



OAIC awards \$13,500 to a person for former employer's unlawful disclosure of medical certificate

In *AYN and Fortrend Securities Pty Ltd*,¹ the Office of Australian Information Commissioner (commonly referred to as "OAIC") awarded a person \$10,000 for non-economic loss and \$3,500 in aggravated damages against their former employer who maliciously shared their medical certificate with the person's client to discredit them.

The OAIC determination clarifies the application of the "employee records exemption" and APP 6 about the use and disclosure of personal information for a "secondary purpose" under the Privacy Act 1988 (Cth).

Under section 52 of the Act, the OAIC has discretion to declare that compensation is due in respect of loss or damage whether arising from injury to feelings, humiliation or otherwise.² This is understood to include pain, anxiety, distress, decline in psychological health and even disruption to an individual's life and relationships.³

Background

After the person resigned, their employer's managing director subjected them to "hostile and aggressive behaviour". The person started feeling anxiety and emotional distress which resulted in their absence during the notice period. Upon seeking medical advice, the person obtained medical certificates which stated they were unfit for work.

It is alleged that after the end of their employment, the managing director contacted the person's clients to tell them that the person "was suffering from a nervous breakdown and was unfit to continue managing client portfolios". One client took issue with these claims and it is alleged that the employer anonymously posted to them the person's medical certificate to "prove it". The employer later denied doing so.

The person alleged that the privacy interference by the managing director was a "serious and deliberate abuse of power designed to inflict maximum harm and embarrassment ... taking advantage of ... private medical situation ... He further exacerbated ... by the untrue statement ...[about] nervous breakdown ... conduct was deeply hurtful and humiliating". Evidence from the person's psychiatrist confirmed that the person suffered from anxiety and depression.

The OAIC was satisfied that the disclosure was "malicious, improper and unjustifiable in the circumstances". The former employer's circumstances were further exacerbated by their failure to engage with the OAIC, denial of the allegations, lack of cooperation and by providing unreliable and inaccurate information to the OAIC.

The 'employee records' were not exempt

The employer claimed that the medical certificate was an "employee record" exempt under the Act.

¹ [2025] AICmr 167.

² Section 52(1AB) Privacy Act 1988 (Cth).

³ *NWFQ v Privacy Commissioner* [2019] AATA 1302 ([link](#)).

Any act or practice concerning an “employee record” by an employer directly related to a past or present employment relationship with an individual is exempt from the Act.⁴ “Employee records” generally include staff records relating to an individual’s employment including health information.⁵

The OAIC agreed that the medical certificate was an “employee record” received during and relating to the person’s employment. However, the OAIC could not see how the malicious disclosure was based on any “employment related purpose”. The exemption did not apply.

Disclosure contravened APP 6

Under APP 6, the person’s consent or special circumstances are required to lawfully use or disclose personal information for a purpose other than that for which it was initially collected (i.e. a “primary purpose”). The use or disclosure of health information for such “secondary purpose” might be permitted with consent, where it is directly related to the primary purpose and reasonably expected by the person or when a statutory exemption applies.

The OAIC found that the disclosure was “not for the primary purpose of assessing the complainant’s fitness to work, or for the purposes of their employment more generally” and there was “no need” to disclose the medical certificate to a third party after the end of the person’s employment. The disclosure was unlawful.

How can organisations mitigate risk of privacy interference?

Indifference to privacy obligations in the context of an employment relationship can give rise to aggravated damages. Organisations should put in place a framework for the correct handling of staff personal information, including a collection notice, privacy policy, access controls and staff training underpinned by robust information security measures.

The use of “employee records” for purposes unrelated to a current or former employment relationship will not be exempt. In practice, the exemption may not apply to:

- any plan to capture information before it becomes a record (e.g. staff monitoring);
- any information relating to staff who are not considered an “employee” (e.g. temporary worker, contractor, volunteer, etc., depending on circumstances);
- any record about a person’s private matter or emergency outside of work that is captured on a corporate system;
- any sharing of employee records with a third party without a justification grounded in the employment relationship or after the end of their employment.

Further, staff data sharing is a daily occurrence in the modern workplace with digital collaboration tools, interconnected services and benefits, mandatory reporting and data sharing with authorities and agencies. Organisations should carefully consider whether the proposed use or disclose of personal information can stay on the right side of APP 6. The assessment of a secondary purpose, reasonable expectations, appropriate transparency or implied consent should not happen without considering reputational, legal and management risks.

⁴ 7B(3) Privacy Act 1988 (Cth).

⁵ 6(1) Privacy Act 1988 (Cth).

This matter does not end there. The employer was ordered to engage an independent reviewer to assess and report on the organisation's data privacy compliance within six months. The organisation will then have to take steps to rectify any compliance shortcomings.

Danielle Dimakis is a Graduate Lawyer and **Alexander Dittel** is Principal Solicitor in KHQ's Data Privacy, Cyber and Digital