REPUBLIC OF KENYA

**OFFICE OF THE DATA PROTECTION COMMISSIONER**

**ODPC COMPLAINT NO. 1085 OF 2023**

**GRACE GATAMBU..... COMPLAINANT**

**-VERSUS-**

**AAR HEALTHCARE KENYA LIMITED.....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 Constitution of Kenya 2010, under Article 31 recognizes the right to privacy. Consequently, in an effort to further guarantee the same, the Data Protection Act, 2019 (hereinafter as "the Act") was enacted.

2. The Office of the Data Protection Commissioner (Hereafter '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.

3. 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.

4. It is on that basis that the Office received a complaint on 24th June, 2023, pursuant to Section 56 of the Act, from Grace Gatambu (hereinafter "the Complainant"), who was an aggrieved data subject.

5. AAR Healthcare Kenya Limited (hereinafter as "the Respondent) operates as a medical service provider while the Complainant was a patient at the Respondent's Roysambu clinic on 21st December, 2021.

6. The Office in the exercise of its mandate as envisaged under the Act and in the promotion of justice, notified the Respondent of the complaint filed against it *via* a letter dated 17th July, 2023, which was served upon the Respondent on 18th July, 2023. In the notification of the complaint filed against the Respondent, the Respondent was to provide: -

   (a) A response to the allegations made against it by the Complainant;

   (b) Any relevant materials or evidence in support of its representations above;

   (c) The mitigation measures adopted or being adopted to address the complaint to the satisfaction of the Complainant;

   (d) The legal basis relied upon to store, process and engage with the Complainant's personal data and whether or how it fulfils the duty to notify under Section 29 of the Act;

   (e) Details of how it fulfils the data subject's right of rectification and erasure as per Section 40 of the Act;

   (f) The technical and organizational safeguards that have been put in place to ensure that such occurrences mentioned in the complaint do not occur again;

(g) It's data protection policy outlining the complaints handling mechanism to deal with matters relating to the rights of a data subject under the Act, the Regulations and any alleged contravention directed to its attention by data subjects;

(h) Proof of registration with the Office as data controllers and data processors; and

(i) Demonstration (by way of written statement) of its level of compliance with the requirements under the Act and the Regulations. In particular, an elaborate representation of how a data subject can exercise their rights in relation to data protection.

7. On 2nd August, 2023, the Office sent a reminder to the Respondent through a letter reference number ODPC/CONF/1/5 VOL 1(370), advising it to respond to the Notification of Complaint letter dated 17th July 2023 within the next seven days.

8. On 16th August, 2023, the Respondent filed its response to the complaint *via* a letter of the same date.

9. This determination is premised on the provisions of Regulation 14 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 which states that the Data Commissioner shall, upon conclusion of the investigations, make a determination based on the findings of the investigations.

## B. NATURE OF THE COMPLAINT

10. The complaint relates to the alleged release of the Complainant's confidential medical information contained in a medical form to a third party without her consent. The medical information pertained to the treatment of the Complainant when she visited the Respondent's clinic located at Roysambu on 24th December, 2021. The information was then used to market insurance products to the Complainant.

11. The Complainant stated that on January 2022, she was contacted by an insurance agent who wanted to sell insurance products to her. She probed the insurance agent on how she got her contacts and it was revealed to her that her contacts were obtained from her medical form which the Respondent accidentally shared with the insurance agent. The insurance agent revealed that she was expecting her client's results from the Respondent but the Complainant's records were shared instead.

12. The Complainant averred that the Respondent gave a verbal apology but due to the seriousness of the matter, she demanded a written acknowledgement and an apology along with an assurance that such a breach wouldn't happen again to her or anyone else. The same was not forthcoming from the Respondent and that necessitated the filing of a complaint at this Office.

## C. ANALYSIS OF EVIDENCE ADDUCED

### I. EVIDENCE ADDUCED BY THE COMPLAINANT

13. The Complainant filled the complaint's form and provided the following documents;
    a) A copy of the subject medical claim form from her insurer Madison Insurance Company.
    b) Email correspondences between her and the aforesaid insurance agent.
    c) Email correspondences between her and the Respondent.

14. The medical claim form contained the Complainant's sensitive personal data such as her medical diagnosis which revealed her illness/medical condition. Additionally, the form also contained various personal data of the Complainant, including her name, date of birth, mobile phone number, name of employer and her signature.

15. The forwarded email exchange between the Complainant and the insurance agent contained the subject medical claim form as an attachment signifying that the insurance agent had received the form from the Respondent.

16. The email correspondences between the Complainant and the Respondent contained the complaint made by the Complainant to the Respondent over the

alleged sharing of her medical records with third parties, the Respondent's response and further follow up messages regarding the complaint including scheduled meetings between the Complainant and the Respondent.

## II. EVIDENCE ADDUCED BY THE RESPONDENT

17. The Respondent *via* a letter dated 16th August, 2023 responded to the notification of complaint letter.

18. In the said letter, the Respondent confirmed that the Complainant visited its clinic on 21st December, 2021 and was attended to by its medical staff. It indicated that the Complainant duly filled and executed a Medical Insurance form for Madison General Insurance Kenya Limited and was aware that the Respondent would use the form to claim payments.

19. The Respondent stated that it later received a complaint indicating that the medical form was posted to the wrong insurance being ICEA Insurance on 24th December 2021 and the recipient (ICEA Insurance) contacted the Complainant seeking to sell her a medical insurance policy.

20. The Respondent admitted to the occurrence of the aforementioned breach of the health data of the Complainant and stated that the said staff who shared it was deeply remorseful and highly regretted the incident. Further, the said staff admitted that she only became aware when she got a call from the Complainant and later confirmed that she mistakenly sent the form to ICEA Insurance.

21. The Respondent stated that it took this matter as a single isolated incident and contacted the Complainant to offer an apology and explain the unfortunate incident. Additionally, the Respondent offered a verbal apology but withheld putting the same in writing out of abundance of caution.

22. Further, the Respondent stated that it found the actions of the recipient of the email rather malicious and intentionally meant to disparage the name and conduct

of its institution and that it has attached a disclaimer in all its emails as part of its technological and organizational safeguards.

23. Finally, the Respondent stated that it continues to educate its staff on the Data Protection Policy recently approved for adoption by the company that is aligned with the Data Protection Act of Kenya.

## D. ISSUES FOR DETERMINATION

24. Having considered the nature of the complaint and the evidence adduced it is not in dispute that the Respondent shared the Complainant's medical information with a third party.

25. The issues that then fall for determination are whether the Respondent, by such disclosure: -

    i) Applied the Principles of Data Protection in processing of the Complainant's personal data

    ii) Violated the Complainant's rights as a data subject.

### I. WHETHER THE RESPONDENT APPLIED THE PRINCIPLES OF DATA PROTECTION IN PROCESSING OF THE COMPLAINANT'S PERSONAL DATA.

26. The Office notes that the complaint relates to the sharing of the Complainant's confidential medical information contained in a medical form to a third party without the Complainant's consent. The sensitive personal data released was then used by the third party to market insurance products to the Complainant.

27. 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 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.*

28. The Act further defines **sensitive personal data** as *data revealing a 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."*

29. **Section 44 of the Act** provides that no category of sensitive personal data shall be processed unless Section 25 of the Act applies to that processing.

30. The principles of data protection are laid out in **Section 25** of the Act which states that, "*Every data controller or data processor shall ensure that personal data is:*

*(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) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;*

*(f) 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;*

*(g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and*

*(h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject."*

31. The Complainant visited the Respondent's Roysambu clinic and provided her personal data for the purposes of being treated and for processing of her medical insurance claim. She did not consent to the sharing of her personal data with a third party. The further processing of her personal data by the Respondent, by

sharing the Complainant's personal data with a third party, was unlawful and goes against the principle of lawfulness and fairness.

32. The purpose limitation principle means that personal data should only be processed for specific purposes and should not be used for any other purpose inconsistent with the identified purpose. The Complainant provided her personal data for the purpose of medical treatment and also for processing of her insurance medical claim. The Respondent, by sharing the Complainant's personal data with a third party who in turn used the data to market insurance products to the Complainant violated the principle of purpose limitation. The Complainant's personal data was used for purposes other than those for which it was originally collected. It is worth noting that Regulation 15 (1) of the Data Protection (General Regulations), 2021 **prohibits the use of sensitive personal data for the purpose of direct marketing.**

33. Further, 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.

34. 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. The Respondent did not fulfill its duty to notify as provided for under Section 29 of the Act thereby violating the principle of fairness and transparency.

35. While the Respondent admits that the Complainant's personal data was mistakenly shared with an unauthorized third party, the Respondent did not report the alleged data breach to this Office within 72 hours of becoming aware of the breach in accordance with Section 43 of the Data Protection Act. By dint of Regulation 37(1)

& (3) of the Data Protection (General) Regulations, the same amounted to a notifiable breach under the Act.

36. In conclusion, this Office finds that the Respondent failed to implement data protection by design and by default as provided in Section 41 of the Act to ensure the principles of data protection are inculcated in their data processing activities. For instance, the Respondent could have conducted a data protection impact assessment in order to identify and mitigate potential privacy risks in the processing of personal data.

37. The upshot is that I find that the Respondent did not apply the principles of data protection when processing the Complainant's data.

## II. WHETHER THERE WAS ANY VIOLATION OF THE COMPLAINANT'S RIGHT AS A DATA SUBJECT

38. The Complainant's complaint is founded on Article 31 (c) of the Constitution of Kenya, 2010 which states that ***"every person has the right to privacy, which includes the right not to have information relating their family or private affairs unnecessarily required or revealed."***

39. From the above it is clear that the Complainant's right to privacy as provided for under **Article 31 (c) of the Constitution** was violated, by the disclosure of her medical records without her consent.

40. **Section 26** of the Act provides for **the rights of a data subject** and states that, *"a data subject has a right —*

*(a) to be informed of the use to which their personal data is to be put;*

*(b) to access their personal data in custody of data controller or data processor;*

*(c) to object to the processing of all or part of their personal data;*

*(d) to correction of false or misleading data; and*

*(e) to deletion of false or misleading data about them."*

41. The Respondent by not informing the Complainant of the use to which her personal data was to be put, at the point of collection of the personal data, violated her right to be informed. The Respondent collected the personal data of the Complainant, including sensitive personal data contained in a medical form, and did not inform her that her data was going to be shared with an insurance agent for the purposes of marketing insurance products to her. The data should not have been shared with a third party without the Complainant's consent and used to market insurance products to her without her prior consent.

42. The Respondent has a right to object to the processing of her personal data when the data is being or has been shared with third parties without her consent. The Respondent being the data controller in this case had a duty to inform the insurance agent being its data processor to stop further processing of the Complainant's personal data after the Complainant raised a complaint regarding the unauthorised disclosure and misuse of her personal data to market insurance products to her.

43. Moreover, processing of sensitive personal data for direct marketing purposes is prohibited by the Data Protection (General) Regulations, 2021 and the Respondent had a duty to inform the insurance agent to stop using the Complainant's data to market insurance products to her. This was not done thereby violating the Complainant's right to object to the processing of their personal data.

44. **Section 40 (2)** of the Act provides for the **right of erasure** and states that,

> *"Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to inform third parties processing such data, that the data subject has requested the erasure or destruction of such personal data that the data controller is no longer authorized to retain, irrelevant, excessive or obtained unlawfully."*

45. The Respondent having shared the Complainant's sensitive personal data with an insurance agent, without the consent of the Complainant, did not demonstrate that it took measures to inform the insurance agent, to erase the personal data of the Complainant. The Respondent only indicated in its response, that it has attached a disclaimer to all its emails that states,

> *"....If you are not the intended recipient(s), please note that any distribution, forwarding, copying or use of this communication or the information is strictly prohibited... if you have received it in error, please contact the sender immediately by return e-mail. Please then delete the e-mail and any copies of it and do not use or disclose its contents to any person..."*

46. No evidence of attachment of the disclaimer was adduced to this Office. The Office further notes that the email correspondences between the Complainant and the Respondent did not contain the aforementioned disclaimer. The Respondent by its action and inaction thus violated the Complainant's right of erasure.

47. From the foregoing, I find that the Respondent violated the Complainant's right to be informed, right to object to the processing of her personal data and her right of erasure.

**E. FINAL DETERMINATION**

1. The Data Commissioner therefore makes the following final determination;

    i. The Respondent is hereby found liable.
    ii. An Enforcement Notice to hereby be issued to the Respondent.
    iii. Parties have the right to appeal this determination to the High Court of Kenya.

**DATED** at **NAIROBI** this 21st day of September 2023.

**IMMACULATE KASSAIT, MBS**
**DATA COMMISSIONER**