Australian Government
Office of the Australian Information Commissioner

'EZ' and 'EY' [2015] AICmr 23 (27 March 2015)

Determination and reasons for decision of Privacy Commissioner, Timothy Pilgrim

Applicant:	**'EZ'**
Respondent:	**'EY'**
Determination date:	**27 March 2015**
Application number:	**C16088**
Catchwords:	**Privacy — Privacy Act — National Privacy Principles (NPP) — NPP 2.1, 3.1, 4.1 —Use and disclosure by medical practitioner of patient's medical information to police officer — Breach of NPPs 2.1 and 4.1 – Compensation awarded — (CTH) *Privacy Act 1988* s 52**

Summary

1. The respondent ('Dr Y') interfered with the complainant (Mr Z's) privacy by disclosing Mr Z's personal information to a third party, in breach of National Privacy Principles (NPP) 2.1 and 4.1.

2. Within 28 days from the date of this determination, Dr Y shall:

   - personally apologise in writing to Mr Z, and
   - pay Mr Z $6500 for the loss caused by the interference with Mr Z's privacy.

Background

3. The following sequence of events is based on the information provided by Mr Z, Dr Y, and a police officer (Sergeant X's) recount of his dealings with Mr Z and Dr Y, as accepted by the Office of the Australian Information Commissioner (OAIC).

4. Dr Y is a medical practitioner who works within a medical centre. Mr Z was a patient of Dr Y.

5. During November 2006, Mr Z contacted his local police station to report harassment and damage to his property as part of an ongoing neighbourhood dispute.[1] On 11 November 2006, Sergeant X attended Mr Z's address along with another police officer to investigate Mr Z's complaints. Sergeant X reported that Mr Z explained his concerns to him in a 'highly excited and at times paranoid fashion'.[2] Sergeant X reported that Mr Z admitted to suffering 'Post Traumatic Stress Disorder, Anxiety Disorder,[and] severe back and knee pain'.[3]

6. On 4 December 2006, Sergeant X called Dr Y, as Mr Z's treating doctor.[4] Dr Y was unavailable and the clinic transferred Sergeant X's call to another doctor (Dr A) within the clinic.[5] Dr A noted in Mr Z's medical records that Sergeant X 'rang… concerned [Mr Z] is psychotic and acting strangly [sic]'.[6]

7. Several days later, Sergeant X called Dr Y.[7] It appears from the documents provided by QPS and Dr Y that Sergeant X asked her whether, in her opinion, Mr Z 'was psychotic'. Dr Y advised Sergeant X that 'it was possible but further assessment was needed'.[8]

8. Mr Z alleges that he became aware of the discussions between Dr Y and Sergeant X through documents he received in response to a freedom of information (FOI) request.[9]

---

[1] As reported by Sergeant X; report attached to a letter provided by Queensland Police Service (QPS) on 30 May 2012.

[2] Report by Sergeant X as attached to a letter provided by QPS employer on 30 May 2012.

[3] As reported by Sergeant X; report attached to a letter provided by QPS employer on 30 May 2012.

[4] It is not clear as to how Sergeant X knew that Dr Y was Mr Z's treating doctor or how he obtained Dr Y's contact details.

[5] This is the subject of a separate complaint (reference number C15438) which has been finalised.

[6] Dr A's note on Mr Z's medical records, 4 December 2006 at 2:45 pm.

[7] The OAIC made enquiries about the exact date of the contact but it was not able to ascertain the date with certainty.

[8] Report by Sergeant X as attached to a letter provided by QPS employer on 30 May 2012 and submission by Dr Y of 15 March 2013

Privacy complaint and investigation

9. On 13 December 2011, Mr Z lodged a complaint under s 36 of the Privacy Act[10] in relation to Dr Y's conduct.

10. Mr Z's complaint raised three allegations, that Dr Y interfered with his privacy in December 2006 by:

    - improperly disclosing his personal information, contained in his medical records, to Sergeant X (alleged breach of NPP 2.1)
    - disclosing inaccurate personal information about him to Sergeant X (alleged breach of NPP 3.1)
    - failing to have adequate security safeguards to protect his personal information from improper disclosure (alleged breach of NPP 4.1).

11. Mr Z is seeking an apology, compensation and a letter from Dr Y to the Queensland Police Service (QPS) to rectify the breach.

12. On 29 May 2012, I opened an investigation into Mr Z's allegations under s 40(1) of the Privacy Act. As this matter relates to events that occurred prior to reforms to the Privacy Act that commenced on 12 March 2014, the complaint has been dealt with under the Privacy Act as it was at the time the acts and practices are alleged to have occurred.

13. As part of the investigation process, the OAIC sought information from the QPS. The QPS provided a copy of Sergeant X's police report and a copy of the activity logs for 4 December 2006.

14. Further written submissions and evidence was provided by both parties.

15. Dr Y does not dispute that the information disclosed is personal information under the Privacy Act. Dr Y acknowledged that she disclosed Mr Z's personal information to Sergeant X. Dr Y also acknowledged that the matter caused Mr Z some stress but did not consider that this incident accelerated or exacerbated any medical condition Mr Z has or had at the time of the events.

16. The matter was not resolved through conciliation and I decided to determine the matter under s 52 of the Privacy Act. Section 52 of the Privacy Act provides that, after investigating a complaint, I may make a determination:

    - dismissing the complaint (s 52(1(a)); or
    - finding the complaint substantiated and declaring:
        - that the respondent has engaged in conduct constituting an interference with the privacy of an individual and should not repeat or continue such conduct (s 52(1)(b)(A)); and/or

[9] The OAIC has not able to ascertain the scope of the request and when the request was lodged. According to correspondence from the QPS dated 30 May 2012, the police report that set out the discussions between Dr Y and Mr Z was released to Mr Z in November 2009.

[10] The Privacy Act as it was at 13 December 2011, prior to the reforms introduced on 12 March 2014.

- the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant (s 52(1)(b)(ii)); and/or
- the respondent is entitled to compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint (s 52(1)(b)(iii)); and/or
- it would be inappropriate for any further action to be taken in the matter (s 52(1)(b)(iv)).

Information taken into consideration

17. In making this determination, I considered the following material:

- the Privacy Act, specifically NPPs 2, 3 and 4
- *Guidelines to the National Privacy Principles*[11]
- *Privacy in the Private Health Sector*[12]
- information provided by Mr Z, including his complaint, relevant medical records, and various submissions provided to the OAIC during the investigation process
- information provided by Dr Y, including submissions to the OAIC and correspondence to the QPS
- information provided by the QPS relating to the alleged disclosure and events leading up to the disclosure
- privacy determinations and case law relating to the Privacy Act.

Legislative framework

18. The NPPs outlined the standards for 'organisations' handling personal information at the time of these allegations.[13]

19. Under s 16A(2) of the Privacy Act, an organisation was prohibited from doing an act, or engaging in a practice, that breaches an NPP.

[11] *Guidelines to the National Privacy Principles* (2001). The Guidelines to the National Privacy Principles (NPP) were developed to help organisations to comply with the NPPs and to avoid interfering with an individual's privacy. The Guidelines indicate some factors the Commissioner may take into account when handling a complaint. The guidelines are advisory only and not legally binding. The Guidelines are available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guidelines-to-the-national-privacy-principles.

[12] *Privacy in the Private Health Sector* (2001). This guide aims to assist the private health sector in better understanding the application of the NPPs to its business and services. The guide is available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-in-the-private-health-sector-november-2001.

[13] The NPPs were contained in Schedule 3 of the Privacy Act. The Australian Privacy Principles replaced the National Privacy Principles (NPPs) and the Information Privacy Principles (IPPs) from 12 March 2014 (except for ACT Government agencies, who continue to be covered by the IPPs). These new APPs apply to both Australian Government agencies and organisations covered by the Privacy Act.

20. ‘Organisation’ under the Privacy Act include as meaning:

(a) an individual; or

(b) a body corporate; or

(c) a partnership; or

(d) any other unincorporated association; or

(e) a trust

that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

21. Dr Y is a medical practitioner. Dr Y falls within the definition of ‘organisation’ under s 6C of the Privacy Act, being a health service provider, and is accordingly bound by the NPPs. As she is an individual, consistent with my obligations under the Privacy Act, Dr Y has not been personally named in this determination.[14]

22. The complainant alleges that Dr Y breached NPP 2.1 (use and disclosure), 3.1 (data quality) and 4.1 (data security). I will consider each alleged breach and the relevant NPP in turn.

Alleged breach of NPP 2.1

23. NPP 2.1 provided that:

> An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:
>
> (a) both of the following apply:
>
> (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
>
> (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;...

24. The *Guidelines to the National Privacy Principles* issued by the then Office of the Federal Privacy Commissioner in September 2001 (the NPP Guidelines)[15] state that ‘[t]o be related, the secondary purpose must be something that arises in the context of the primary purpose. If personal information is sensitive information, the use or disclosure must be directly related to the primary purpose of collection. This means that there must be a stronger connection between the use or disclosure and the primary purpose for collection’.[16]

[14] It is the general practice of the OAIC not to name a party if the party is an individual.

[15] These guidelines have been superseded by the APP *Guidelines to the National Privacy Principles*, page 35, Guidelines which apply from 12 March 2014.

[16] *Guidelines to the National Privacy Principles*, page 35.

25. Mr Z alleges that Dr Y breached NPP 2.1 by discussing his personal information with Sergeant X.

26. Dr Y acknowledges that she disclosed Mr Z's personal information in her discussions with Sergeant X. Dr Y initially submitted that she was entitled to rely on the exceptions set out in NPP 2.1(e), (f), (g) and (h). I have considered each of these below.

27. Dr Y has since acknowledged that her disclosure of Mr Z's personal information to Sergeant X was an interference with Mr Z's privacy, although Dr Y maintains that the disclosure was made in good faith and under the belief that 'the mere fact that the police called a medical practitioner concerning someone with whom they were clearly having dealings could only suggest that there was a serious and imminent threat'. For the reasons set out below, I am satisfied that Dr Y was not entitled to rely on the exceptions set out in the NPPs, specifically NPP 2.1(e), (f), (g) and (h) and therefore breached NPP 2.1.

Exception: NPP 2.1(e)

28. Dr Y relied on NPP 2.1(e) for her disclosure to Sergeant X, stating that as '[the police officer] spoke of a neighbourhood dispute, [Dr Y] was under the impression that there was a concern of public safety'. Dr Y also claims that because 'the police were concerned enough to telephone to ask [Dr Y] if [Mr Z] was psychotic, this suggested to [Dr Y] that this was an urgent matter of public, and [Mr Z's] safety, and so a response was appropriate and justified'.

29. NPP 2.1(e) permitted the disclosure of personal information where the:

> 'organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:
>
> i. a serious and imminent threat to an individual's life, health or safety; or
>
> ii. a serious threat to public health or public safety'

30. In considering NPP 2.1(e), I have considered the terms 'reasonably' and 'necessary'.

31. The term 'reasonable' and 'reasonably' are not defined in the Privacy Act. The Macquarie Dictionary relevantly defines these terms as 'agreeable to reason or sound judgement'. What is reasonable is a question of fact in each individual case.

32. The term 'necessary' is also not defined under the Privacy Act. I recently considered it's meaning in *'DO' and Department of Veterans' Affairs* [2014] AICmr 124 in the context of the Information Privacy Principles (IPPs) which apply to agencies:

> The word 'necessary' is also not defined in the Privacy Act. The Macquarie Dictionary, 3rd edition, relevantly defines necessary as 'indispensable' or 'requisite'. The Plain English Guidelines note that an agency must reasonably believe that it is necessary to take this action, that is to use or disclose an individual's personal information, to prevent the threat or lessen the threat to a noticeable extent. Using or disclosing personal information, even to prevent or lessen a serious threat to health or life, may significantly disadvantage the person the information is about. If this is the case, an

agency should seriously consider if there are any effective alternatives available that do not have this consequence.[17]

33. In relation to NPP 2.1(e)(i), I have considered the meaning of the terms 'serious' and 'imminent'. These terms are not defined in the Privacy Act although I have considered them in recent privacy determinations:

> [27] … In attempting to define the term, I have relied on the ordinary meaning of the words 'serious' and 'imminent'. The Macquarie Dictionary relevantly defines 'serious' as 'grave' or 'being in earnest; not trifling'. It defines 'imminent' as 'impending' or 'likely to occur at any moment'.
>
> [28] Though not binding or exhaustive, the Plain English Guidelines explain that whether a threat is 'serious' is to be determined on the particular circumstances of each matter. Examples may include, relevantly here:
>
> - an explicit threat of ... assault
> - a specific threat of physical harm to a particular officer in an agency (although abuse directed to staff in general does not usually count as a serious threat)
>
> In relation to whether a threat is imminent, the Plain English Guidelines explain that this means 'the threatened harm must be about to happen'.[18]

34. The NPP Guidelines provides guidance as to whether a threat is 'serious and imminent':

> This exception is aimed at emergency situations where there is a serious threat to health and safety and using or disclosing information will help reduce that threat. Serious and imminent threats to an individual's life health or safety may be a threat to the individual the organisation is dealing with or another person.
>
> Ordinarily a serious threat would be a threat of bodily injury, threat to mental health, illness or death. 'Imminent' means the threatened harm is about to happen. Threats to finances and reputation or a threat of stress or anxiety would not ordinarily be serious threats to life or health.[19]

35. The *Guidelines on Privacy in the Health Sector* (Health Sector Guidelines) also relevantly says:

> In limited circumstances, a health service provider may need to use or disclose personal information to lessen or prevent:
>
> - a serious and imminent threat to an individual's life, health or safety
> - a serious threat to public health or public safety.

[17] *'DO' and Department of Veterans' Affairs* [2014] AICmr 124 at [26] (footnotes omitted).
[18] *'DO' and Department of Veterans' Affairs* [2014] AICmr 124 at [27]-[29] (footnotes omitted).
[19] *Guidelines to the National Privacy Principles*, pages 17-18.

> This exception allows for such uses and disclosures and generally relates to emergencies. Depending on the circumstances, this exception can allow disclosures to the police service or other government authorities, such as a community services department or mental health crisis team. The exception also allows for disclosure to an individual whose life, health or safety is threatened.
>
> A 'serious and imminent' threat to an individual's life, health or safety relates to harm that could be done to any person (including the individual seeking treatment and care).
>
> A 'serious' threat must reflect significant danger, and could include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. Alternatively, it could include the threat of infecting a person with a disease that may result in death or disability. A threat could also relate to an emergency, following an accident, when an individual's life or health would be in danger without timely decision and action.
>
> A threat is 'imminent' if it is about to occur. This test could also include a threat posed that may result in harm within a few days or weeks. It is much less likely to apply to situations where the risk may not eventuate for some months or longer. [20]

36. In relation to NPP 2.1(e)(ii), the Health Sector Guidelines provide that:

> A 'serious' threat to public health or public safety relates to broader safety concerns affecting a number of people. This could include the potential spread of a communicable disease, harm caused by an environmental disaster or harm to a group of people due to a serious, but unspecified, threat. [21]

37. In forming my view as to whether Dr Y had a 'reasonable belief' that Mr Z posed a serious and imminent threat to himself under NPP 2.1(e)(i) or a serious threat to public safety under NPP 2.1(e)(ii), I considered Dr Y's submissions, subsequent correspondence to QPS and notes on Mr Z's medical records:

- Dr Y says in her submissions that she was 'not up to date' with Mr Z's personal situation at the time of the phone contact.
- Mr Z's medical records show that Dr Y's last consultation with Mr Z had been approximately one month before the disclosure. Dr Y had been involved in Mr Z's medical management for at least the two years prior to the last consultation. Dr Y consulted Mr Z on no less than 26 occasions over the two year period.
- Dr Y's correspondence to the QPS dated 9 July 2010 stated that Mr Z 'is not and has never been psychotic'.
- Dr Y says in her submissions she has been unable to recall or suggest any specific threat that Mr Z posed to himself or the public. Further, it does not appear that Dr Y made any enquiries to Sergeant X, consistent with requirements of the Health Sector Guidelines, as to the nature of the circumstances that had led Sergeant X to contact her. I note that Sergeant X's

[20] *Guidelines on Privacy in the Health Sector*, pages 18-19.
[21] *Guidelines on Privacy in the Health Sector*, pages 18-19.

call to Dr Y was 'several days' after the initial call to the clinic which also indicates that there was no sense of imminent threat to Mr Z or the public.

- Mr Z's medical records do not contain any indication that, following the phone call from Sergeant X, Dr Y was concerned that Mr Z posed or may pose a serious and imminent threat to himself or to public safety.

38. I accept Dr Y's claim that she has made the disclosure 'in good faith to a law enforcement officer' and that Dr Y assumed that Sergeant X 'had the authority to request the information'. I further accept that Sergeant X could be regarded as a person to be in a position to prevent or lessen a serious or imminent threat.

39. I note, however, that Dr Y had been treating Mr Z for two years prior to the event and as noted above at [37], on no less than 26 occasions over the two year period. Given Dr Y's prior regular involvement in Mr Z's care, and lack of more detailed questioning of Sergeant X as to the reasons for his request for information, I am not satisfied that Dr Y could have formed a reasonable belief that Mr Z at the time posed a serious and imminent threat to himself or to public safety at the time of Dr Y's disclosure to Sergeant X.

40. Consequently, I am not satisfied that Dr Y could rely on the exception set out in NPP 2.1(e).

Exception: NPP 2.1(f)

41. NPP 2.1(f) permits the disclosure of personal information where:

> the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities

42. Dr Y also relied on NPP 2.1(f) for the disclosure, stating that she 'assumed that the matter was important otherwise Sergeant [X] would not have taken the steps to contact you [me]'.

43. The NPP Guidelines state:

> This acknowledges that one of an organisation's legitimate functions is to investigate and report on suspected unlawful activity. Ordinarily but not in all cases, the suspected unlawful activity would relate to the organisation's operations.[22]

The Health Sector Guidelines make similar references.

44. There is insufficient information before me to support that Dr Y suspected, or had reason to suspect, unlawful activity. The information before me indicates that the phone conversation with Sergeant X was not part of an investigation into unlawful activity. Consequently, I am not satisfied that Dr Y can rely on the exception set out in NPP 2.1(f).

[22] *Guidelines to the National Privacy Principles*, page 41.

Exception: NPP 2.1(g)

45. NPP 2.1(g) permits the disclosure of personal information where 'the use or disclosure is required or authorised by or under law'.

46. Dr Y submitted that she was entitled to rely on NPP 2.1(g) for the disclosure as 'Sergeant [X] identified himself as a law enforcement officer and therefore [she] assumed that he had the authority to request the information'.

47. The NPP Guidelines state:

> The Privacy Act does not override specific legal obligations relating to use or disclosure of personal information. 'Law' includes Commonwealth, State and Territory legislation, as well as common law. If an organisation is required by law to use or disclose personal information it has no choice and it must do so. If an organisation is authorised by law to use or disclose personal information it means the organisation can decide whether to do so or not. The authority is there but the organisation can decide.[23]

48. The Health Sector Guidelines provide:

> If the law requires that a health service provider use or disclose information, the provider must do so. Examples of such requirements include the mandatory reporting of child abuse (under care and protection laws) or the notification of diagnoses of certain communicable diseases (under public health laws).
>
> Disclosure must occur if there is a warrant or law requiring the health service provider to do so.
>
> If the law authorises the use or disclosure of information, the health service provider can decide whether to do so or not - the legal authority exists, but the provider has discretion.[24]

49. The Health Sector Guidelines further note that:

> The Privacy Act does not compel a health service provider to use or disclose personal information, but other law may do so.
>
> Where a use or disclosure is authorised by law, health service providers' professional codes of practice and ethics may offer relevant guidance.
>
> Other disclosures in the health and welfare sectors, under this provision, would include those to guardians or administrators (depending on the decision-making powers conferred upon them) and to guardianship, administration and mental health tribunals.[25]

50. As there was no warrant or any evidence provided by Dr Y of any legislative provisions that required or authorised Dr Y to disclose Mr Z's personal information to the QPS, I am not satisfied that Dr Y can rely on NPP 2.1(g).

---

[23] *Guidelines to the National Privacy Principles*, page 41.
[24] *Guidelines on Privacy in the Health Sector*, pages 20-21.
[25] *Guidelines on Privacy in the Health Sector*, page 21.

Exception: NPP 2.1(h)

51. NPP 2.1(h) permits the disclosure of personal information where:

> the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
>
> i. the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
>
> ii. the enforcement of laws relating to the confiscation of the proceeds of crime;
>
> iii. the protection of the public revenue;
>
> iv. the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
>
> v. the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

52. NPP 2.2 provides that:

> If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

53. Dr Y has not provided any information to support the claim the disclosure was permitted under 2.1(h).

54. The NPP Guidelines and the Health Sector Guidelines provided detailed and relevant guidance in the application of this exception.

55. The NPP Guidelines provide:

> This allows an organisation to use or disclose personal information where it reasonably believes this is reasonably necessary for a range of functions or activities carried out by, or on behalf of, an enforcement body (see section 6 for what is an enforcement body). Unless the law prohibits it, the organisation must make a written note of such a use or disclosure (see NPP 2.2).[26]

56. The Health Sector Guidelines also provides a useful discussion:

> This provision permits a health service provider to use or disclose personal information, where they have a reasonable belief that this is reasonably necessary for a range of functions or activities carried out by, or on behalf of, an enforcement body. An enforcement body in this context includes the National Crime Authority, the Australian Customs Service and other Commonwealth, State or Territory authorities established under law to conduct criminal investigations or inquiries. Permitted uses and disclosures could relate to suspected unlawful activity, criminal offences or other breaches of law, suspected improper conduct or preparation for and conduct of Court or Tribunal proceedings. This is not an exhaustive list; refer to NPP 2.1 (h) for more information.

[26] *Guidelines to the National Privacy Principles*, page 41.

> The Privacy Act does not intend to interfere with health service providers' legal obligations, which might already affect the use and disclosure of personal information. For example, this provision does not override the duty of confidentiality between a medical practitioner and an individual. A health service provider is entitled not to disclose personal information if there is no law that requires it.
>
> However, the Privacy Act does not intend to deter health service providers from lawfully co-operating with agencies performing law enforcement functions. Police and other enforcement bodies are generally reliant on voluntary co-operation to provide information.
>
> Many health service providers, including mental health or drug and alcohol workers, general practitioners and counsellors, treat people who engage in unlawful activity. These individuals need to have access to health services in confidence, particularly for treatment of health issues intrinsically linked to unlawful behaviour. Usually, this approach sits at the core of the 'harm minimisation' model in dealing with a range of 'at risk' behaviours.
>
> When considering a request for such a disclosure, the importance of maintaining the individual's confidentiality must be balanced with the public interest in the investigation and enforcement of the criminal law.[27]

57. The Health Sector Guidelines further provide:

> Before deciding to use or disclose health information under this provision, health service providers should consider:
>
> - the seriousness of the situation – for instance, an investigation into an alleged murder or sexual offence would be more serious than property theft;
> - the risks associated with a disclosure without the individual's consent or knowledge, balanced against the implications of non-disclosure;
> - their relevant professional and ethical obligations; and
> - whether the circumstances indicate a serious and imminent threat to the health, life or safety of any person.[28]

58. I note that the Federal Court has examined a similar issue in *Jones v Office of the Australian Information Commissioner* [2014] FCA 285. In that case, the applicant sought review of the decision by a delegate of the Information Commissioner to cease further investigation of her complaint. The complaint related to the disclosure of her medical records by her doctor to the QPS. The QPS contacted the doctor and advised that they intended to execute a warrant at the doctor's place of practice to seize the applicant's clinical records and sought to arrange a time to execute the warrant. The QPS attended the doctor's place of practice, produced the warrant and drew the doctor's attention to the part of the warrant authorising seizure of the applicant's records.

[27] *Guidelines on Privacy in the Health Sector*, page 21.
[28] *Guidelines on Privacy in the Health Sector*, pages 21-22.

59. The delegate of the Information Commissioner decided to cease further investigation of the complaint as he was satisfied that the doctor *reasonably believed* that the disclosure was *reasonably necessary* for the detection, investigation, prosecution or punishment of a criminal offence, breach of a law imposing a penalty or sanction, or breach of a prescribed law, by an enforcement body (in this case the Queensland Police Service). Greenwood J dismissed the application as he was satisfied that there was material before the delegate of the Information Commissioner upon which the delegate could be satisfied, that the doctor held a reasonable belief that disclosure of the applicant's medical records was reasonably necessary for the investigation of a criminal offence.

60. In my view, Mr Z's complaint can be distinguished from *Jones.* As noted at [50], there is no evidence before me to suggest that a warrant required or authorised Dr Y to disclose Mr Z's personal information to the QPS. Further, while I accept that the QPS is an enforcement body, there is no information before me to demonstrate that the activities listed in NPP 2.1(h)(i) to (v) are relevant to the circumstances surrounding Sergeant X's phone call to Dr Y in December 2006.

61. There is also insufficient information before me to suggest that Dr Y considered the risks associated with disclosing Mr Z's personal information without his consent, or to suggest that Dr Y enquired about the purpose of Sergeant X's phone call to establish the severity of the situation.

62. I also note that Dr Y has not made a written note of the use or disclosure which is required under NPP 2.2 for NPP 2.1(h) to apply.

63. Consequently, I am not satisfied that Dr Y is entitled to rely on the exception set out in NPP 2.1(h).

Findings

64. The exceptions set out in NPP 2.1(e), (f), (g) and (h) do not apply.

65. Dr Y has breached NPP 2.1 and has interfered with Mr Z's privacy.

Alleged breach of NPP 3

66. NPP 3.1 provides:

> An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

67. Mr Z alleges that Dr Y informed Sergeant X that he [Mr Z] had a 'history of psychosis' or is 'psychotic' and this is inaccurate. In reply, Dr Y submits that:

> Sergeant C asked if in my opinion that Mr Z was psychotic. I replied that it was possible but further assessment was needed.

68. The NPP Guidelines and the Health Sector Guidelines referred to particular factors to consider in determining what are 'reasonable steps':

- how likely it is that the personal information is complete, accurate and up-to-date;
- whether this kind of personal information changes over time;

- how recently the organisation collected the personal information;
- how reliable the personal information is likely to be;
- who provided the personal information; and
- what the organisation uses the personal information for. [29]

69. As the Health Sector Guidelines state, 'risks relating to poor data integrity can include the misrepresentation of an individual's health condition'.[30]

70. Dr Y's says that 'it was made clear [to Sergeant X] that I was not up to date with his [Mr Z's] personal situation at that moment and recommended that assessment by a psychiatrist might be appropriate'. Sergeant X asked for her opinion and Dr Y provided her response based on her professional assessment of the situation at the time.

71. While it may have been a reasonable step in the circumstances for Dr Y to refer to Mr Z's medical records prior to responding to the inquiry by Sergeant X, I do not think that in not doing so Dr Y has disclosed inaccurate information to QPS. I have viewed Mr Z's medical records from 25 November 2004 up to the December 2006. Mr Z's records indicate that he had anxiety and stress. Mr Z's records do not indicate that Mr Z had a history of psychosis or was psychotic, or was possibly psychotic. The only mention of the word 'psychotic' is the entry made by Dr A on 4 December 2006, stating [Sergeant X] was concerned that Mr Z was 'psychotic and acting strangly [sic]'.

72. While it would have been a more accurate and complete response to acknowledge, based on the medical records that were available, that Mr Z did not have any recent history or diagnosis of psychosis, I am of the view that the absence of that additional information does not render the information that was provided inaccurate.

Findings

73. While Dr Y's comments to QPS have caused significant distress to Mr Z Dr Y, I do not think they constitute a breach of NPP 3.1.

Alleged breach of NPP 4

74. NPP 4.1 provides:

> An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

75. Mr Z alleges that Dr Y failed to follow specific protocols, as Dr Y was required to do as a general practitioner, before releasing his personal information to Sergeant X. Implicitly, Mr Z alleges that Dr Y failed to take reasonable steps to protect his personal information from improper disclosure.

76. The NPP Guidelines and the Health Sector Guidelines discuss what are reasonable steps in the context of physical security and electronic security.[31] In my view, security

[29] *Guidelines to the National Privacy Principles*, page 43 and *Guidelines on Privacy in the Health Sector*, page 25.
[30] *Guidelines on Privacy in the Health Sector*, page 25.

of personal information does not only relate to physical security of that information, it clearly relates to the steps taken by the holder of the information to ensure it is only disclosed in circumstances that are lawful. In this case, I consider 'reasonable steps' to include:

- questioning the police officer about his reasons for contacting Dr Y in relation to Mr Z's health, including ascertaining if there was a warrant or other relevant legislation that authorised the collection and disclosure of the information
- ascertaining if the circumstances could constitute a serious and imminent threat to the person or the public
- consideration of the various polices, guidelines and obligations in law that apply to the disclosure of personal health information.

77. Dr Y says that she follows the Code of Conduct stipulated by the Australian Health Practitioner Regulation Agency (AHPRA) and the privacy policy of the Independent Practitioner Network (IPN). Dr Y also submits that the medical centre that employs her is governed by the Royal Australian College of General Practitioners' (RACGP) Rules on privacy, which stipulate that confidentiality and privacy of health information is to be safeguarded in accordance with the NPPs.

78. I have considered the parties' submissions. I note that the AHPRA only came into being on 1 July 2010, several years after the disclosure occurred and so the Code of Conduct was not relevant at the time of the events. I have reviewed the IPN's Privacy Policy as it existed at the time of the breach. The policy provides that personal information may be disclosed in a number of circumstances, most relevant to this case are:

- as required under compulsion of law and
- where there is a serious and imminent threat to an individual's life, health or safety; or a serious threat to public health or public safety.

79. In this case, there is no information before me to suggest that Dr Y questioned the reasons for the police seeking her views on Mr Z. Further, it is my view that insufficient consideration was given to the obligations imposed on health providers to protect an individual's health information, and the need for rigour in considering when it was permitted to disclose that information as articulated in various policies, guidelines. I believe that such steps are a necessary part of securing personal information from unauthorised disclosure.

80. I appreciate Dr Y's advice that she is now mindful of the obligations imposed by APHRA, the RACGP and the Privacy Act. However, at the time of this incident I do not believe reasonable steps were taken to protect Mr Z's health information.

Findings

81. Dr Y did not take reasonable steps to protect Mr Z's personal information. Dr Y breached NPP 4.1.

[31] *Guidelines to the National Privacy Principles*, page 23 and *Guidelines on Privacy in the Health Sector*, page 26.

Damages

82. I have the discretion under s 52(1)(b)(iii) of the Privacy Act to award compensation for 'any loss or damage suffered by reason of' the interference with privacy. Under section 52(1A), loss or damage can include 'injury to the complainant's feelings or humiliation suffered by the complainant'.

83. The principles for awarding compensation in such matters have been canvassed by the Administrative Appeals Tribunal (AAT) in *Rummery and Federal Privacy Commissioner:*[32]

    (a) where a complaint is substantiated and loss or damage is suffered, the legislation contemplates some form of redress in the ordinary course

    (b) awards should be restrained but not minimal

    (c) in measuring compensation the principles of damages applied in tort law will assist, although the ultimate guide is the words of the statute

    (d) in an appropriate case, aggravated damages may be awarded

    (e) compensation should be assessed having regard to Mr Z's reaction (including injury to feelings, distress and humiliation) and not to the perceived reaction of the majority of the community or of a reasonable person in similar circumstances

    (f) once loss is established, there must be good reason not to award compensation for that loss.

Complainant's submissions

84. As noted at [11], Mr Z is seeking an apology and compensation. Mr Z makes the following submissions in relation to how the disclosure has affected him:

> As a result of [Dr Y's] breach of my privacy in December 2006, I have suffered the following hardships:
>
> … I have seen him [medical practitioner] 30 times since December 2011 mostly regarding stress related to this process. I also claim the travel expenses to and from medical appointments. Other outlays include [for] paper, photocopying, ink cartridges and postal stamps. I have had to travel to have various affidavits witnessed by a Justice of the Peace.
>
> 2. Financial hardship for the following outlays (for example)
>
> Medical treatment, as set out in enclosed letter of [name omitted] …., I have seen him 30 times since December 2011
>
> 3. An adverse impact to my health (both physically and emotionally)
>
> - I have been greatly upset and concerned by the stigma of mental illness that has been attached to me as a result of this breach and the disclosure of this

[32] [2004] AATA 1221 [32] *(Rummery)*.

information to the police. This has been particularly hurtful given that it is not true.

- As a person with a disability this stress, caused by the incorrect breach of privacy of [Dr Y], has had a greater impact on me than it would perhaps on others and is preventing me from contributing to society in a positive way as this process takes up all my time.

- I see my occupational therapist [name omitted] regularly to undertake work-ready-training. Due to my mental illness the stress of this process and the statement to police by [Dr Y] have meant my mind is preoccupied and I am unable to participate in a meaningful way in our sessions.

4.Significant strain and stress placed on my family, in particular my daughter and elderly [mother]

4. [sic] Significant strain and stress placed on my family due to the adverse impact to my physical and emotional well-being.

Respondent's submissions

85. Dr Y was of the view that she bears no liability in relation to the compensation. During the course of the investigation into the complaint, Dr Y submitted that:

> It is clear that both prior to and subsequent to the matter about which this complaint has been made [Mr Z] was under significant medical supervision for his mental illness. Whilst [Dr Y] acknowledges that this matter has undoubtedly caused [Mr Z] some stress, [Dr Y] does not consider that this incident has in any meaningful way accelerated or exacerbated [Mr Z's] mental illness. The medical evidence used by [Mr Z] to support this contention is equivocal in the extreme'

86. Dr Y further submitted:

> Dr Y does not agree with the diagnosis of [Mr Z's psychologist] in his report dated 15 April 2013 that Mr [Z] suffers from post traumatic stress disorder as a result of this incident. Dr Y states that Mr [Z] does not meet the criteria in the DSMIV for such a diagnosis.

87. Dr Y also submitted that it is Mr Z who continued to 'agitate' in relation to this matter notwithstanding her early correspondence with the QPS in which she corrected the information she provided that the complainant was not psychotic at the time of the phone call in 2006. Dr Y submitted that:

> If it is alleged that this matter has had detrimental effect on [Mr Z's] pre-existing mental condition then [Dr Y] would submit that arises significantly from [Mr Z's] own pre-occupation with this matter. This is clear from the medical reports obtained on his own behalf in particular those from Dr [name omitted] and [name omitted].

Considerations

88. In my view, the statements made by Mr Z in his complaint and subsequent submissions and the reaction of Mr Z to the disclosure made by Dr Y indicates that Mr Z suffered injury to his feelings and distress because of Dr Y's conduct. I also have

regard to the volume of correspondence received by the OAIC from Mr Z outlining his continued distress arising from these events. In my view, an award of compensation is appropriate.

89. In deciding the appropriate amount of compensation, I have had particular regard to the AAT's decision in *Rummery.* In *Rummery*[33], the applicant sought review of the Privacy Commissioner's determination not to make a declaration as to compensation. The applicant was an employee of the Australian Capital Territory Department of Justice and Community Safety (JACS). The applicant had made a public interest disclosure to the ACT Ombudsman under the Public Interest Disclosure Act 1994 (ACT) alleging that the JACS had failed to enforce provisions of the *Liquor Act 1975* (ACT). During the course of the investigation, the JACS disclosed to the ACT Ombudsman the applicant's personal information, including employment related issues. On learning of this disclosure, the applicant made a complaint to the Privacy Commissioner that his privacy had been interfered with. The Privacy Commissioner had determined[34] the complaint was substantiated but decided not to make a declaration regarding compensation.

90. The AAT in its assessment of an appropriate amount of compensation said:

> [53] …we have considered Mr Rummery's evidence as to his feelings when he learned of the details of the disclosures made by Mr Keady [the head of the department]. This was clearly a breach in Mr Rummery's eyes.
>
> [54] It is our opinion also that this was a serious breach. We have had regard to this in assessing the significance of Mr Rummery's evidence as to the injury to his feelings and humiliation. It assists us in assessing the depth of his feelings. ..

91. The AAT in that matter concluded that an appropriate award for the injury to Mr Rummery feelings and humiliation was $8000.

92. I have also considered previous determinations where compensation was awarded. The following determinations, in particular, provide support to the finding that the disclosure by Dr Y to Sergeant X contributed to Mr Zs' injury to his feelings and distress:

- In '*D' v Wentworthville Leagues Club*[35]*,* I awarded $7500 after finding that the Club interfered with the complainant's privacy by disclosing their membership details and gaming information to the complainant's ex-partner, who further disclosed the information to the complainant's family, friends, previous neighbours, parents of children's friends and work colleagues, causing the complainant to suffer humiliation as well as serious anxiety and panic attacks.

- In *'BO' and AeroCare*[36], I awarded $8500 for non-economic loss caused by the interference with the complainant's privacy. In that case, I found that AeroCare

[33] *Rummery and Federal Privacy Commissioner and Anor* [2004] AATA 1221.
[34] Complaint Determination No 5 of 2004
[35] *'D' and Wentworthville Leagues Club* [2011] AICmr 9 (9 December 2011)
[36] *'BO' and Aerocare* [2014] AICmr 32 (8 April 2014)

had breached the complainant's s privacy both in its collection and disclosure of his sensitive medical information, and in circumstances where the complainant's disability made him particularly vulnerable.

- In *'CP' and Department of Defence*[37], I awarded $5000 after finding that the Department interfered with the complainant's privacy by disclosing personal information to the complainant's treating general practitioner without his consent.

93. I am satisfied that Dr Y's unlawful disclosure had a significant impact on Mr Z. In deciding the appropriate amount of compensation to award in this matter, I have also placed weight on:

- the sensitive nature of the personal information that was disclosed; and
- the responsibility of Dr Y to have a sound understanding of privacy obligations and the need to ensure disclosure of health information are authorised under the Privacy Act.

I have also placed weight on:

- that the information was disclosed to an officer of the QPS, noting that the officer would also have been subject to a legal framework that requires confidentiality; and
- that the information disclosed was clarified by Dr Y in subsequent correspondence with the QPS

Findings

94. Mr Z suffered injury to his feelings and distress because of the interference with his privacy by Dr Y's conduct.

95. Taking all the circumstances into account, I have decided that compensation in the amount of $6500 is appropriate.

96. I acknowledge that Mr Z is also seeking for Dr Y to write to the QPS to rectify the information it was provided by Dr Y about Mr Z. I am aware that Dr Y has written to the QPS on at least two occasions and I am satisfied that the letters address the concerns raised by Mr Z. Given this, I do not think it necessary for me to require Dr Y to write to the QPS again.

Determination

97. I declare in accordance with s 52(1)(b)(i)(B) of the Privacy Act that Mr Z's complaint is substantiated and that Dr Y breached NPPs 2.1 and 4.1 by disclosing the personal information of Mr Z.

98. I declare in accordance with s 52(1)(b)(ii) of the Privacy Act that:

[37] *'CP' and Department of Defence* [2014] AICmr 88 (2 September 2014)

- Dr Y shall apologise to Mr Z in writing within four weeks from the date of this determination; and
- Dr Y shall pay Mr Z $6500 for the loss caused by the interference with Mr Z's privacy within four weeks from the date of this determination.

Timothy Pilgrim
Privacy Commissioner

27 March 2015

Review rights

A party may apply under s 96 of the *Privacy Act 1988* to have the decision reviewed by the Administrative Appeals Tribunal (AAT). The AAT provides independent merits review of administrative decisions and has power to set aside, vary, or affirm a privacy determination. An application to the AAT must be made within 28 days after the day on which the person is given the privacy determination (s 29(2) of the *Administrative Appeals Tribunal Act 1975*). An application fee may be payable when lodging an application for review to the AAT. Further information is available on the AAT's website (www.aat.gov.au) or by telephoning 1300 366 700.

A party may also apply under s 5 of the *Administrative Decisions (Judicial Review) Act 1977* to have the determination reviewed by the Federal Court of Australia or the Federal Circuit Court. The Court will not review the merits of the determination, but may refer the matter back to the OAIC for further consideration if it finds the Information Commissioner's decision was wrong in law or the Information Commissioner's powers were not exercised properly. An application to the Court must be lodged within 28 days of the date of the determination. An application fee may be payable when lodging an application to the Court. Further information is available on the Court's website (http://www.federalcourt.gov.au/) or by contacting your nearest District Registry.