



## **Ombudsman Tasmania**

Report into Investigation under section 21 of the *Personal Information Protection Act 2004*

**Mrs A, Mr B and Mrs C and the Glamorgan Spring Bay Council**

April 2018

---

### **Contents**

|                               |    |
|-------------------------------|----|
| Complaint.....                | 1  |
| Declaration by Ombudsman..... | 1  |
| Background.....               | 2  |
| The Medical Records.....      | 3  |
| Current situation.....        | 3  |
| Issues for investigation..... | 4  |
| The Law.....                  | 4  |
| Alleged breach PIPP 2.....    | 7  |
| Alleged breach PIPP 4.....    | 10 |
| Recommendations.....          | 13 |

## **Complaint**

1. I received individual complaints from Mrs A, Mr B and Mrs C concerning the way in which the Glamorgan Spring Bay Council (the Council) had handled their medical records.
2. Mrs A complained to the Council on 25 July 2017 regarding lack of compliance with the *Personal Information Protection Act 2004* (the PIP Act) in that the Council did not seek permission to copy and relocate her and her family's medical records. Not satisfied with the response from the Council Mrs A complained to my office on 25 July 2017.
3. Mr B complained to my office on 4 August 2017 and Mrs C complained to my office on 24 August 2017.
4. Each of the complaints raised substantially the same issues and for the sake of convenience in investigating and reporting the matters, they have been considered together. I will therefore group Mrs A, Mr B and Mrs C together and refer to them as the complainants.
5. After making a preliminary assessment of the complaints pursuant to section 19 of the PIP Act, I determined to deal with the complaint under section 21 of the Act. An investigation has been conducted in accordance with Division 3 of Part III of the *Ombudsman Act 1978* as required by section 21(1) of the PIP Act.
6. The substance of each complaint is that the Council has breached its obligations under the PIP Act by:
  - Arranging for the copying and transfer of medical records to a Council-owned server without the consent of the complainants;
  - Providing for the back-up of medical records to an external server located at the Council municipal offices; and
  - Not taking adequate steps to prevent potential access to the medical records whilst they were backed up to the external server located at the Council municipal offices.
7. The complainants are patients of Dr Pranesh Naidoo. The circumstances which gave rise to the complaints occurred when Dr Naidoo relocated his medical practice to new premises located at 1 Victoria Street, Triabunna on 31 July 2012.

## **Declaration by the Ombudsman**

8. I declare that I am a patient of Dr Naidoo. I am aware that each of the complainants are also patients of Dr Naidoo. Other than having this in common with the complainants I

do not have a particular interest in this complaint and have been able to assess and investigate them in an impartial and objective manner.

## **Background**

*Acknowledgement: This information is largely sourced from the Review of East Coast Health report prepared by consultants Campbell & Jones, completed in September 2013.*

9. From the 1990's Dr Naidoo practiced as 'Spring Bay Medical' under State Government arrangements from a building owned by the Department of Health in Triabunna. The practice received rent-free premises, the use of community nurses and materials at no cost. There was no documentation detailing these arrangements.
10. The Council became involved in discussions about the provision of medical services due to concerns in the municipality regarding the workload for one general practitioner. It was apparent that patients had to travel to Sorell, Richmond and Swansea to access medical services. These discussions commenced around 2005.
11. In 2010, the Council issued a paper outlining its vision for a self-funding and supported health company for the municipality that would be wholly owned by the Council. The company would provide practice management support and employees to all medical practices in the municipality.
12. In 2010, the Council formed a special committee to oversee the realising of the Council's vision for East Coast Health, known as the East Coast Health Committee (EHC).
13. In 2010, Council recruited Dr Johnston to work in Triabunna and he commenced practice in April 2010. Prior to this, the Council contacted Dr Naidoo about possible sharing of staff and resources. Dr Johnson commenced work using Dr Naidoo's original IT infrastructure and software. As conditions were crowded, the Council committed resources to redevelop and equip the premises at 1 Victoria Street, Triabunna as a new site to locate both medical practices.
14. Council's lawyers drafted a Medical Practice Management Agreement, which was given to the EHC to consider. The agreement set out the responsibilities of the practice manager (the Council) and doctor involved.
15. In June 2012, the existing professional practice management company for the medical practice at Bicheno ceased providing services. The Council had discussed its practice management model with practitioners at Bicheno. The Bicheno practice signed the Medical Practice Agreement and the Council employed the practice staff.

16. Dr Johnson signed the Medical Practice Agreement. Negotiations between Dr Naidoo and the Council about the terms and conditions of the Medical Practice Agreement broke down and Dr Naidoo refused to sign the agreement. The Council and Dr Naidoo exchanged letters, both on legal advice but despite without prejudice negotiations were unable to reach agreement.
17. Both Dr Naidoo's and Dr Johnson's practice moved into the new premises on 31 July 2012.

## **The Medical Records**

18. Hypertronics (IT consultants) first provided IT maintenance to Spring Bay Medical Centre in 2006 as Dr Naidoo's private contractor.
19. In March 2010, Hypertronics supplied a laptop computer for Dr Johnson and set up a user account for him to use Dr Naidoo's Medical Director (MD) database.
20. In 2012, Hypertronics was asked by the Council to set up computer equipment at the new premises, including the transfer of the MD database. Hypertronics met with the General Manager of the Council and Mr Hansen (Council's external IT consultant) on 22 May 2012. The brief was to provide the computer hardware and software necessary to support the two doctors from Triabunna, another doctor working in Bicheno plus various administrative staff. Hypertronics submitted a quotation, which would have provided full IT functionality within the new premises with no need to connect to the Council's network. Hypertronics commenced work on 12 July 2012 at the new premises and set up remote access to the MD database for Bicheno staff. The transfer of patient records from the community health centre to the new premises in Triabunna occurred during July 2012.
21. The Council has confirmed that the transfer to the new premises entailed the copying of the database of both Dr Naidoo and Dr Johnson (combined) and combining it with the database for the doctor at Bicheno (Dr Vane-Tempest) to form one database located on the Council-owned server.
22. On 29 May 2012, Hypertronics was copied into an email from Mr Hansen to Mr Metcalf suggesting changes to the configuration it had proposed. A revised quote was submitted and accepted by the Council. The main changes to the scope of work were that a server at the Council chambers would be used for user authentication and the backup files would be copied to another Council server rather than to the tape drive Hypertronics had recommended.
23. It seems it was arranged that from 1 August 2012 to 1 October 2012 an encrypted back up was placed on the council server at municipal chambers for security purposes. The

Council suggests that both doctors knew this, however, there is ongoing dispute about whether Dr Naidoo agreed to this set up. The encrypted back up arrangement ended when Dr Naidoo raised issues with the Council and via the ECHC in relation to the practice.

24. From July 2012, the patient records of both doctors were stored on a new Council owned server and infrastructure but the Council asserts it had no access to this system.
25. Hypertronics advises that on 3 June 2015 it received an email from Mr Phil Pyke (Practice Manager employed by the Council) to provide a backup of the shared patient database to be picked up by Mr David Metcalf the General Manager for the Council. It was Hypertronics' understanding that the backup was to be used to import the data into a new 'Best Practice' database to be used at Bicheno. The Council advised that the subsequent transfer of patient records to the Bicheno practice was carried out by ITB Computing, which was engaged by the Council.

### **Current situation**

26. The practices associated with East Coast Health, a trading name owned by the Council, are the Bicheno General Practice and Dr Winston Johnson.
27. East Coast Health operates Dr Johnson's practice out of the building at 1 Victoria Street, Triabunna. The Council owns the building and IT equipment. There is a practice management agreement in place with the Council. Only Dr Johnson's patient records are held on a Council owned server.
28. Dr Naidoo operates his medical practice, Spring Bay Medical, from the Council owned premises and IT infrastructure located at 1 Victoria Street, Triabunna. There is no practice management agreement in place and Dr Naidoo operates independently of the Council. Dr Naidoo has retained the combined database on a Council owned server.
29. The Bicheno practice runs from a Council owned medical centre. Since 11 June 2015, it has operated on an independent server.

### **The Law**

30. The relevant legislation in Tasmania is the *Personal Information Protection Act 2004* (PIP Act).
31. The PIP Act defines "personal information custodian" which includes a public authority. A public authority has the same meaning as provided for in the *Right to Information Act 2009*. By definition, the Council is a personal information custodian.

32. For the purposes of the PIP Act, health information about an individual is considered 'sensitive information'. Therefore, the patient records are by definition sensitive information.
33. Section 17 of the Act specifies that a personal information custodian must comply with the personal information protection principles (PIPP).
34. The making of complaints is covered by Section 18, which states that 'a complaint may be made by a person in relation to the alleged contravention by a personal information custodian of a personal information protection principle that applies to the person.'
35. The relevant PIPP's can be found in Schedule 1 of the PIP Act as follows:

## **2 Use and Disclosure**

- (1) A personal information custodian must not use or disclose personal information about an individual for a purpose other than the purpose for which it was collected unless –*
  - (a) both of the following apply:*
    - (i) that purpose is related to the primary purpose and, if the personal information is sensitive information, that information is directly related to the primary purpose;*
    - (ii) the individual would reasonably expect the personal information custodian to use or disclose the information for that purpose; or*
  - (b) the individual has consented to the use or disclosure;*

## **4 Data security**

- (1) A personal information custodian must take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure.*
- (2) A personal information custodian must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.*
- (3) A personal information custodian, the records of which are subject to the Archives Act 1983, must take the reasonable steps referred to in subclause (2) only with the approval of the State Archivist.*

In dealing with a complaint under section 21 of the PIP Act, an investigation is to be conducted in accordance with Division 3 Part III of the *Ombudsman Act 1978*.

## **Issues for investigation**

36. The issues raised by the complainants are:
  - Did the creation of a shared database by the Council and its subsequent transfer from one server to another constitute a breach of Personal Information Protection Principle (PIPP) 2 Use and Disclosure?

- In organising patient records to be backed up/stored on a server at its municipal chambers did the Council breach PIPP 2 Use and Disclosure?
- Did the Council breach PIPP 4 Data Security by not taking adequate steps to protect the personal information from misuse, loss, unauthorised access, modification or disclosure?

## **PIPP 2 – the Law**

37. There is scant case law on the PIP Act in Tasmania but there is some guidance provided by commentary, legislation and decisions in other jurisdictions.

### ***PIPP 2 Use and Disclosure***

38. The Australian Privacy Principle (APP) guidelines of the Office of the Australian Information Commissioner (OAIC) consider the key points of APP 6 Use and Disclosure. APP 6 contained in the *Commonwealth Privacy Act 1988* is almost identical to PIPP 2 in that an entity can only use or disclose personal information for a purpose for which it was collected. The term 'use' is not defined in the *Commonwealth Privacy Act 1988* or the PIP Act. The OIAC considers that an entity uses information where it handles or undertakes an activity with the information, within the entity's effective control. One example is the entity passing the information from one part of the entity to another.
39. The OAIC key points discuss that in limited circumstances, providing personal information to a contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure. This occurs where the entity does not release the subsequent handling of personal information from its effective control. For example, if an entity provides personal information to a cloud service provider for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a 'use' by the entity in the following circumstances:
- a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes;
  - the contract requires any subcontractors to agree to the same obligations; and
  - the contract gives the entity effective control of how the information is handled by the provider. Issues to consider include whether the entity retains the right or power to access, change or retrieve the information, who else will be able to access the information and for what purposes, the security measures that will be used for the storage and management of the personal information and whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.
40. In addition, sensitive information is generally afforded a higher level of privacy protection under the APPs than other personal information. This recognises that inappropriate

handling of sensitive information can have adverse consequences for an individual or those associated with the individual. Mishandling of sensitive information may also cause humiliation or embarrassment or undermine an individual's dignity. This is also reflected in the PIP Act.

41. The APP 6 guidelines provide that 'there must be more than a tenuous link' in terms of the use being related to the primary purpose. The 'reasonably expects' test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances.
42. The OIAC suggests that a directly related purpose is one that is closely associated with the primary purpose, even if it is not strictly necessary to achieve that primary purpose. An example of directly related purpose in the context of sensitive information would be for the purpose of de-identifying the information. The OIAC cites that an example where an individual may reasonably expect their personal information to be used would include normal internal business practice such as auditing, planning or de-identifying personal information.

## **Alleged breach of PIPP 2 – Use and Disclosure**

43. In this case, the complainants alleged a breach of PIPP 2 on the basis that the Council arranged for the copying, transfer and backup of medical records (which are classed as sensitive information) to a Council owned server without the consent of the complainants.
44. It is noted that ordinarily records containing patient medical information do not belong to the patient, however, the patient has a legal right to access those records<sup>1</sup> and this is enshrined in the PIP Act. In the context of this complaint, the medical records remained the property of the medical practitioners involved. There was no legal requirement for the Council to obtain consent to transfer the medical records. The Council maintained an interest in the transfer and storage of the medical records due to its involvement in negotiating the arrangements for the management and delivery of general practice services to the municipality.
45. The determination of whether or not a breach of PIPP 2 has occurred depends on the circumstances of each case. The circumstances the subject of complaint are noted as somewhat unusual in that a private medical practice was operating with assistance from the Council which, by virtue of the definition in the PIP Act, is a personal information custodian.
46. Specifically, the complainants allege that the Council has breached PIPP 2 in that:

---

<sup>1</sup> AMA Transfer of Medical Records – A guide

- it created a shared database of patient records and it arranged the transfer of those records from one server to another; and
  - From 1 August 2012 to 1 October 2012 an encrypted back up of those records was stored electronically on a server at its municipal chambers.
47. The relevant exceptions to PIPP 2 are outlined at paragraph 35.
48. In *B v Hotel*<sup>2</sup> the Privacy Commissioner considered the concept of primary purpose. In this case, a hotel had disclosed an individual's name to a third party in a situation where some garments left at the hotel belonged to the third party who shared the same name as the complainant. The Commissioner formed the view that the disclosure of the complainant's personal information did not appear to be consistent with the primary purpose for which the information was collected and none of the exceptions listed in National Privacy Principle (NPP) 2.1<sup>3</sup> applied to permit the disclosure.
49. The case of *N v Commonwealth*<sup>4</sup> considered the link between the purpose and use of information. The complainant had lodged several complaints against the agency relating to their conditions of employment. The agency engaged a contractor to investigate its handling of the complainant's various complaints, and in doing so gave the contractor a copy of the complainant's personnel and related files. The Commissioner was satisfied that the agency's collection of personal information in the personnel and related files was for the purpose of administering the complainant's employment. As the contractor was engaged to investigate complaints about the complainant's working conditions, the Commissioner considered the use to be directly related to the administration of the complainant's employment. Therefore, the Commissioner was of the view that the agency's use of the complainant's personal information was permissible.
50. The case of *F v Medical Specialist*<sup>5</sup> considered the concept of reasonable expectation. The circumstances involved a consultant medical practitioner disclosing information about the complainant's treatment needs and the consultant's reasons for refusing to accept the complainant as a patient to the medical clinic manager. It was found that the disclosure of the complainant's personal information to the clinic manager was both directly related to the purpose for which the information was collected, and was within the complainant's reasonable expectations.
51. Similarly, in *IR and NRMA Insurance, Insurance Australia Limited*<sup>6</sup> a joint policy holder of the complainant was provided with a Certificate of Insurance, which included a detailed list

<sup>2</sup> [2008] PrivCmrA 2

<sup>3</sup> The NPP's were replaced by the APP's in March 2014

<sup>4</sup> [2009] PrivCmrA 17

<sup>5</sup> [2009] PrivCmrA 8

<sup>6</sup> [2016] AICmr 37 (27 June 2016)

of all of the assets owned by the policy holder. The Commissioner found that the connection between disclosing the full extent of information about the complainant's other policies, such as the detailed information about the assets to which the policies related, to Ms X was tenuous. The Commissioner observed, "In my view providing on a certificate of insurance a detailed description of assets that are unrelated to the policy for which a certificate is issued, is not consistent with the notice provided in the PED guides about what information to expect on a certificate of insurance. There is no information before me to suggest that the complainant should have reasonably expected that descriptions about other assets unrelated to the policy in respect of which the Certificate was issued would be disclosed to the extent they were".

52. It is clear from the facts that the Council arranged for the creation of the shared database, its subsequent transfer and for the encrypted backup to be made. It did this in consultation with its own IT contractors. Based upon the considerations and decisions above, in my assessment the Council has used the medical records but not disclosed them<sup>7</sup>. Whether that use is permitted, requires consideration of the exceptions under PIPP 2, which are expressed in the PIP Act in the alternative.
53. It is clear from the complaints and responses from the Council that there was no consideration given to seeking consent from patients prior to the creation of a shared database and the transfer of the medical records from one server to another. However, consent is one of the exceptions provided for in PIPP 2. The fact that the Council did not seek the consent of the complainants does not preclude the other exception to PIPP 2 regarding primary purpose and reasonable expectation.
54. For the other exception to PIPP 2 to be established, it has to be demonstrated that the use of the information is directly related to the primary purpose and the individual would reasonably expect the personal information custodian to use the information in that way.
55. In general, the primary purpose of medical records is to facilitate patient care and allow the medical practitioner to continue the management of the patient. However, I consider that it is commonly known that electronic medical records are prevalent in medical practice and that the way in which those records are handled in terms of their storage is a use directly related to the primary purpose.
56. Accepting that the primary purpose of the medical records is related to patient care and management, it also follows that it would be reasonably expected that management would include the way in which patient information is copied and stored. It seems within the bounds of reasonable expectation that in the event that a medical practice was closing or moving premises that the transfer of medical records would normally occur. The transfer of the patient records is similar to the example in the APP 6 guidelines of the de-identifying of information. It is proposed that in this context the transfer of a

---

<sup>7</sup> See OAIC Key Points summary at paragraph 38

database is part of normal internal business practice and directly related to the primary purpose for which the information was collected.

57. Presumably, it was widely known that the medical practice of Dr Naidoo was relocating to new premises and accordingly it would be reasonably expected that the management of the move would include arrangements for the transfer of the medical records. The evidence shows that considerations for the IT set up at the new premises fell to the Council. There is dispute about whether this was explicitly agreed by Dr Naidoo however, that is not directly relevant to compliance with the PIP Act.
58. In summary, it is acknowledged that Dr Naidoo collected the medical records of the complainants for the purpose of providing a health service, however, the copying and movement of those records by the Council is directly related to that purpose. In applying the 'reasonably expects' test I find that arrangements for the transfer and storage of the records by the Council would be expected in the circumstances. For this reason, whilst I do find that the Council used the information, it did not breach the provisions of the PIP Act. This allegation is therefore unsubstantiated.

#### **PIPP 4 Data Security – the Law**

59. Again, there is no particular guidance in relation to Tasmania however, PIPP 4 is almost identical to APP 11 and provides that a personal information custodian must take reasonable steps to protect the information it holds from misuse, loss, unauthorised access, modification or disclosure.
60. The reasonable steps that an entity must take depend on the circumstances of each case but would include consideration of the sensitivity of the information, the possible adverse consequences in the event of a breach and the practical implications of implementing security measures.
61. The OIAC has commented that reasonable steps should include implementing strategies in relation to the following:
  - governance, culture and training;
  - internal practices, procedures and systems;
  - ICT security;
  - access security;
  - third party providers;
  - data breaches;
  - physical security; and
  - standards.

62. The terms 'misuse', 'interference', 'loss', 'unauthorised access', 'unauthorised modification' and 'unauthorised disclosure' are not defined in the PIP Act and analysis must draw on the ordinary dictionary meaning of the terms.

### **Alleged breach of PIPP 4 – Data Security**

63. The allegation is that the Council did not take adequate steps to prevent potential access to the medical records whilst they were backed up to the external server located at the Council municipal offices and because the network at the East Coast Health (ECH) building shared connectivity to the Council municipal offices. It has been suggested by the complainants and Dr Naidoo that the records were susceptible to unauthorised access during this period. There is no evidence of any actual misuse, loss, unauthorised access, modification or disclosure. The question for consideration is therefore whether the Council took reasonable steps to protect the patient records from misuse, loss, unauthorised access, modification or disclosure.
64. The Information Commissioner has also considered these concepts in the following cases:
65. *LB and Comcare*<sup>8</sup> concerned the publication of a redacted Comcare Report, which contained the complainant's personal information, including health information that was not properly de-identified and was published on Comcare's website. The Commissioner found that Comcare improperly disclosed the complainant's personal information including sensitive health information in breach of IPP 11, and interfered with the complainant's privacy in that regard. The Commissioner further found the redacted Comcare Report included the complainant's sensitive health information, which deserves a higher level of protection than non-sensitive information. The Commissioner said "It seems in this case that the person responsible for publishing the documents online inadvertently overlooked the personal information. I consider that it would have been reasonable for Comcare to ensure the removal or de-identification of all of the complainant's health information from the report prior to making it publicly available on its website. This could have been achieved by second and third tier reviews to ensure inadvertent mistakes such as this one were not made."
66. The case of *HS and AMP Life Ltd*<sup>9</sup> considered what constituted reasonable steps to protect personal information held by an agency. In this case, the complainant's tax file number was disclosed to a third party by AMP. AMP had stated that its *practice* is 'to request that any financial documentation provided has the tax file number redacted/blacked out, and any documents received by AMP and held on AMP's files has this information blacked out' and its submission that it is 'unable to confirm whether the tax file number had been

---

<sup>8</sup> (Privacy) [2017] AICmr 28 (24 March 2017)

<sup>9</sup> [2015] AICmr 81 (17 December 2015)

blacked out in the taxation documents which were provided to FOS'. The decision states, "that, at a minimum, 'reasonable steps' to secure information' would be for AMP to take proactive steps to ensure its information handling practices are understood and implemented. It was found that AMP did not have processes in place to ensure that what it says is its own practice was followed, and indeed, those practices were not followed in this case. This indicates that AMP did not take reasonable steps to secure the sensitive information it had collected". Therefore, a breach of NPP 4 was established.

67. The Council does not dispute that it arranged for the backup of patient records to a server at its municipal offices. It also does not dispute that there was connectivity between the Council offices and the East Coast Health building via a roof top wireless link. The evidence suggests that the reason for connecting the two networks was to reduce the setup costs by utilising some of the Councils existing infrastructure. I consider this a reasonable approach in terms of the business arrangements for East Coast Health.
68. The Australian Medical Association Guidelines for Providing Patient Access to Medical Records in the context of electronic medical records says that appropriate security measures include adopting policies, procedures and safeguards that help maintain confidentiality, integrity and availability of information.
69. As far as the connectivity between the two networks, the advice from the Council's IT provider is that communication was limited to login authorisation, email and telephone traffic. It is apparent that the server at East Coast Health was password protected with at least two levels of security in that all users had individual logins and passwords. The advice also commented that any network connected to the internet cannot be said to be 100 per cent secure.
70. It is apparent that the domain administrators, presumably the Council as owners of the infrastructure, could potentially access the East Coast Health server. There is no evidence that there has been any unauthorised access and the Council has rejected the possibility that there was ever any unauthorised access. The advice from Hypertronics is that the Medical Director software was set up at the new premises to require username/password combination authentication to gain access. In this context, the security set up appears to be reasonable.
71. The issue of the encrypted back up of records to the server at the Council offices is no longer contentious because the practice has been discontinued. However, the advice I have received in the course of my investigation is that an encrypted back up offers the highest level of security and that an individual would have to go to extraordinary lengths to extract any data. Again, applying the 'reasonable steps' test this appears to be an appropriate level of security in the circumstances.

72. The information provided by the IT contractor and the Council is that all IT staff sign confidentiality agreements. In my opinion, this constitutes reasonable action in terms of protecting the information from possible unauthorised access by external contractors.
73. I note the OIAC guidelines for APP 11 Security of Personal Information have identified that reasonable steps should include implementing strategies for governance, culture and training, internal practices, procedures and systems, third party providers and physical security.
74. I note in the context of arrangement for third party providers that the Better Practice Guide 'Privacy and Cloud Computing for Australian Government Agencies' established by the Information Management Office suggests that the most straight forward way to ensure a cloud service complies with the *Privacy Act 1988* is to get a provider to acknowledge in its contract that it will comply with the APP's.
75. In summary, I am satisfied that the Council has not breached PIPP 4 because it has taken reasonable steps to protect the personal information from misuse, loss, unauthorised access, modification or disclosure. This allegation is therefore unsubstantiated.
76. Although I have found no breach of PIPP 4, I have further considered the steps taken by the Council to implement strategies for governance, standards and policies around privacy as outlined by the OIAC, the AMA Guidelines and the Better Practice Guide of the Information Management Office.
77. It is apparent that the Council did not turn its mind to any consideration of the requirements of the PIP Act during the copying, move or back up of the medical records. Further, the confidentiality agreement that the Council had in place with its IT contractor does not refer directly to the requirements of the PIP Act.
78. As far as its privacy policy is concerned the Council currently refers to the PIP Act in the context of its Customer Service Charter as follows:

**PERSONAL INFORMATION PROTECTION**

*Council has a commitment to protection of Personal Information provided by a customer to Council in accordance with the requirements of the Federal Privacy Act 1988 and the Personal Information Protection (PIP) Act 2004 (Tas). The Tasmanian PIP is available on [www.thelaw.tas.gov.au](http://www.thelaw.tas.gov.au)*

79. During this investigation, the Council did not provide any evidence that it had considered its role as a personal information custodian within the meaning of the PIP Act. The statement above indicating a commitment to protection of personal information whilst indicative of written commitment to personal information protection was not fully demonstrated by the Council in light of the factual situation which gave rise to these

complaints. Indeed, it is evident that the Council does not currently have a written policy documenting its management of personal information. This is a technical breach of PIPP 5 of the PIP Act.

80. Whilst I am satisfied there has been no breach of PIPP 4 nonetheless, I make the following recommendations which I believe will improve the Council's governance of these matters:
81. **Recommendation 1:** Any contracts and confidentiality agreements signed by Council contractors be amended to specifically make reference to the requirement to comply with the PIP Act and the PIPP's.
82. **Recommendation 2:** The Council consider an updated and improved privacy statement.
83. In relation to the breach of PIPP 5 I make the following recommendation:
84. **Recommendation 3:** The Council implement a separate Personal Information Protection policy to comply with the PIP Act, namely PIPP 5 – Openness, which provides that a custodian must clearly set out in a document its policies on its management of personal information and must make the document available to anyone who asks for it.



---

**Richard Connock**  
**Ombudsman**

