2026 JULY | DATA PROTECTION

EMERGING DATA PROTECTION OBLIGATIONS FOR HEALTHCARE PROVIDERS IN KENYA

Healthcare providers routinely collect, use, store and share significant volumes of personal data in the course of providing medical services. This may include ordinary personal data, such as names, contact details, identification information, billing details and images, as well as sensitive personal data relating to a patient's health or medical treatment.

Health data is classified as sensitive personal data under the Data Protection Act, 2019. Section 2 of the Act defines health data as data relating to the state of physical or mental health of a data subject, including records concerning the past, present or future state of a person's health, data collected in the course of registration for, or provision of, health services, and data which associates the data subject with the provision of specific health services.

Accordingly, healthcare providers must process all personal data in accordance with the principles of data protection, on the basis of an appropriate lawful basis, and subject to appropriate technical and organisational measures. Where the data constitutes sensitive personal data, including health data, providers must also comply with the additional requirements for processing sensitive personal data set out in Part V of the Act.

This article explores the emerging obligations of healthcare providers when processing both personal data and sensitive personal data, including obligations relating to accuracy, lawful basis, transparency, purpose limitation, data governance, data subject rights and consent.

1. **Healthcare providers must ensure the accuracy of personal and health data shared with patients**

   Case background. In Esther Gitau v Shree Swaminarayan Hospital, the Complainant alleged that, following a medical consultation and laboratory testing, she received laboratory results belonging to an unknown patient. The disclosure involved health data, which is classified as sensitive personal data under the Data Protection Act, 2019.

   Commissioner's finding. The Data Commissioner held that the Respondent had failed to ensure the accuracy of the personal data processed and shared with the Complainant. This failure amounted to a breach of sections 25(a) and 25(f) of the Act, read together with section 44, which require personal data to be processed lawfully and kept accurate, particularly where sensitive personal data is involved.

   Outcome. Although no compensation was awarded, the Data Commissioner issued an Enforcement Notice against the hospital for non-compliance with the Data Protection Act.

2. **Healthcare providers must have an appropriate lawful basis before sharing health data with third parties**

   Case background. In Merceline Akoth Odeyo v St. Luke Orthopaedic Trauma

Hospital, the Complainant received medical test results belonging to another patient on two separate occasions. The other patient had a similar first name but a different surname. The Complainant alleged that the Respondent indicated that it would contact the third-party laboratory that had conducted the tests for clarification. She further maintained that she had not been informed that her sensitive personal data, including health data, would be shared with the laboratory and that she had not consented to such disclosure.

Respondent's position. The Respondent stated that the Complainant visited the health facility on 3 July 2025, where samples were collected for testing. According to the Respondent, the Complainant was informed that the testing services had been outsourced to a third-party laboratory and was asked to collect the results after two weeks. The Respondent asserted that the Complainant had given verbal consent for the processing of her data and also sought to rely on legitimate interests as a lawful basis for processing. It attributed the incorrect results to an administrative error in the processing of her data.

Commissioner's finding. The Data Commissioner held that section 45 of the Data Protection Act sets out the permitted grounds for processing sensitive personal data, and that legitimate interests is not one of those grounds. Since the Respondent relied on consent as the lawful basis for processing the Complainant's data and transferring it to a third party, it bore the burden of proving that valid consent had been obtained. The Respondent's failure to provide any written record of consent meant that it could not demonstrate that the alleged verbal consent met the legal standard of explicit and informed consent.

Outcome. The Data Commissioner found the Respondent liable for failing to prove that it had obtained the Complainant's express consent before sharing her sensitive personal data with the third-party laboratory. The Respondent was directed to compensate the Complainant in the amount of KES 525,000.

3. **Healthcare providers must not repurpose personal data for marketing without consent**

Case background. In Erickson Kipkirui Langat v AGC Tenwek Hospital, the Complainant alleged that the Respondent had repurposed his telephone number beyond the purpose for which it was originally collected. The Complainant had provided his telephone number for hospital registration and payment of bills. The Respondent subsequently used the same number to send unsolicited marketing messages.

Respondent's position. The Respondent did not submit a response to the complaint.

Commissioner's finding. The Data Commissioner held that, under section 25 of the Data Protection Act, personal data must be collected for explicit, specified and legitimate purposes, and must not be further processed in a manner that is incompatible with those purposes. By using the Complainant's telephone number, which had been collected for registration and billing purposes, to send marketing communications, the Respondent processed the data for a purpose that was incompatible with the original purpose of collection. The Commissioner further held that the Respondent should have obtained the Complainant's consent before using his telephone number for marketing, in line with sections 30, 32, and 37(1) of the Act.

Outcome. The Data Commissioner found the Respondent liable for processing the

Complainant's personal data beyond the original purpose for which it had been collected and directed the Respondent to compensate the Complainant in the amount of KES 250,000.

4. **Healthcare providers may be subject to independent investigations for systemic data protection failures**

Case background. In the Matter of Eldoret Hospital, the Data Commissioner commenced investigations on her own initiative following public interest concerns regarding the hospital's personal data processing practices. The concerns related to the alleged misuse of personal data, violation of data subject rights, unlawful data transfers and inappropriate processing of personal data.

Commissioner's findings. The investigation revealed several areas of non-compliance in the Respondent's processing operations, including:

i) failure to identify appropriate lawful bases for processing personal data, contrary to sections 25(b) and 30 of the Act;

ii) failure to notify data subjects of the purposes for which their data would be used, contrary to sections 25(b) and 29 of the Act;

iii) failure to implement adequate security measures, contrary to sections 41 and 42 of the Act and Regulation 32 of the Data Protection (General) Regulations, 2021;

iv) violation of the principle of data minimization, contrary to section 25(d) of the Act and Regulation 33 of the Data Protection (General) Regulations, 2021; and

v) violation of the storage limitation principle, contrary to section 25(g) of the Act.

vi) In addition, it was established that:

- The Respondent lacked a functional data governance framework.
- The Respondent had not registered with the Office of the Data Protection Commissioner as a data controller or data processor, despite collecting and processing personal data from the public.
- The Respondent had not conducted a data protection impact assessment, despite processing large volumes of personal data.
- The Respondent did not have a data protection policy for its processing activities.
- The Respondent had not conducted data protection training for its staff.
- The Respondent did not have a functional data breach incident response plan.
- The Respondent did not have a data retention policy.
- The Respondent had no mechanism for handling data subject access requests.
- The Respondent had no mechanism for handling data subject rectification requests and was sharing personal data with third parties without data sharing agreements.
- The Respondent had not implemented data protection by design and by default.
- The Respondent failed to apply the principle of data

minimisation by collecting excessive patient data without a justifiable purpose.

- Data subjects were not adequately informed of how their data would be used.
- The measures in place were insufficient for handling the large volumes of personal data and sensitive personal data processed by the Respondent.

Respondent's position. The Respondent did not respond to the queries raised by the Data Commissioner.

Outcome. The Data Commissioner consequently issued an Enforcement Notice against the Respondent.

5. **Healthcare providers must obtain consent before using a person's image for promotional or commercial purposes**

Case background. In Allan Tirop v Port Florence Community Hospital, the Complainant alleged that the Respondent used his image on its social media pages without his consent. The Respondent had posted the Complainant's image on its Meta pages alongside a caption promoting its *medical and diagnostic services* in Siaya, including *ultrasound* and X-ray *services*.

Commissioner's finding. The Data Commissioner found that the image had been published in a manner that suggested the Complainant was an employee of the Respondent and was offering professional services as a radiographer in its radiology department. In fact, the Complainant was not an employee of the Respondent and had not consented to the use of his image. The Commissioner held the Respondent liable for using the Complainant's image for commercial gain without consent and for failing to remove the image after the Complainant requested its removal.

Outcome. The Respondent was directed to compensate the Complainant in the amount of KES 750,000.

Conclusion

The determinations discussed above demonstrate that healthcare providers must approach the processing of personal data and sensitive personal data as a core compliance obligation, not a peripheral administrative function. Given the nature and volume of information handled in the healthcare sector, providers must ensure that personal data is accurate, processed for clear and lawful purposes, disclosed only on an appropriate lawful basis and protected through adequate technical and organisational measures.

They also underscore the need for strong data governance frameworks, including clear privacy notices, documented consent where required, data protection policies, staff training, data retention controls, breach response procedures, mechanisms for handling data subject requests and appropriate agreements with third parties who receive or process patient data.

Ultimately, compliance requires healthcare providers to embed data protection into their day-to-day operations. This is particularly important where health data is involved, as failures in processing can expose data subjects to significant privacy risks and expose providers to regulatory enforcement, compensation awards and reputational harm.

Key Contacts

Anne Muema
Advocate / Managing Partner

Email: amutheu@mutieadvocates.com

Maureen Kubai
Associate

Email: mkubai@mutieadvocates.com

About Mutie Advocates

Mutie Advocates is a Nairobi-based law firm with a strong focus on legal compliance, data protection and privacy law, complemented by a broad range of legal services. Built on a foundation of legal excellence, the firm provides expert support in corporate and commercial law, employment and labour relations, intellectual property, litigation, dispute resolution and regulatory compliance. Known for its practical and client-centered approach, Mutie Advocates helps organizations navigate complex legal and regulatory landscapes through data audits, policy development and strategic legal advisory. The firm serves a diverse clientele, including individuals, corporates, non-governmental organizations and public institutions, delivering timely, effective and solution- oriented legal services.

Website: www.mutie-advocate.com
Phone: +254 768 042 180
E-mail: info@mutieadvocates.com
Address: Assi Centre, School Lane, Westlands
P O Box 211-00621, Nairobi

Disclaimer:

The views expressed in this article are for general guidance and should not be interpreted as legal advice. Mutie Advocates shall not be held liable for any reliance placed on this information without formal legal consultation. Always seek professional advice tailored to your situation.