Australian Government Solicitor

Express law
fast track information for clients

AGS

27 MAY 2015

Privacy determination – need to scrutinise law enforcement requests before disclosing personal information

A recent privacy determination by the Privacy Commissioner creates a significant precedent about the standard expected when scrutinising requests from police for information about medical practitioners' patients. It is not enough to make a disclosure in good faith to a law enforcement officer or assume the officer has the authority to request the information.

Unauthorised disclosure (even on a mistaken belief that it was authorised) can result in a breach of both the disclosure principle (APP 6) and security of personal information principle (APP 11).

Key points

In *'EZ' and 'EY'* [2015] AICmr 23, the Privacy Commissioner determined that the medical practitioner, 'Dr Y', had interfered with the privacy of the complainant, 'Mr Z', by unlawfully disclosing his personal information to the Queensland Police Service and failing to take reasonable steps to protect his personal information. The Commissioner determined that Dr Y must:

- personally apologise to Mr Z
- pay $6,500 for the loss caused by the interference with Mr Z's privacy.

Mr Z's complaint was made in December 2011 about conduct in December 2006, so the National Privacy Principles (NPPs), not the current Australian Privacy Principles (APPs), applied to the matter. However, the APPs impose substantially similar requirements on APP entities.

The complaint

Dr Y was Mr Z's treating doctor. In December 2006 Sergeant X called Dr Y to ask her whether Mr Z 'was psychotic'. Dr Y advised Sergeant X that 'it was possible but further assessment was needed'.

Dr Y noted in Mr Z's medical records that Sergeant X 'rang … concerned [Mr Z] is psychotic and acting strangely [sic]'.

Mr Z subsequently complained that Dr Y interfered with his privacy by:

- improperly disclosing his personal information to Sergeant X
- disclosing inaccurate personal information about him to Sergeant X
- failing to have adequate security safeguards to protect his personal information from improper disclosure.

No reasonable belief of serious and imminent threat

The Commissioner did not accept Dr Y's submissions that she was permitted to disclose Mr Z's personal information because it was reasonably necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or safety (NPP 2.1(e) and current s 16A).

While accepting Dr Y's claim that she made the disclosure 'in good faith to a law enforcement officer' who she assumed 'had the authority to request the information', the Commissioner was not satisfied that Dr Y could have formed a reasonable belief that Mr Z posed a serious and imminent threat to himself or public safety at the time of disclosure.

No exception for law enforcement activity

The Commissioner noted that the situation here was factually similar to that in *Jones v Office of the Australian Information Commissioner* [2014] FCA 285 (*Jones*). In that matter, a doctor's disclosure of medical records to police based on a reasonable belief that disclosure was reasonably necessary was not found to be an unlawful disclosure. However, he found that *'EZ' and 'EY'* could be distinguished because, unlike in *Jones*, there was no warrant for the information or evidence to demonstrate that any of the specific law enforcement activities were relevant in this situation.

NPP 2.1(h)(i) relates to 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'.

The Commissioner rejected Dr Y's reliance on NPP 2.1(f) (current s 16A) on the basis that

> 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. ([44])

Similarly, in the absence of a warrant or evidence provided by Dr Y of any legislative provisions that required or authorised disclosure of Mr Z's personal information, the Commissioner was not satisfied that Dr Y could rely on NPP 2.1(g) to say that the disclosure was required or authorised by or under law.

Failure to take reasonable steps to protect personal information from unauthorised access

The Privacy Commissioner also found that Dr Y had breached the requirement to take reasonable steps to protect personal information from misuse and loss and from unauthorised access, modification or disclosure. The Commissioner made it clear that:

> security of personal information does not only relate to physical security, it clearly relates to the steps taken by the holder of the information to ensure it is only disclosed in circumstances that are lawful. ([76])

To meet the requirement to take 'reasonable steps', Dr Y would have needed to:

- question the police officer about his reasons for contacting Dr Y about Mr Z's health
- ascertain if there was a warrant or other relevant legislation that authorised collection and disclosure of the information
- ascertain if the circumstances could constitute a serious and imminent threat to the person or the public
- consider the various policies, guidelines and legal obligations that apply to the disclosure of personal health information. ([76])

Implications for APP agencies

This decision has implications for APP entities dealing with requests from law enforcement bodies. APP 6, which deals with use and disclosure, and APP 11, which deals with security of personal information, impose substantially similar requirements to NPP 2 and NPP 4.

It is not enough to make a disclosure in good faith to a law enforcement officer or assume the officer has the authority to request the information. A person receiving this kind of request would need to make inquiries to satisfy themselves that the disclosure of requested information is authorised.

Inquiries would also need to be made to support disclosure on the basis that the use or disclosure is necessary to lessen or prevent a serious or imminent threat to an individual's life, health or safety or to public health or safety. If the request is made a few days after an event, the imminence requirement may not be satisfied. (Note: the requirement for imminence has been removed from the APPs.)

Security of personal information requirements extend to taking reasonable steps to protect information from unauthorised disclosure. In the context of requests from law enforcement agencies, this includes making inquiries and being satisfied about the law enforcement agency's need to know and right to obtain this information.

For further information please contact:

Charine Bennett
Senior Lawyer
T 02 6253 7264
charine.bennett@ags.gov.au

Jane Lye
Senior Executive Lawyer
T 07 3360 5736
jane.lye@ags.gov.au

Elena Arduca
Senior Executive Lawyer
T 03 9242 1473
elena.arduca@ags.gov.au

Tara McNeilly
Senior General Counsel
T 02 6253 7374
tara.mcneilly@ags.gov.au

Justin Davidson
Senior Executive Lawyer
T 02 6253 7240
justin.davidson@ags.gov.au