused on ensuring the patient understands the nature of the medical procedure, its risks, benefits, and alternatives, so they can make an informed decision about their healthcare. The focus here is on bodily autonomy and informed medical decision-making.

Data Protection Consent: This form of consent relates to the collection, processing, and storage of personal data, including health-related data. Under the Data Protection Act, individuals have the right to know how their data will be used, stored, and who it will be shared with. The focus here is on informational self-determination—the right to have control over one's own personal data.

While both types of consent require clear, informed, and explicit permission, they are distinct in what they govern and protect. Medical consent does not necessarily grant the right to share or store medical data for other purposes, and conversely, data protection consent does not permit medical procedures or treatments

Example 1:

A group of medical practitioners in Kenya organised for a free medical camp in their hometown. Mr. Patient who was a resident of the town had a health issue that he wanted treated. He visited the camp and after consulting with the doctor, he was informed that the medical practitioners needed to see his medical file from the previous treatment. In such a situation, Mr. Patient may give his consent for his personal data such as medical history, test results to be shared by the hospital with the medical practitioners to ensure he receives the best possible healthcare service from the camp.

Example 2:

A person agrees to receive promotional emails to an address he or she provides to an insurance agent. Should the person withdraw consent, the agent must immediately stop sending promotional emails. In additional, there must be a provision in place to allow the person to withdraw their initial consent.

5.2. PERFORMANCE OF A CONTRACT

Personal data may be processed if the processing is necessary for performance of a contract to which the data subject is a party.

Entities in the health sector may process personal data to fulfill a contractual obligation, and must not use the personal data for any other purposes that are not related to the performance of the contract. This provision also covers pre-contractual relationships. For instance, in cases where a party intends to enter into a contract, but has not yet done so, possibly because some checks remain to be completed. If one party needs to process data for this purpose, such processing is legitimate as long as it is necessary in order to take steps at the request of the data subject prior to entering into a contract.

Example 1:

A hospital has a contract with a health insurance company to provide medical services to its members. As part of the contract, the hospital is required to process personal data related to the health of the members in order to provide medical care and bill the insurance provider.

The hospital will process this data in compliance with applicable data protection laws and the terms of the contract.

5.3. COMPLIANCE WITH LEGAL OBLIGATION

Personal data may be processed if it is necessary for compliance with a legal obligation to which the data controller is subject.

Entities in the healthcare 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.

Example 1:

Regulatory bodies in the health sector such as the Pharmacy and Poisons Board has legal obligation to inspect, monitor and evaluate the standards of services engaged in the health sector. In this case, to carry out their duty, the Pharmacy and Poisons Board may process personal data to comply with their legal obligation.

Example 2:

Employers in the healthcare sector are obliged to process data about their employees for the purpose of employment benefits, salary payments, performance evaluation taxation and others.

5.4. PROTECTION OF VITAL INTERESTS OF THE DATA SUBJECT

The Data Protection Act provides that personal data processing is lawful if it "is necessary in order to protect the vital interests of the data subject.

In the health sector, a vital interest of a data subject could be their medical emergency situation.

Example 1:

if a patient is unconscious and unable to communicate, their medical records and health information could be accessed by healthcare providers without their consent in order to provide the necessary medical treatment to save their life. This is considered a vital interest because it is necessary to protect the life of the patient and ensure they receive appropriate medical care in an emergency situation.

5.5. LEGITIMATE INTERESTS PURSUED BY THE HEALTH CARE PROVIDERS

The Data Protection Act provides that personal data may lawfully be processed if it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection.

The health services providers must ensure that the processing of personal data is necessary for the legitimate interest pursued and that the individual rights and freedoms of data subjects are not outweighed by those legitimate interests.

Example 1:

Healthcare providers may process personal data for the purposes of managing and administering health care services. For example, they may use personal data to schedule appointments, maintain patient records, or manage billing and insurance claims. This processing is necessary for the proper administration of healthcare services and is considered a legitimate interest.

Example 2:

Healthcare providers may process personal data for the purposes of clinical research to develop new treatments, drugs or therapies to improve patient outcomes. The processing of personal data in this context is necessary for scientific research purposes and is considered a legitimate interest.

5.6. PUBLIC INTEREST

The Act provides that personal data may be lawfully processed if it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

Entities in the health sector may process personal data to safeguard the public interest. However, these entities must ensure that the processing of personal data 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.

Example 1:

Healthcare providers may share with public health authorities' personal data to monitor and track the spread of infectious diseases, such as COVID-19, Ebola, Cholera, to help identify the outbreaks and contain the spread of the disease.

5.7. HISTORICAL, STATISTICAL, JOURNALISTIC, LITERATURE AND ART OR SCIENTIFIC RESEARCH

Historical, statistical, journalistic, literature, and art or scientific research 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 in the society.
c) **Statistical Research**: Health care providers can carry out statistical research using health data for purposes of monitoringtrends in disease incidences and the prevelance to predit and control any outbreaks of contagious diseases, such as cholera.

Example 1:

A research institution is conducting a study on the prevalence of a particular genetic disease in a certain population. In order to conduct this research, the institution needs to collect personal data from individuals who have been diagnosed with the disease.

The personal data that the institution requires includes:

a) Personal identifying information, such as name, age, and contact details
b) Health-related information, such as medical history, genetic test results, and disease diagnoses

The institution must process this data solely for the purpose of conducting scientific research and will implement appropriate technical and organizational measures to ensure the security of the personal data and prevent unauthorized access, disclosure, or loss of the data. Further, the institution must comply with the requirement under data protection laws such as obtaining valid consent from the individuals whose personal data is being processed for research purposes.

6. RIGHTS OF A DATA SUBJECT

These are rights of a data subject (a patient) exercisable with respect to the processing of their data. The Data Protection Act provides data subjects (patients) with certain enforceable rights regarding their personal health information.

The Data Protection Act aims to empower citizens to exercise their rights in a world increasingly dominated by technology companies and other players that process vast amounts of data relating to citizens. The empowerment of citizens is equally important in the context of medical care and similar health-related settings.

Adherence to the rights of data subjects is of the utmost importance – in particular, in the context of public health activities, as such compliance by healthcare institutions fosters citizens' trust in the processing activities.

It is the duty of Health service providers to provide data subjects with modalities and avenues where the data subject can exercise their rights.

6.1. RIGHT TO BE INFORMED

This is the right to be informed of the use to which data is put. It allows data subjects (patients) to know what personal data is collected about them, why, and who is collecting data, how long it will be kept, how they can file a complaint, and with whom they will share the data.

Example 1:

Mr. Patient visits a hospital in his home area to get health service using his medical cover and the health facility receptionist requested him to fill out a form. The receptionist is required to inform Mr. Patient before collecting the data, what data is to be collected, the basis of collection, the purpose of collecting, how long it will be kept, how it is protected, and with whom they will share the data.

6.2. RIGHT TO ACCESS PERSONAL DATA

The Data Subject has the right to access personal data in the custody of the health care provider that is, which type of data is held about them, details of the data control, details of any recipients, and data retention period. This right allows the data subject to have visibility on what personal data is being processed.

The health sector is required to develop a mechanism to verify the request, track all the data access requests, and provide the information requested to the data subject.

Example 1:

After personal data is collected, the Data Subject has the right to access what data about him/her exist in the custody of the health care provider, and for what purposes. He/she can request the health care provider to grant access to the personal data and the request should be addressed within 7 days.

Example 2:

Mr. Patient went to the hospital he visited the last time where he filled out the form. He requested to access his personal data in the custody of the hospital. Mr. Patient must be granted access to his personal data in a portable, machine-readable manner and the request should be addressed within 7 days.

Example 3:

Accessing his personal data will help Mr. Patient to determine whether or not the data are accurate. It is, therefore, essential that the data subject is informed, in an intelligible form, not only of the actual personal data that are being processed, but also the categories under which these personal data are processed.

6.3. RIGHT TO RECTIFICATION OF PERSONAL DATA

This means that individuals have the right to request corrections to inaccurate or incomplete information held about them in their health records. The health sector must implement a process and the technical capabilities to verify the request, correct the data and confirm correction with the data subject. In addition, this also applies to data the data controller passed on to third parties, health service providers need a process to securely inform them of the correction.

Overall, the right to rectification of personal health data is important for ensuring that individuals have accurate and complete information in their health records, which can ultimately lead to better healthcare outcomes.

Example 1:

Mr. Patient discovered that his record in the NHIF portal is incorrect. Mr. Patient has the right to request that inaccurate personal data be corrected, or incomplete data be completed. Mr. Patient, request the NHIF that the information about him in the portal is incorrect and should be corrected. The NHIF is required to correct the data within 14 days

Example 2:

A patient has a genetic predisposition to a certain disease, but their medical records does not reflect this information. They can request that the health care provider update their records to include this important information.

6.4. RIGHT TO OBJECT TO ALL OR PART OF THEIR PERSONAL DATA BEING PROCESSED

This right allows individuals to object to the processing of their personal health data, including medical records and other health-related information.

Examples of when an individual may exercise their right to object to the processing of their personal health data include:

a) **Marketing**: If an individual's personal health data is being used for marketing purposes without their consent, they may object to the processing of their personal health data.
b) **Research**: If an individual's personal health data is being used for research purposes without their consent, they may object to the processing of their personal health data.
c) **Third-party access**: If an individual's personal health data is being shared with third parties without their consent, they may object to the processing of their personal health data.
d) **Inaccurate data**: If an individual believes that their personal health data is inaccurate or incomplete, they may object to the processing of their personal health data until it is corrected.
e) **Automated decision-making**: If an individual's personal health data is being used for automated decision-making processes without their consent, they may object to the processing of their personal health data

It is important to note that the right to object is not an absolute right and can be limited in certain circumstances. For example, if the processing of personal health data is necessary for the provision of healthcare services or for the establishment, exercise, or defense of legal claims, then the right to object may not apply.

6.5. RIGHT NOT TO BE SUBJECTED TO AUTOMATED DECISION MAKING

A person can object to automated processing of their data. A data subject has the right to demand human intervention, rather than having important decisions made solely by algorithm automatically.

Example 1:

Mr. Patient is a patient at Newcare hospital and is receiving treatment for a chronic condition. A machine learning algorithm is used to predict patient outcomes and determine the best course of treatment for Mr. Patient. However, Mr. Patient expresses his concern about being subject to automated decision- making and asserts his right to not be subject to such decisions.

In response, the healthcare providers at Newcare hospital ensure that Mr. Patient's right to not be subject to automated decision-making is respected. They involve Mr. Patient in important conversations about his treatment plan and consider his individual circumstances and preferences. They also provide Mr. Patient with alternative options for treatment that do not rely on automated decision-making tools.

This approach prevents discrimination against patients like Mr. Patient and ensures that their rights are respected. It also highlights the importance of healthcare providers being aware of patients' rights and preferences regarding automated decision-making, and taking steps to ensure that those rights are upheld.

6.6. RIGHT TO ERASURE.

This right is also known as the right to be forgotten. It allows individuals to request the deletion or removal of their personal data by healthcare providers.

Example 1:

Mr. Patient was transferred from his workstation in Nairobi to a new station in Mombasa. He requested his data be deleted from the database of the hospital he used to visit for health services using his medical card. The hospital is required to delete the personal information from its records and immediately cease further dissemination of the data.

6.7. RIGHT TO DATA PORTABILITY

This right gives individuals the right to receive a copy of their personal data in a structured, commonly used, and machine-readable format, and the right to transmit that data to another data controller without hindrance.

In relation to processing personal data for health services, the right to data portability is important for individuals who wish to switch from one healthcare or transfer their personal data to new healthcare.

Example 1:

Mr. Patient was transferred from his workstation in Nairobi to Mombasa. He went to the hospital he used to visit for health service using his medical card and tell them "I want to transfer the information you hold on me to another health service provider". To comply with this provision, the hospital should provide data in a structured, machine-readable format that can transmit directly to the other provider within 30 days from the date of request.

7. COMPLIANCE OBLIGATIONS OF HEALTH SECTOR

7.1. REGISTRATION WITH THE ODPC

All entities involved in the healthcare sector must undergo mandatory registration.

The Office has published a Guidance Note on Registration of Data Controllers and Data Processors which is accessible through www.odpc.go.ke. The Guidance Note includes a step-by-step guide on how to complete the registration process and the information required during the registration process.

7.2. PRIVACY BY DESIGN OR BY DEFAULT

Data protection by design is a concept that refers to the incorporation of data privacy and security measures into the design of products, services, and systems from the very beginning, rather than as an afterthought. This is especially important in the players in the health sector, where sensitive personal health information is processed.

The Data Protection Act, in section 41, outlines the requirement for entities in the health sector to implement appropriate technical and organisational measures to ensure the effective implementation of data protection principles and necessary safeguards in data processing. Additionally, the act requires that only necessary personal data is processed, considering the amount of data collected, the extent of its processing, storage period, accessibility, and cost of processing.

Data protection by default requires data controllers and processors to ensure that only data that is necessary to achieve your specific purpose is processed. Data protection by default requires entities to ensure that data protection issues have already been considered and protection methods incorporated into existing systems and practices.

This concept requires organisations to implement data protection measures by default, without the need for individuals to take any specific actions to protect their personal data. In the health sector, this means that data protection measures must be in place from the outset, without relying on individuals to opt-in or take additional steps to protect their health information.

Examples of data protection by default in the health sector include:

a) **Access controls:** Implementing access controls, such as password-protected accounts, can help to ensure that only authorised personnel have access to sensitive health information.
b) **Data encryption:** Encrypting sensitive health information at rest and in transit can help to prevent unauthorized access and protect against data breaches.
c) **Anonymization:** This involves removing all identifying information from health data, making it impossible to identify individuals. This can help to protect privacy while still allowing for analysis of health data.

d) **Data retention policies:** Implementing policies that limit the retention of personal health information to only what is necessary can help to reduce the risk of privacy breaches and protect individual privacy.
e) **Data protection impact assessments:** Conducting regular data protection impact assessments can help organizations identify and mitigate potential privacy risks in the processing of personal health information.
f) **Data protection policies and procedures:** Organizations should establish clear and comprehensive data protection policies and procedures that outline the measures taken to protect personal data. These policies should be communicated to all employees and regularly reviewed and updated.
g) **Staff training:** All staff should receive regular training on data protection policies and procedures. This can include how to handle personal data, how to recognize and respond to data breaches, and how to comply with data protection regulations.

Example 1:

A healthcare provider in Kenya recently learned about the existence of the new Data Protection Act and the need to comply with data privacy by design or default obligations. In response, they decided to integrate privacy considerations into the design process of their new electronic medical records system. They formed a design team that included privacy experts and performed a Data Protection Impact Assessment (DPIA) to identify and mitigate potential privacy risks. Furthermore, the healthcare provider ensured that all system components were designed with privacy in mind, such as implementing access controls and data encryption. They also developed privacy policies and procedures to govern the collection, use, and disclosure of personal data in their organization. This included training employees on data protection and requiring them to sign confidentiality agreements.

7.3. DATA STORAGE

The storage limitation principle is a critical part of data protection that mandates that personal information should only be held for as long as it's required. 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.

The storage limitation principle is essential for several reasons. Firstly, it helps to make sure that personal information is accurate and current, as old data can be misleading or damaging. Secondly, it can prevent the misuse of personal data, as data that's no longer needed is less likely to be used intentionally or accidentally. Finally, it safeguards the privacy rights of individuals, as personal data that's no longer needed is less likely to be accessed or revealed without the individual's permission.

As a result, entities have a responsibility to comply with the storage limitation principle. They must put in place personal data retention schedules that specify the retention purpose, duration, and audit provisions, among other things.

During the audit, entities must pay attention to personal data that has already fulfilled its purpose, ensure that the information is up-to-date, and specify the purpose of retention. They must also guarantee that the security measures are sufficient and identify the best course of action when the retention period has elapsed.

Health sector players must establish policies and procedures for the retention and deletion of personal data and regularly review and update them to ensure they remain relevant and effective.

Example 1:

A researcher in Kenya conducting a study on malaria prevalence is obligated to securely store personal data after the study concludes, in accordance with the data storage limitation principle. To meet the requirements of the Kenya Data Protection Act, the researcher needs to establish clear guidelines, performs regular reviews of the data, and employs pseudonymization and other anonymization techniques to safeguard the privacy of the individuals whose data was collected.

7.4 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The carrying out of a DPIA is only mandatory where processing is "likely to result in a high risk to the rights and freedoms of data subjects". In cases where it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers and/or data processors comply with data protection law. In addition to the aforesaid, the Act requires that all data controllers and processors implement appropriate technical and organisational measures and integrate appropriate safeguards to ensure the adequate protection of personal data of data subjects.

EXAMPLE 1:

A pharmaceutical firm is developing a new medication that requires the processing of sensitive health data of clinical trial participants. Such exercise is likely to result in a high risk to the rights and freedoms of data subjects, so conducting a Data Protection Impact Assessment (DPIA) is a requirement. In conducting a DPIA, the firm will identify and assess the potential risks and impacts on the rights and freedoms of the data subjects, such as the privacy and confidentiality of their health data. Based on the DPIA results, the firm implements appropriate technical and organizational measures, such as data encryption and access controls, to ensure the adequate protection of personal data. The firm must ensure that appropriate safeguards are integrated throughout the medication development process to prevent any unauthorized or unlawful processing, accidental loss, or destruction of personal data. The firm will also be required to regularly review and update its data protection policies and procedures to ensure compliance with data protection laws and regulations.

The Office has published a Guidance Note on Data Protection Impact Assessments on www.odpc.go.ke The Guidance Note includes the form in which a Data Protection Impact Assessment should be submitted and guidance on when it should be submitted.

7.5. NOTIFICATION AND COMMUNICATION OF BREACH

Data Controllers have to report personal data breaches to the ODPC without delay within 72 hours of becoming aware of the breach. Where there has been unauthorised access, players within the health sector are required to communicate to the affected data subjects in writing within a reasonable period, unless the identity of the data subject cannot be established.

Entities are required to report data breaches to the Office and provide certain information about the breach. This information includes the date and circumstances in which the data breach was discovered, a chronological account of the steps taken after the breach was discovered, and details on how the breach occurred. Additionally, entities must provide the number of data subjects affected, the personal data or classes of personal data affected, and the potential harm to affected data subjects. The entity must also provide information on any action taken to mitigate the harm and remedy any failure or shortcoming that contributed to the breach, and how affected individuals can mitigate potential harm.

Example 1:

If a hospital experiences a data breach where the personal health information of patients is accessed by an unauthorized third party, they must report it to the Office of the Data Protection Commissioner (ODPC) within 72 hours. The hospital should also inform the affected patients in writing unless their identity is unverifiable. They must provide details such as the date and circumstances of the breach, a chronological account of the actions taken following the breach, the number of impacted patients, and the types of personal data involved. The hospital must also explain the steps taken to mitigate harm and prevent future breaches, including employee data protection training, stronger access controls, and regular security protocol reviews.

7.6. ENGAGEMENT OF DATA PROCESSORS

Health industry players engage with a variety of data processors that handle different types of health data. Some examples of data processors that the health sector may engage with include: Electronic health record (EHR) vendors who provide software platforms that health facilities can use to manage patient health records. They may also provide data storage and backup services, Clinical research organizations (CROs) who conduct clinical trials and other research studies in the health sector. They may handle large amounts of health data related to clinical trial participants, Health information exchanges (HIEs) who facilitate the sharing of health data between different health facilities and providers. They may process large volumes of health data from different sources, medical billing companies that process claims and payments for healthcare services. They may handle sensitive financial and personal information related to patients and Analytics companies who provide data analysis services to help health facilities and providers make informed decisions. They may process large volumes of health data from different sources among other data handlers.

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.

The Act sets out that where an entity engages a vendor or service provider (processor) to process information on its behalf, there must be a written contract (Data Protection Agreements) stipulating that the processor acts only on the controller's instructions and is bound by the obligations of the controller. Further, both parties should take all reasonable steps to ensure that any person employed by or acting under the authority of the data controller or data processor complies with the relevant security measures.

Example 1:

A hospital contracts a laboratory firm to process medical tests for its patients. The laboratory will handle sensitive health information, such as the patient's medical history and test results. To comply with relevant laws and regulations related to data protection and confidentiality, the hospital and laboratory will need to have a written contract stipulating that the laboratory acts only on the hospital's instructions and is bound by the obligations of the hospital as the data controller. Additionally, both parties would need to take all reasonable steps to ensure that any person employed by or acting under the authority of the hospital or laboratory complies with relevant security measures to ensure the secure and ethical handling of patient health data and protection of patient privacy.

Example 2:

A hospital engages a Hospital Management Information System (HMIS) as a data processor to manage and analyse patient health records. Both parties will sign a written contract stipulating that HMIS acts only on the hospital's instructions and is bound by the hospital's obligations as the data controller. They will also take all reasonable steps to ensure that any person employed by or acting under the authority of the hospital or HMIS complies with relevant security measures to ensure the confidentiality and security of patient health data. This would help to ensure that health data is handled securely and ethically, and that patient privacy is protected.

7.7. DATA SHARING

The obligation of Data Sharing is governed by several laws and regulations, including the Health Act of 2017, the Data Protection Act of 2019 and Regulations, and the Kenya Health Policy 2014- 2030.

Under these laws and policies, healthcare institutions and practitioners are required to share health data with relevant stakeholders, such as government agencies, researchers, and other healthcare institutions, to improve health outcomes for the population. However, data sharing must be done in accordance with the principles of confidentiality, privacy, and informed consent.

Additionally, the Ministry of Health in Kenya has established the Health Information System (HIS) to facilitate the collection, analysis, and sharing of health data across the country. The HIS includes various data systems, such as the District Health Information System (DHIS2), which is used to collect and manage health data at the facility level, and the Kenya Health Information System (KHIS), which is used to aggregate data from different sources.

The obligation of data sharing in the health sector in Kenya is critical for improving health outcomes and addressing health disparities, but it must be done in a responsible and ethical manner, ensuring the protection of individuals' privacy and confidentiality.

Example 1:

A hospital in Kenya is participating in a multi-center study on a new cancer treatment. To contribute to the study, they need to share patient data with other participating hospitals. To comply with data- sharing principles, the hospital establishes clear data-sharing agreements, anonymizes the data, obtains patient consent, and uses secure data transfer methods.

7.8. DATA TRANSFER

Data controllers or data processors transferring personal data must ensure that the transfer complies with appropriate data protection safeguards, is a necessity, or has the consent of the data subject. If personal data is being transferred to a third country or relevant international organization, appropriate safeguards must be in place.

This can include data protection legislation equivalent to Kenya's Data Protection Act or assessments made by the data controller that appropriate safeguards exist to protect the data. The data controller also has an obligation to document the transfer and provide documentation to the Data Commissioner upon request. If the transfer is a necessity, it must be strictly necessary for purposes such as performing a contract or establishing a legal claim, and the data subject's fundamental rights and freedoms must not be overridden.

If there are no appropriate safeguards or necessities for the transfer, then the data subject must explicitly consent to the transfer and be informed of the possible risks. Sensitive personal data can only be transferred with the consent of the data subject, and a written agreement can be made between the transferring entity and the recipient with provisions for accessing a robust information system and identifying the countries and territories to which the personal data may be transferred.

7.8.1 DATA LOCALIZATION

Data localization in the health sector refers to the practice of storing and processing health data within the country's borders. The Data Protection Act of 2019 mandates that all data controllers and processors must ensure that personal data is stored and 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.

Example 1:

Specialist doctors in Kenya want to transfer patient data to doctors in India who do not have a Data Protection Act. To ensure compliance with data protection regulations, the Kenyan doctors must establish appropriate safeguards for the transfer. Additionally, the patient must explicitly consent to the transfer and be informed of any risks involved. Sensitive personal data can only be transferred with the patient's consent and a written agreement with provisions for identifying the countries and territories to which the data may be transferred.

7.9. DUTY TO NOTIFY

One of the fundamental principles of data protection is transparency, which means that personal data collected by entities in the health sector must be processed in a fair and transparent manner. According to Section 29 of the Act, data controllers and data processors are obligated to notify data subjects of their rights specified in the Act, 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. All this information should be contained in a data protection policy, which should be made available to data subjects before or as soon as possible after the collection of their personal data.

When drafting a privacy policy, it is important to use clear and plain language that is easy to understand, avoiding technical or legal jargon as much as possible. The policy should be comprehensive, covering all relevant information that data subjects need to know about the processing of their personal data, including their rights, the purpose of data collection, third-party recipients, and safeguards in place. The policy should also be accessible to data subjects, for example, by providing it on the entity's platform or upon request. Regular review and updates of the policy are necessary to ensure that it reflects any changes in data processing practices or relevant laws and regulations.

To ensure that privacy policies are comprehensible for data subjects, entities can utilize various methods, such as incorporating visual aids like illustrative elements and visual representations, implementing a question-and-answer structure, and dividing the policy into shorter sections with distinct headings. Additionally, giving practical examples of how personal data might be utilized can assist data subjects in comprehending the policy and understanding the consequences of sharing their personal information.

8. ANNEX A- OTHER APPLICABLE LEGISLATIVE FRAMEWORK AND POLICIES

HEALTH ACT 2017

The Health Act was enacted in June 2017 to establish a unified health system, to coordinate the inter-relationship between the national government and county government health systems, to provide for the regulation of health care service and health care service providers, health products, and health technologies, and for connected purposes.

The Act recognizes the right to privacy in the context of standards of health. It recognizes the right to be treated with dignity and respect and has their privacy respected in accordance with the provisions of the constitution and the Act.

There are other legal frameworks that exist in the health sector which address the aspect of data protection and the right to privacy. More elaboration of the additional legal frameworks is available in Annex A.

HEALTH SECTOR ICT STANDARDS AND GUIDELINES

The Standards and Guidelines were developed in 2013 by the Ministry of Health in recognition of the value of using ICT to enhance efficiency and delivery of service in the health sector. The standards are applicable to those in the health sector using ICTs in offering services or information to the public, further, the standards were developed to provide guidance and a consistent approach in the health sector in establishing, acquiring, and maintaining current and future information systems and ICT infrastructure.

The Standards and Guidelines, addressing the operation of ICT systems include references to data protection, privacy, and confidentiality. Privacy is perceived in the context of the users who use the MOH ICT systems. Confidentiality is also perceived in the context of keeping the users' documented account information confidential, information security requirements that must be adhered to by staff using information systems also include confidentiality.

KENYA STANDARDS AND GUIDELINES FOR M-HEALTH SYSTEMS.

The Standards and Guidelines on mHealth systems were developed in 2017 with the intention of ensuring that all mHealth-based systems are correctly implemented, with the implementation of the Standards reducing duplication of efforts in promoting data and information sharing among systems and harnessing the proper use of mobile technology. The Standards and Guidelines apply to the health sector at all levels of health care and health management levels and provide guidance in establishing, acquiring, and maintaining mobile-based health information systems that foster data and information sharing across multiple systems

KENYA NATIONAL EHEALTH POLICY 2016-2030

The national eHealth policy was formulated in 2016 and is intended to be applicable till 2030 the policy document was developed to develop long-term strategies, policy guidelines, and standards governing the adoption, deployment, and utilization of eHealth products and services in Kenya. Data protection in this policy is also viewed in the context of privacy and confidentiality.

THE KENYA NATIONAL PATIENTS' RIGHTS CHARTER

The Patient's Rights Charter was issued by the Ministry of Health in 2013, in recognition of health as a constitutional right. The charter is meant to inform clients and patients of their rights and responsibilities and provides guidelines for the resolution of conflicts where conflict arises between parties. The first chapter covers patients' rights, under these rights, those that can be directly linked to data protection are the right to confidentiality, the right to give informed consent to treatment, and the right to information. The second chapter covers responsibilities, linked to data protection is the responsibility to give health care providers relevant, accurate information.

HEALTH INFORMATION POLICY 2014-2030

First issued in 2014 by the Ministry of Health, the Health Information Policy was developed to provide guidance on the management of health information. This was due to the introduction of the Health Information System (HIS) and the continued adoption of ICT in the health sector. The policy addresses data collection and information sharing, guidelines on data processing, data warehousing, mandatory reporting by healthcare providers, and quality data management in the health sector.

HIV AND AIDS PREVENTION AND CONTROL ACT

Enacted in 2006, the HIV and AIDS Prevention Control Act came into force in 2009 and provides measures for the prevention, management, and control of HIV and AIDS, the protection and promotion of public health, and for the appropriate treatment, counseling, support, and care of persons infected or at risk of HIV and AIDS infection, and for connected purposes.21 The Act recognizes the sensitive nature of information relating to HIV tests and related medical assessments and makes specific provisions on privacy and confidentiality.

9. ANNEX B- CHECKLIST FOR COMPLIANCE

Health service providers can use the following checklist to determine if they are compliant with the Act and other subsidiary regulations.

CHECKLIST FOR COMPLIANCE:

#	Description	Yes	No	Comments/ Remedial Actions
1.	We respect the right to privacy as a fundamental human right as provided by Article 31(c) and (d) of the Constitution.			
2.	We have identified an appropriate legal basis for our processing under Section 30 of the Data Protection Act (DPA).			
3.	In Health Sector, we process sensitive data, we have identified permitted grounds under section 44 of the DPA			
4.	We restrict processing where the legal basis ceases to apply.			
5.	We do not do anything generally unlawful with the personal data or inconsistent purpose for processing.			

6.	If we are subject to mandatory registration, we have submitted to the Office of Data Protection Commissioner (ODPC) accurate and up-to-date information concerning our processing activities.			
7.	We have considered how the processing may affect the individuals concerned and can justify any adverse impact.			
8.	We only handle data about individuals in ways they would reasonably expect, or we can clearly explain why any unexpected processing is justified			
9.	We do not allow any discrimination or exploitation of the needs or vulnerabilities of a data subject.			
10.	We do not deceive or mislead people when we collect their personal data.			
11.	We have clearly identified our purpose or purposes for processing and have clearly documented those purposes.			

12.	We include details of our purposes in our privacy notices.			
13.	We regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.			
14.	If we plan to use personal data for a new purpose, we check that this is compatible with our original purpose, or we obtain specific consent for the new purpose.			
15.	We use technical measures to limit the possibility of repurposing personal data.			
16.	We only collect personal data which is adequate, relevant, and limited to what is necessary for our specified purposes.			
17.	We can demonstrate the relevance of the data to the processing in question.			
18.	We periodically review the data we hold, and delete anything we don't need.			

19.	We avoid the creation of more copies or entry points for data collection than is necessary.			
20.	We ensure that it is not possible to re-identify anonymised data or recover deleted data and test whether this is possible.			
21.	We ensure the accuracy of any personal data we process and the reliability of our sources.			
22.	We have appropriate processes in place to check and verify the accuracy of the data we collect, and we record the source of that data.			
23.	We carry out tests for accuracy at critical steps.			
24.	We use technological and organisational design features to decrease inaccuracy and mitigate the effect of an accumulated error in the processing chain.			
25.	We have a process in place to identify when we need to keep the data updated to fulfill our purpose properly, and we update it as necessary.			

26.	If we need to keep a record of a mistake, we clearly identify it as a mistake.			
27.	We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of personal data.			
28.	As a matter of good practice, we keep a note of any challenges to the accuracy of personal data.			
29.	We know what personal data we hold and why we need it.			
30.	We carefully consider and can justify how long we keep personal data.			
31.	We have a policy with standard retention periods where possible.			
32.	We regularly review our records with a view of identifying personal data that no longer requires to be retained and delete or anonymise such data.			

33.	We have appropriate processes in place to comply with individuals' requests for rectification and/or erasure of false or misleading data about them.			
34.	We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.			
35.	We do not transfer data outside Kenya unless there is proof of adequate data protection safeguards or valid consent from the data subject.			
36.	We checked and fulfilled all conditions set under part VI of the DPA and Regulations 2021.			
.				
38.	We have documented those purposes.			
39.	We include details of our purposes in our privacy notices.			