‘AA’ and the Royal Australasian College of Surgeons (Privacy)

National Health Practitioner Privacy Commissioner

Decision and reasons for decision of the National Health Practitioner Privacy Commissioner, Richelle McCausland

Complainant	‘AA’
Respondent	Royal Australasian College of Surgeons
Reference number	NHPO/11782023
Decision date	17 September 2024
Catchwords	PRIVACY – Australian Privacy Principles – APP 12 – Access to personal information – Whether personal information was held – No breach – Privacy Act 1988 (Cth)

All references to legislation in this document are to the *Privacy Act 1988* (Cth) (Privacy Act) unless otherwise stated.

Determination

1. This is a determination of a privacy complaint made under s. 36(1) to the National Health Practitioner Privacy Commissioner (NHPPC) about the Royal Australasian College of Surgeons (the Respondent).
2. I find that the Respondent does not hold personal information about the Complainant in the Morbidity Audit and Logbook Tool (MALT database) and therefore does not have responsibilities with respect to the Complainant’s personal information under Australian Privacy Principle (APP) 12.
3. The Respondent has not interfered with the privacy of the Complainant. The complaint is dismissed pursuant to s. 52(1)(a).

Background

4. The Respondent is responsible for training surgeons in Australia and New Zealand. The Respondent’s MALT database is used by surgeons to electronically log procedures and to conduct self-audits and peer-review audits.
5. The Complainant made a complaint about the Respondent to the NHPPC on 27 July 2023. The Complainant raised concerns about the Respondent’s refusal to provide them with personal information stored on its MALT database.

6. The Complainant stated that:
    - when they underwent surgery at a hospital, many surgical trainees and other clinicians associated with the Respondent were present
    - surgical trainees and their supervisors must document their surgical training on the MALT database. The MALT database was created, and is owned and maintained, by the Respondent
    - on 6 March 2023 they wrote to the Respondent and requested all personal information held about them in the MALT database. In response, the Respondent advised them that:
        - it does not hold patient records or any of their personal information
        - it does not own the data entered by clinicians into the MALT database; the clinician who entered the data is the owner of the data
        - encryption of the MALT data prevents the Respondent's staff from accessing any identifiable data held in the MALT database.
    - they were dissatisfied with the response they received from the Respondent. They believe the MALT database holds their personal information. The policy on the Respondent's website states it will release information from the MALT database if it obtains consent from the relevant trainee or supervisor, which they consider indicates that the Respondent does have access to the information.
7. On 28 July 2023 the office of the NHPPC transferred the complaint to the Respondent for a further response. The Respondent's further response outlined that:
    - identifiable information can only be accessed and released by the clinicians who own the data and who entered the information into the MALT database
    - patient information is not readable by the Respondent's staff because it is encrypted. The Respondent does not know if the MALT database contains the Complainant's personal information as it does not have access to the identifiable information
    - the Respondent's policy covers the release of deidentified aggregated data for research purposes and does not relate to individual cases.
8. On 17 August 2023 the Complainant outlined their concerns regarding the Respondent's response, including that:
    - the Respondent failed to provide a reason for denying access to their personal information
    - the Respondent holds their personal information on the MALT database and it should be possible for the Respondent's employees to locate personal information by searching the database by patients' personal identifiers
    - the Respondent provided insufficient information about what steps it took to try to obtain the information they requested and why it is certain that none of their personal information is accessible to the Respondent's employees
    - the Respondent has explained that encryption prevents its staff from accessing data stored on the MALT database; however, encryption is only for the purposes of protecting data from outside sources and not from the Respondent's employees

- the Respondent did not supply a copy of its disclosure of personal information procedure or any internal policies and procedures that would provide further information about its encryption
- the Respondent did not provide a statement from an information technology expert confirming that the information they requested is not accessible
- the Respondent's policies indicate that employees and committee members have access to the information held in the MALT database.

9. Having formed the view that there was no reasonable likelihood that the complaint would be resolved by conciliation, an investigation into the complaint was commenced under s. 40(1) on 15 September 2023.

The Law

10. The NHPPC's power to consider privacy complaints comes from the Privacy Act as modified by the Health Practitioner Regulation National Law and the Health Practitioner Regulation National Law Regulation 2018 (as in effect in each state and territory of Australia).
11. The APPs in Schedule 1 of the Privacy Act regulate the collection, use, disclosure and security of personal information held by APP entities. An act or practice of an APP entity is an interference with the privacy of an individual if the act or practice breaches an APP.
12. APP 12 is relevant to this complaint, as it concerns an individual's right to access their personal information subject to certain exceptions.
13. Section 36 allows an individual to complain about an act or practice that may be an interference with their privacy.
14. Section 52 provides that, after investigating a complaint, the NHPPC may make a determination either dismissing the complaint, or finding the complaint substantiated and making one or more declarations.

Information considered

15. In making this determination I have had regard to information provided by the Complainant and the Respondent. This includes the Complainant's and the Respondent's comments on a 'proposed determination' provided to them on 28 June 2024.
16. I have also considered:
    - the Privacy Act
    - the APP Guidelines of the Office of the Australian Information Commissioner
    - guidance from the Office of the Victorian Information Commissioner (OVIC)
    - the Respondent's policies and procedures, including the MALT database terms of use and the MALT data access policy.

Assessment of whether AAP 12 has been breached

17. APP 12.1 provides that an APP entity that holds personal information about an individual must, on request, give that individual access to the information.

18. The Complainant requested that the Respondent give them access to their personal information held on the Respondent's MALT database. The Complainant claims the Respondent refused to provide them with access to the requested personal information.

19. In coming to a view regarding whether the Respondent has breached APP 12, I have considered:

    - whether the information in the MALT database includes personal information about patients
    - whether the Respondent holds personal information about patients in the MALT database.

Issue 1: whether the information in the MALT database includes personal information about patients

20. 'Personal information' is defined in s. 6(1) as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

    - whether the information or opinion is true or not, and
    - whether the information or opinion is recorded in a material form or not'.

21. During the investigation of the complaint, the Respondent confirmed that personal information is collected in the MALT database.

22. The Respondent was unable to confirm, however, whether the MALT database specifically contains the Complainant's personal information. For the purpose of determining whether the Respondent has responsibilities in relation to APP 12, I am willing to accept that the MALT database generally contains the personal information of patients.

Finding

23. I find that the MALT database contains personal information about patients.

Issue 2: whether the Respondent holds personal information about patients in the MALT database

24. APP 12 only applies to personal information that an APP entity 'holds'. An APP entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information' (s. 6(1)). The term 'record' includes a document or an electronic or other device.

25. The APP Guidelines explain that the term 'holds' "extends beyond physical possession of a record to include a record that an… entity has the right or power to deal with."[1] The APP Guidelines describe, for example, that an APP entity 'holds' personal information where it physically possesses a record containing the personal information and can access that information physically or by use of an electronic device (such as decryption software).

[1] APP Guidelines [B.84].

26. The Respondent submitted that it does not 'hold' personal information in the MALT database. Instead, the Respondent suggests that the clinicians who enter the data into the MALT database own and hold the personal information.

Analysis of relevant case law

27. I consider the concepts of 'possession' and 'control' as constitutive components of the definition of 'holds'. These concepts were considered by the Victorian Civil and Administrative Tribunal (VCAT) in *Colonial Range Pty Ltd v Victorian Building Authority* [2017] VCAT 1198. In this matter, the Vice President of VCAT considered whether the meeting minutes of the Building Appeals Board (BAB) were in the possession of the Victorian Building Authority (VBA) for the purposes of a request for access to documents under the relevant freedom of information legislation.

28. Both parties agreed that the concept of possession embraced "not just physical possession but also legal or constructive possession and a right and power to deal with the document in question." Constructive possession is based on an entity's right to immediately acquire possession of an object, or the establishment of control over that object.

29. VCAT ultimately accepted that the BAB minutes were properly described as being in the physical custody of the VBA. However, VCAT did not accept that it therefore followed that the minutes were in possession of the VBA. VCAT considered that for this to be accepted, there would have to be evidence of the VBA's intention to possess the minutes, and/or a right to control the minutes.

30. VCAT assessed that the procedures adopted by the VBA to quarantine documents of the BAB demonstrated no intention by the VBA to possess the minutes or other documents relating to the BAB's work. It found that the quarantining procedures used by the VBA for documents of the BAB distinguished the situation from one where the VBA could be said to have constructive possession of the minutes, and ultimately decided that the document being sought was not in the possession of the VBA.

Analysis of OVIC guidance

31. I also reviewed the guidance provided by OVIC regarding the concept of 'possession.' OVIC outlines that a document is in the 'possession' of an agency if the agency has:

    - actual possession of the document – having physical possession and control of the document (for example, in the agency's electronic document management system, on shared drive, or in hard copy complaint file); or
    - constructive possession of the document – a legal right to obtain actual possession or power to deal with the document (for example, a contractual or legal right to require someone to provide the document to the agency).

32. The guidance explains that in determining whether an agency has possession of a document, various factors should be considered, including:

    - whether the agency has an intention to possess the document
    - whether the agency has a right to control or request a copy of the document from a third party (for example another agency or contracted service provider)
    - the purposes for which the document was created and by who.

Analysis of information received from the Respondent

33. I have applied the above concepts to the information obtained about how the MALT database is configured and overseen by the Respondent. Based on the information provided by the Respondent, I understand that:

    - The Respondent owns the MALT database and the servers on which MALT data is stored.
    - The data entered by clinicians into the MALT database is encrypted.
    - Each clinician who enters the data into the MALT database is the only party able to access and release identifiable patient data.

34. The Complainant highlighted that the Respondent's policies indicate it can release information from the MALT database. The Respondent's MALT data access policy refers to the release of de-identified aggregate data. This refers to the collection of metadata which the Respondent uses for the purposes of supporting the administration of the MALT database to determine usage and to support the administration of training programs. I understand that this data can be retrieved by the Respondent without it having access to identifiable patient data. I do not consider that the collection of metadata from the MALT database indicates that the Respondent is able to access personal information in the form of identifiable patient data stored in the MALT database.

35. I am satisfied that the Respondent's staff do not have permission or the ability to access data stored in the MALT database. An encryption key for the MALT database is held by the manager of the Respondent's information technology department, but this key has never been used. The Respondent has expressed no intention to use the key, as this would expose over five million patient records, and has said that, if it received a request to de-encrypt the MALT database, it would refuse to do so.

36. I am satisfied that the Respondent has arrangements in place to ensure it does not access the MALT data, by encrypting the data stored on the MALT database and separating its internal systems from the MALT database by firewall technology.

37. Additionally, the Respondent advised that it has no intention to possess the patient data stored on the MALT database. If the Respondent wished to obtain patient data on the MALT database, it would have to request the data from the clinicians who own it, as it has no right to access the data without the clinicians' consent.

38. I am satisfied that patient data stored on the MALT database is created only by the clinicians for training, professional development and auditing purposes.

39. Based on the above, while the MALT data is within a physical location controlled by the Respondent, I consider it is not information in the possession or the control of the Respondent for the purposes of the Privacy Act. This is because I consider that the MALT data is intended to facilitate training and development, the information is not controlled by the Respondent, the Respondent has no right to request a copy of it, and the Respondent does not intend to possess the MALT data.

40. In particular, I accept that the Respondent has measures in place to ensure that the data is not accessible to its staff, and that the identifiable patient data stored on the MALT database is intended to be used by clinicians and not by the Respondent itself.

41. Therefore, I consider that the Respondent does not 'hold' personal information about patients that is stored on the MALT database.

Finding

42. I find that the Respondent does not hold personal information about patients on the MALT database.

Conclusion

43. I find that the Respondent does not hold personal information about the Complainant in the MALT database and therefore does not have responsibilities with respect to the Complainant's personal information under APP 12.
44. The Respondent has not interfered with the privacy of the Complainant. The complaint is dismissed pursuant to s. 52(1)(a).

Richelle McCausland

National Health Practitioner Privacy Commissioner

Review rights

A party may apply under s. 96 to have a decision under s. 52(1) to make a determination reviewed by the relevant tribunal. An application to the relevant tribunal must be made within 28 days after the day on which the person is given the privacy determination.

To receive this document in another format phone 1300 795 265, using the National Relay Service 13 36 77 if required, or email our complaints team <complaints@nhpo.gov.au>.

Authorised and published by the National Health Practitioner Ombudsman, 50 Lonsdale St, Melbourne.

GPO Box 2630
Melbourne VIC 3001
Phone 1300 795 265
Email the office of the National Health Practitioner Ombudsman <complaints@nhpo.gov.au>
National Health Practitioner Ombudsman website <www.nhpo.gov.au>