



OFFICE OF THE DATA PROTECTION COMMISSIONER

ODPC COMPLAINT NO. 2125 OF 2025

MERCELINE AKOTH ODEYO.....COMPLAINANT

-VERSUS-

ST. LUKE ORTHOPAEDIC &
TRAUMA HOSPITAL ELDORET.....RESPONDENT

DETERMINATION

(Pursuant to Section 8 (1) (f) and 56 of the Data Protection Act, 2019 and Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021)

A. INTRODUCTION

1. The Complainant alleges that the Respondent mishandled her sensitive personal data by failing to maintain its accuracy and currency and by disclosing medical records of an unrelated individual as though they were hers.

B. LEGAL BASIS

2. Article 31 (c) and (d) of the Constitution of Kenya provides for the right to privacy. Consequently, as an effort to further guarantee the same, the Data Protection Act, 2019 (hereinafter known as 'the Act') was enacted.
3. The Office of the Data Protection Commissioner (hereinafter 'this Office' and/or 'the Office') was established pursuant to Section 5 of the Act and is mandated with the responsibility of regulating the processing of personal data; ensuring that the processing of personal data of a data subject is guided by the principles set out in Section 25 of the Act; protecting the privacy of individuals; establishing the legal and institutional mechanism to protect personal data and providing data subjects with

rights and remedies to protect their personal data from processing that is not in accordance with the Act.

4. Section 8 (1) (f) of the Act provides that the Office can receive and investigate any complaint by any person on infringements of the rights under the Act. Furthermore, Section 56 (1) of the Act provides that a data subject who is aggrieved by a decision of any person under the Act may lodge a complaint with the Data Commissioner in accordance with the Act.
5. This determination is premised on the provisions of Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 (the Enforcement Regulations) which states that the Data Commissioner shall, upon the conclusion of the investigations, make a determination based on the findings of the investigations.

C. BACKGROUND OF THE COMPLAINT

6. This Office received a complaint from the Complainant on 16th December, 2025. The complaint was lodged pursuant to Section 56 of the Act and Regulation 4 of the Enforcement Regulations from the Complainant who was the aggrieved data subject.
7. Pursuant to Regulation 11 of the Enforcement Regulations, the Office, notified the Respondent of the complaint filed against it *vide* a letter dated 15th January 2026 and referenced ODPC/CIE/CON/2/1(1035). In the notification of the complaint, the Respondent was informed that if the Complainant's allegations were true, they would be in violation of various sections of the Act. Additionally, the Respondent was asked to provide this Office with the following:
 - a) A response to the allegations made by the Complainant and a contact person who can provide further details to the complaint;
 - b) Any relevant materials or evidence in support of the statement of response.
 - c) Details of the lawful basis relied upon for processing of the Complainant's personal data.
 - d) Description of how data subjects exercise their data protection rights in accordance with its data protection governance framework

- e) Mitigation measures adopted or being adopted to address the complaint to the satisfaction of the Complainant and ensure the same does not recur.
- f) Any other relevant information.

8. This determination is therefore pursuant to the provisions of Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021.

D. NATURE OF COMPLAINT

9. The Complainant alleges that Respondent mishandled her sensitive personal data by failing to maintain its accuracy and currency, and by disclosing medical records of an unrelated individual as though they were hers.

E. SUMMARY OF RELEVANT FACTS AND EVIDENCE ADDUCED

i. THE COMPLAINANTS' CASE

- 10. The Complainant alleges that on several occasions, the Complainant sought the services of the Respondent, and on two separate visits, she was issued medical results belonging to a third party who shared a similar first name but a different surname.
- 11. The Complainant states that the Respondent disclosed to her that it would contact the third-party lab conducting the test for clarification. She avers that she had not been informed of this transfer.
- 12. The Complainant alleges that the Respondent collected sensitive personal and health information during the course of service provision and that that information should not have been disclosed to a third-party laboratory without obtaining her informed consent.
- 13. She contends that the Respondent's unlawful transfer and misplacement of her sensitive medical data caused her severe harm, including loss of privacy and dignity through unauthorized disclosure of intimate health information.

ii. THE RESPONDENT'S RESPONSE

14. The Respondent submitted a response to the Notification of Complaint letter on 3rd February, 2026.
15. The Respondent confirms that the Complainant visited the health facility on 3rd July, 2025 where samples were collected for testing. That the Complainant was informed that the services were outsourced to a third-party laboratory and was asked to collect the test results after 2 weeks.
16. They maintain that her medical samples were taken to the third-party laboratory who received it and attached a unique sample identification, barcode, to it. Once the tests were completed, the results were shared in a report to its laboratory's official email to the hospital.
17. The Respondent states that it did not share any sensitive data (personal or health) with the referral laboratory. The hospital safeguarded the patients personal and health data by minimizing the data shared with referral lab, and only shared the Complainant's name for purposes of identifying the sample.
18. The Respondent further confirmed that to ensure the confidentiality and security of the data shared including the sample that was taken, the sample was delivered to the referral laboratory by a laboratory technologist from the hospital.
19. The Respondent contends that an administrative error in the processing of the results received from its referral laboratory was identified and that this was an isolated case of human error during data reconciliation.
20. The Respondent states that the transfer of the sample was conducted for the sole purpose of providing medical services requested by the Complainant, which it maintains was necessary in order to protect the legitimate interest of the Complainant as provided under Section 30 of the Data Protection Act. They later tried to contact the Complainant to collect her results to no avail.

F. ISSUES FOR DETERMINATION

21. In light of the above, the complaint, the Respondent's responses and evidence adduced together with the investigations conducted, the following issues fall for determination by this Office.

- i) Whether the Respondent unlawfully disclosed the Complainant's personal data
- ii) Whether the Complainant is entitled to Remedies under the Act

I. WHETHER THE RESPONDENT UNLAWFULLY DISCLOSED THE COMPLAINANT'S PERSONAL DATA

22. Section 25 of the Act provides that every data controller or data processor shall ensure –

- (a) processed in accordance with the right to privacy of the data subject;*
- (b) processed lawfully, fairly and in a transparent manner in relation to any data subject;*
- (c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;*
- (d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;*
- (e) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;*
- (f) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected;*

23. Section 30 (1) (a) of the Act provides that a data controller or data processor shall not process personal data unless the data subject consents to the processing for one or more specified purposes.

24. The Act goes further to state the conditions of consent. It states as follows concerning the conditions of consent: -

32. Conditions of consent

(1) A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose.

(2) Unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time.

(3) the withdrawal of consent under sub-section(2) shall not affect the lawfulness of processing based on prior consent before its withdrawal.

(4) In determining whether consent was freely given, account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is conditional on the consent of the processing of personal data that is not necessary for the performance of that contract. (emphasis ours)

25. The Respondent states in its statement of response of their response that the Complainant was informed of the outsourcing of the testing service and gave verbal consent for the same. Additionally, it relies on legitimate interest as the lawful basis for such processing.

26. The Complainant strongly deny this and states that she was neither informed nor did she consent to her data being transferred to a third-parties without her knowledge.

27. Section 45 of the Act sets out the permitted grounds for processing of sensitive data. Legitimate interest of the Respondent does not fall within the grounds set out therein. The Respondent also relied on consent as the lawful basis of processing the Complainant's data and transferring the same to third parties.

28. It is trite that when processing personal data, the burden of proof rests with the data handler. The Respondent's failure to provide any record of written consent, means it cannot demonstrate that the alleged verbal consent meets the legal standard of explicit and informed consent. The Respondent has failed to discharge this burden.

29. The Respondent also states that it protected the Complainant's privacy by practicing data minimization, sharing only her name with the referral lab.

30. The principle of transparency under Section 25 of the Act is a fundamental data protection principle. A data subject has the right to know who is processing their highly sensitive health data. It is evident that the Respondent failed to submit evidence that the Complainant was duly notified as per Section 29 of the Act prior to sharing her sensitive personal data with any third party.
31. In its statement of response, the Respondent admits there was an administrative error in the processing of the test results an isolated case of human error during data reconciliation and provides a detailed Incident Report.
32. This however, confirms a failure to maintain the integrity and accuracy of the Complainant's sensitive health data. This demonstrates that the technical and organizational measures required under Section 41 of the Act to secure personal data were inadequate. This constitutes a clear breach of security.
33. Additionally, the existence of a Data Sharing Agreement does not negate the requirement to inform the data subject and obtain their explicit consent to share their sensitive personal data with that specific third party. The General Consent form developed after the incident is evidence that its previous consent mechanism was insufficient.
34. Based on the foregoing, the Office finds -
- i) That the Respondent unlawfully disclosed the Complainant's sensitive health data to a third party without obtaining her explicit and informed consent.
 - ii) That there is a violation of the principle of transparency under Section 25 of the Act and the Complainant's right to be informed under Section 29
 - iii) That the admission of an administrative error demonstrates a failure to implement adequate technical and organizational measures to secure the Complainant's personal data, violating Section 41 of the Act.

II. WHETHER THE COMPLAINANT IS ENTITLED TO REMEDIES UNDER THE ACT

35. According to Regulation 14 (2) of the Enforcement Regulations, a determination shall state the remedy to which the Complainant is entitled. Further, the remedies are provided for in Regulation 14 (3) of the Enforcement Regulations.
36. In consideration of the complaint, and having found that the Respondent disclosed the Complainant's sensitive personal data without the requisite consent as stipulated under the Act, it therefore follows that there has been a violation of the Act by the Respondent to that extent.
37. Section 65 (1) of the Act provides for compensation to a data subject and states that a person who suffers damage by reason of a contravention of a requirement of the Act is entitled to compensation for that damage from the data controller. Section 65 (4) of the Act states that "damage" includes financial loss and damage not involving financial loss, including distress.
38. Regulation 14 (3) (e) of the Enforcement Regulations further provides that the Data Commissioner may make an order for compensation to the data subject by the Respondent.
39. Having found that the Respondent has failed to prove that it obtained express consent from the Complainant, the Respondent is hereby directed to compensate the Complainant the amount of **Kes 525,000/= (Kenya Shillings Five Hundred and Twenty-Five Thousand Only)**.
40. In so doing, this Office takes into account the nature and extent of violation, the nature of personal data as regards unlawful processing of the Complainant's sensitive personal data and the attendant harm of processing such personal data.

I. FINAL DETERMINATION

41. In the ultimate, the Data Commissioner makes the following final determination;
- i. The Respondent is hereby found liable

- ii. The Respondent is ordered to compensate the Complainant **Kenya Shillings Five Hundred and Twenty-Five Thousand Only (KES 525,000.)**
- iii. Parties have the right to appeal this determination to the High Court of Kenya within thirty (30) days.

DATED at **NAIROBI** this 16th day of March 2026



**IMMACULATE KASSAIT SC, MBS
DATA COMMISSIONER**

