

Privacy Commissioner Case Note

Case Citation:

S v Health Service Provider [2008] PrivCmrA 19

Subject Heading:

Failure to keep personal information secure

Law:

National Privacy Principle 4.1 in Schedule 3 of the *Privacy Act 1988* (Cth)

Facts:

The complainant received a medical service from the respondent health service provider and gave the health service provider their x-rays. The complainant later requested the return of their x-rays.

The health service provider forwarded copies of the complainant's medical records and original x-ray films by general post (a postal service that could not track the transmission of items of mail) to another health service provider nominated by the complainant. The original medical records were kept by the health service provider. Two staff members sealed the copies of the medical records and the original x-ray films in an envelope and the health service provider recorded when they were sent. The health service provider also contacted the other health service provider and checked it received the medical records and x-rays.

Issues:

National Privacy Principle 4.1 provides that an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

In deciding what are 'reasonable steps' to ensure data security an organisation must consider a number of factors. For instance, what is reasonable depends on the circumstances in which personal information is held. The sensitivity of personal information stored is also an important factor and higher levels of security could be expected for sensitive information, such as health information.

The issue for consideration was whether the health service provider took 'reasonable steps' to protect the complainant's personal information from loss.

Outcome:

The Commissioner considered whether the steps taken by the health service provider, when it mailed copies of the complainant's medical records and the original x-rays in the general mail to the other health service provider, were 'reasonable' in the circumstances.

As health information, the complainant's medical records and x-rays are sensitive information as defined in the Act, which is generally afforded a higher level of protection than other forms of personal information. The potential harm the

Privacy Commissioner Case Note

complainant would suffer, should the original x-rays be lost in the mail, is significant, given the loss of this record of the complainant's condition would be permanent.

The Commissioner noted that while the health service provider was not a large organisation, the cost of alternative methods to transmit the documents would not be a significant financial burden. The Commissioner also considered the level of risk of the medical records and x-rays being lost in a generally dependable and reliable general mail system. The Commissioner formed the view that the health service provider failed to take reasonable steps to protect the complainant's personal information by using the general mail, in breach of National Privacy Principle 4.1.

The Commissioner considered it appropriate to attempt, through conciliation, to effect a settlement of the matters that gave rise to the investigation. The health service provider agreed to participate in conciliation, following which the Commissioner closed her investigation.

OFFICE OF THE PRIVACY COMMISSIONER

August 2008