ENSURING DATA PROTECTION IN THE HEALTH SECTOR !

WWW.SENTINELAFRICACONSULTING.COM

A COMPREHENSIVE GUIDE

In December 2023, the Office of the Data Protection Commissioner released a comprehensive guidance note on the processing of health data. Its purpose is to serve as a resource for healthcare institutions in Kenya, outlining the legislative framework, data protection principles, lawful basis of processing, compliance obligations, and the rights of data subjects in the health sector.
he health sector in Kenya extensively utilizes personal data for various purposes, including registration, diagnosis, storage, analysis, and transfer. Technologies such e-health and m-health have transformed the management and accessibility of healthcare data, improving care coordination and patient outcomes. Key stakeholders in the sector include patients, hospitals, laboratories, donors, health workers, and others.

The adoption of advanced technologies however, raises privacy concerns, as health data becomes a target for cyberattacks and misuse. The legal framework for data protection is crucial, with the Data Protection Act, 2019, playing a key role in safeguarding individuals' privacy rights.While existing laws and policies in the health sector address data protection, they are sometimes inconsistent with the Data Protection Act. Amendments are needed for full compliance. Healthcare providers must therefore show compliance, ensuring lawful data processing, accuracy, and protection against unauthorized access.

NEWTON AMANI

DATA PROTECTION EXPERT

The note extends to digital health platforms, emphasizing rigorous data protection standards. It includes tailored sections for different healthcare institutions, addressing specific challenges and issues. The guidance covers principles like lawful basis, fair processing, data retention, security, automated decision-making, profiling, and biometric data use. Checklists are provided to help institutions understand and comply with legal requirements, including guidance on creating privacy notices. Regular compliance audits are recommended for tailored guidance and recommendations.

Legislative Framework and Data Protection Principles

The legal framework for data protection in Kenya's health sector aims to safeguard personal data by ensuring lawful, fair, and transparent processing, storage, and sharing. The existing laws and policies regulating health information predate the Data Protection Act (DPA) but incorporate data protection principles. Key legislative components include:

Constitution of Kenya 2010: Recognizes the right to privacy, prohibiting unnecessary disclosure of a citizen's personal information related to family or private affairs.

Data Protection Act, 2019: Defines "Health data" as information concerning the physical or mental health of the data subject, encompassing past, present, or future health states. Health data is classified as sensitive personal data under the Act, requiring additional safeguards for protection.

Section 26: Grants individuals the right to access their health data, request corrections for inaccuracies, and, in certain circumstances, demand the deletion of their health data.

The guidance places emphasis on the importance of adhering to data protection principles, including:

Lawfulness, fairness, transparency

This 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.

Purpose Limitation

The purpose limitation principle in the health sector asserts that personal data must only be collected and processed for specific and legal purposes and should not be utilized for any other purposes inconsistent with the identified legal basis.

Data Minimization

The data minimization principle emphasizes limiting the collection, use, and retention of personal data to what is strictly necessary for a specific purpose. The Kenya National eHealth policy dictates that healthcare providers should only process personal data to the extent required to achieve medical care objectives.

Accuracy

The accuracy principle mandates that personal data should be precise, up-to-date, and complete. All stakeholders, including healthcare providers, researchers, and health insurance companies, must take reasonable steps to ensure data accuracy and promptly correct any inaccuracies.

Storage Limitation

The Data Protection Act does not prescribe specific retention times, placing the responsibility on entities in the health sector to justify and not retain personal data on a 'just-in-case' basis. However, for cases where health data is to be retained indefinitely, regulations should outline realistic time frames for pseudonymization and anonymization. Entities must make informed decisions on how long patient file data should be retained after treatment or a patient's passing, with justifications and avoiding indefinite retention.

Storage Limitation

Key aspects of confidentiality and data security include:

a) **Confidentiality:** Healthcare providers must maintain the confidentiality of personal health information, ensuring authorized access and not disclosing information without patient consent, except under legal requirements such as a court order.

b) **Data security:** Healthcare providers must securely store and transmit personal health information, implementing technical and organizational measures to prevent unauthorized access, disclosure, alteration, or destruction of data.

c) **Training and awareness:** Healthcare providers and staff should be trained and aware of their responsibilities in safeguarding personal health information, understanding legal and ethical obligations, as well as the risks and consequences of unauthorized disclosure or data breaches.

d) **Risk assessment:** Regular risk assessments should be conducted by healthcare providers to identify vulnerabilities in systems and processes, allowing the implementation of appropriate safeguards to mitigate potential risks.

Accountability

Emphasis on the need for healthcare institutions to ensure that personal health data is processed in a fair, transparent, and secure manner, with strict adherence to these principles.

Lawful Basis of Processing

The guidance note further emphasizes the importance of having a valid lawful basis for processing personal data in the health sector, irrespective of the purpose. Various lawful bases are outlined, with the most appropriate one dependent on the specific processing purpose and the relationship with the individual. The chosen lawful basis must be determined and documented before processing, and only one legal basis should be relied upon for each processing activity.

Key lawful bases

a) **Consent:** Clear, informed, specific, and unambiguous consent from the data subject is required for processing personal data. Healthcare organizations must obtain explicit consent from its customers to process their personal data for processing. The consent form clearly outlines the purposes of data processing, and individuals have the option to opt-in or opt-out. Consent must be freely given, and entities in the health sector must maintain verifiable records, especially for treatment. Distinctions are made between medical consent and consent under data protection laws.

b) **Performance of a contract:** Personal data may be processed if necessary for the performance of a contract, covering both existing and potential contractual relationships in the health sector. An example to illustrate this is when a hospital processes patient data, including medical history and insurance information, to facilitate the provision of medical services. This processing is necessary for the performance of the contract between the patient and the healthcare provider.
c) **Compliance with legal obligation:** Processing personal data is lawful if necessary for compliance with a legal obligation to which the data controller is subject.
d) **Protection of vital interests:** Processing is lawful if necessary to protect the vital interests of the data subject, especially in medical emergency situations.
e) **Legitimate Interests:** Personal data may be processed if necessary for legitimate interests pursued by the health care provider, ensuring that such interests do not override the rights and freedoms of the data subject.
f) **Public Interest:** Processing is lawful if necessary for tasks carried out in the public interest or the exercise of official authority, with a requirement to respect individuals' rights and freedoms. An illustration of this is when a government agency processes personal data to carry out public health initiatives, such as tracking and controlling the spread of infectious diseases. The processing is in the public interest for the greater good of the community.

Personal data may be processed for historical, statistical, journalistic, literature, art, or scientific research purposes, with examples such as scientific research and statistical research in monitoring disease trends.
The guidance underscores the need for careful assessment by health service providers to determine the appropriate lawful basis for specific processing activities, ensuring compliance with relevant legal requirements.

Rights of Data Subjects

The guidance delineates the rights accorded to data subjects, particularly patients, in the context of personal health information processing. The Data Protection Act serves as the legal framework, aiming to empower citizens amidst the prevalence of technology companies and data processors. Upholding these rights is crucial, fostering trust in healthcare institutions, especially in the realm of public health activities. Healthcare providers are obligated to establish accessible avenues for data subjects to exercise their rights.

Rights of Data Subjects include:

1.Right to be Informed: Data subjects have the right to be informed about the collection and use of their personal data, including details on data collection, purpose, duration, complaints procedure, and data sharing.

2.Right to Access Personal Data: Data subjects are entitled to access their personal data held by healthcare providers, including information on data type, data controller details, recipients, and retention periods. Healthcare sectors must verify requests, maintain tracking mechanisms, and provide requested information to the data subject.

3.Right to Rectification of Personal Data: Individuals can request corrections to inaccurate or incomplete health information. Healthcare providers must establish processes to verify requests, correct data, and inform both the data subject and third parties of corrections.

4.Right to Object to Data Processing: Data subjects can object to the processing of their personal health data for various reasons, such as marketing, research, third-party access, or concerns about data accuracy. However, this right is not absolute and may be limited in certain circumstances.

5.Right Not to be Subjected to Automated Decision Making: Individuals can object to automated processing of their data, demanding human intervention in decision-making processes.

6.Right to Erasure (Right to be Forgotten): Individuals have the right to request the deletion or removal of their personal data by healthcare providers.

7.Right to Data Portability: This right enables individuals to receive a copy of their personal data in a structured, machine-readable format and transmit it to another data controller without hindrance. In the healthcare context, it is significant for those switching healthcare providers or transferring personal data to new healthcare systems.

Compliance Obligations of the Health Sector

Entities within the healthcare sector are mandated to undergo compulsory registration, guided by the Office of the Data Protection Commissioner (ODPC). Data protection by design emphasizes the integration of privacy and security measures into the design of products, services, and systems from the outset, particularly crucial in the health sector dealing with sensitive personal health information.

Entities must adhere to section 41 of the Data Protection Act, implementing technical and organizational measures, ensuring only necessary personal data is processed.

Entities must establish personal data retention schedules, specifying retention purpose, duration, and audit provisions. Regular reviews and updates are essential to ensure relevancy and effectiveness. A DPIA is mandatory when data processing poses a high risk to data subjects' rights and freedoms. It is recommended as a valuable tool even in unclear cases.
Data controllers must report breaches to the ODPC within 72 hours and communicate breaches to affected data subjects unless the identity cannot be established.
Health sector entities engaging data processors must ensure compliance with relevant laws and regulations. Contracts (Data Protection Agreements) must stipulate that processors act only on the controller's instructions and are bound by obligations. Security measures must be upheld. Data sharing is governed by various laws and policies. Sharing must adhere to principles of confidentiality, privacy, and informed consent. Data localization in the health sector mandates that personal data be stored and processed within Kenya's borders, unless explicit consent or an adequate level of protection in the receiving country exists.
Transparency is fundamental, and data controllers and processors must notify data subjects of their rights, purpose of data collection, third-party recipients, safeguards, and consequences of non-provision of data. Privacy policies should be clear, accessible, and regularly updated.

To enhance comprehensibility, entities can use visual aids, implement a question-and-answer structure, and provide practical examples to aid data subjects in understanding privacy policies. Regular reviews ensure alignment with changing data processing practices and relevant laws and regulations.In conclusion, the guidance note serves as a vital tool for healthcare institutions in Kenya, providing clear and practical guidance on data protection in the health sector.

THE END