16 March 2011

Situation Report - Breach of Privacy, Disclosure of Claims Data

Chronology of events

1.0 Breach of Privacy

1.1 On 5th August 2011, an ACC manager within the Recover Independence Service (RIS), during normal communications with an Auckland client, mistakenly included in an email, a file which contained information about other ACC clients.

1.2 The information related to the review status with Dispute Resolution Services Limited (DRSL) of approximately 6,752 clients. The details did not include any specific information such as payments made, or any treatment, rehabilitation or case history with ACC.

1.3 The spreadsheet was a management report issued to ACC offices on a monthly basis listing the numbers of reviews and outcomes of those reviews over the past 12 months. Three worksheets at the end of this spreadsheet listed the individual reviews, including the client name and claim number. The ACC office in which the claim was held is listed and some of these claims (131) were shown against the Sensitive Claims Unit (SCU).

1.4 The file did not contain any information on personal claim histories or claim detail. It was in spreadsheet form and included:

- Review lodgement date
- Client name
- File reference number
- Branch identification
- Review category (e.g. weekly comp, cover, vocational independence etc)
- Review outcome (e.g. upheld, quashed, withdrawn etc)

1.5 The client who received the file contacted an ACC Board member to discuss matters pertaining to her specific case. No specific reference was made to the data held or the breach of privacy. As is normal practice the Director referred the matter to the Chairman, who in turn referred the matter to senior ACC management, who confirmed the matter would be dealt with at an operational level.

2.0 Notification of alleged Privacy Breach

2.1 ACC was notified of the alleged breach on 1 December, when two senior managers met with the recipient of the information to discuss the recipient's individual case.

2.2 During this meeting the client who had received the information advised that she had been sent a document by ACC which contained a list of ACC clients. No specific details were provided other than confirmation that the information had not been provided to any one else. The client said that the information she had received had been included in an email sent to her by one of the ACC managers attending the meeting. The client did not identify who from ACC had sent her the email containing the incorrect information.

2.3 The ACC manager at the meeting;

- Stated that the client would be breaching the individuals' privacy if she acted upon the information

and

- That the information must be returned to ACC and that any other copies held must be destroyed or deleted electronically

2.4 At the same meeting the client proposed that in relation to her own individual case she would like to negotiate a guaranteed benefit payment for two years. She made threats that if her demands were not met she would not return the information and she would inform the media of the alleged privacy issue.

2.5 Given the serious nature of the alleged breach and the presence of a threat, the details should have been escalated to senior ACC management at that time and the police advised.

3.0 ACC Response to Notification of alleged Privacy Breach

3.1 ACC wrote to the client requesting the information alleged to be held by the client be returned;

"At the meeting you stated that you were in possession of information sent to you by ACC that made reference to other clients. You did not elaborate what that was. I asked at the meeting that this information be returned to ACC and that any copies you may have of that information is destroyed or deleted electronically. I would therefore appreciate that you return this information to ACC and give me your assurance that you or anyone else do not have copies of the information referred to."

3.2 The client who had received the information incorrectly advised staff that the information had been received in an email from one of the managers attending the December meeting. In fact the information had been sent in August by an ACC staff member who was not at the meeting. The result of this was that when an email sweep was made of the email records of the managers attending the meeting, no information was found to support the client's claim.

4.0 Media Request

4. 1 A media request was received on Friday the 9th March 2012 from the Dominion Post.

4.2 The ACC Media officer gave the information request to ACC's Privacy Officer, copying in the Head of Communications, the Chief Executive and the Ethics Officer.

4.3 The senior manager who attended the December meeting was contacted and they advised that an allegation had been made, but no formal privacy complaint lodged. A sweep of his email had been completed but nothing found. A request for the return of the alleged information had been made.

4.4 A response was provided to the Dominion Post enquiry.

5.0 Dominion Post Article

5.1 The article (Appendix 1) appeared in the DomPost on Tuesday 13th March 2012 providing specific details relating to the client who was the recipient of the breach.

6.0 ACC Actions taken

Tuesday 13th March

6.1 The Minister and Chairman were advised of the article.

6.2 The client's lawyer was contacted and requested to advise their client that the information and any copies, electronic or otherwise, must be returned immediately or proceedings would be issued.

6.3 Assurances were quickly received that the information had been destroyed and that an independent third party had removed all related computer records from the client's computer. Third party confirmation has been sought to confirm that the client's computer has been cleaned.

6.4 Confirmation from the Chairman was received that no directors were aware of nor had been advised of the breach prior to the media announcement.

6.5 The Privacy Commissioner was advised of the breach. A meeting was held and suggestions discussed on an effective review of the ACC privacy process that could be conducted in conjunction with the Privacy Commissioner, an independent third party and ACC.

6.6 A situation report was requested from the senior ACC manager who was present at the December meeting with the client.

6.7 A media statement was released, confirming the breach had been made, the data had been recovered and that all affected clients would be contacted to confirm that their individual details had now been safe guarded.

6.8 An 0800 number was established to take incoming calls from clients concerned about the breach.

6.9 Call centre hours were extended to allow phone calls to be made to each of the 6,748 clients affected. Where contact can not be made by phone a letter will be sent and an apology letter for affected clients will follow the phone calls.

7.0 The police were contacted regarding the meeting with the client in December and the threat made.

7.1 All ACC staff were advised of the breach.

7.2 The data was a standard management report in which it was possible to connect the classification Sensitive Claims Branch with an individual client name and reference number. The report has now been changed to remove this connection to further protect the privacy of Sensitive Claims clients.

Wednesday 14th March

7.3 ACC Audit and Risk Committee convened and are briefed on the privacy breach.

7.4 Decision taken to appoint an independent auditor to review the privacy management process and to work closely with the Privacy Commissioner to ensure a co-ordinated and complete report is completed as soon as possible. Management were requested to develop and repeat privacy training and awareness throughout the Corporation.

7.5 Privacy Commissioner acts to post information on the website of the Privacy Commissioner with information for clients concerned about the breach

7.6 ACC at the direction of the Audit and Risk Committee will revisit, re-establish and repeat our privacy workshop and training modules on for all ACC staff.

Thursday 15th March

7.7 Calls to affected clients continue. The following table explains the situation as at 10:00am Thursday, 15 March.

		Totals
1.	Total clients to contact	6752
2.	Attempted to contact	4457
3.	Successfully contacted	2611
4.	Unsuccessful	1846

7.8 ACC is continuing to call clients who were on the spreadsheet to advise them of the breach and to apologise. Following contact, a letter confirming the breach and apologising further is being sent, although many people have advised they do not wish to receive the letter as they are comfortable with the phone call.

7.9 A business process was drafted to support the call scripting and 'Q&As' that were developed. This was intended to provide some consistency in logging details of the calls in Eos and reporting. It also provides staff with instructions to validate the client's identity and manage unsuccessful contact attempts. The process is being updated as necessary.

7.10 Planned system outages have been postponed so that ACC staff can work later into Friday evening and on Saturday.

7.11 Management protocols have been reviewed and amended to document and communicate the need to refer all privacy breaches to both the ACC Privacy Officer and the relevant ACC General Manager.

Next steps

We understood from the client that she had sent a copy of the spreadsheet to the State Services Commission, the Office of the Privacy Commissioner, and the Office of the Ombudsmen. As at the date of this report, all three agencies had confirmed they had not received the information, but would return it to ACC if located. We are continuing to pursue this with them daily.

A further meeting has been held with the Privacy Commissioner and it has been agreed that a joint Terms of Reference will be developed for a review of ACC's privacy procedures. The draft TOR is to be prepared by Friday 23 March.

An all staff communication will be sent from the Privacy Officer today, advising that we are looking at some long term solutions to assist with protecting the information in our care. It will include the following messages

> ***There are some short term things that we can all do that will help:***
> - ***One thing at a time - as a work habit, ensure that you only have one piece of work on your desktop or on your screen at any one time. Make sure everything is closed down when you have finished working on that item before you begin or open a new work task.***
>
> - ***Best practice says that if we have a spreadsheet with sensitive information on it, we should password protect it.***

Privacy at ACC

ACC believes the privacy of client records is of paramount importance.
The measures the Corporation has in place to safeguard client privacy include:

- ACC has a strong focus on it's obligations under the Privacy Act and the Health Information Privacy Code. ACC has designated Privacy Champions throughout the country, who monitor and promote best practice of personal information.

- In 2011 ACC's Government Services team, in conjunction with our Claims Management division provided a series of training workshops for Managers and Privacy Champions across the county. This initiative was endorsed by the Office of the Privacy Ccommissioner in July last year. I have attached a copy of this for your quick reference.

- Privacy Act training is a mandatory part of the standard staff induction training package. Where mistakes are made by staff, every effort is made to not only rectify the situation but find ways to prevent or minimise the same mistakes being made again.

As stated above ACC is entering into a joint review with the Office of the Privacy Commissioner and an independent auditor to fully review ACC's privacy procedures.

Appendices

1. Dominion Post Article, Tuesday 13 March

The Dominion Post
Tuesday, March 13, 2012
Page : 1
Section :
Edition :
Region : New Zealand Metropolitan

Page : 1 o
Circulation : 98,3
Area Of Clip : 421.39 sq
Clip ID : 3715

ACC EMAIL ERROR

Privacy breach on 9000 claims

Phil Kitchin
INVESTIGATIONS EDITOR

PRIVATE details of more than 9000 ACC claims – some featuring well-known people – have been emailed to a person who should not have received them, in what is being described as one of the worst privacy breaches in New Zealand history.

The details included personal information on nearly 250 clients from ACC's most secure unit – the sensitive claims unit. Full names, the nature of each claim and dispute, and individual claim numbers were among the information revealed.

Senior management at ACC were told three months ago that they had possibly made the biggest privacy breach in New Zealand history, but they have made no effort to investigate or contain the breach with the recipient.

Some of the names in the huge files were public figures, the recipient said, and they also included victims of violent and sexual crimes. Without going through all the files, the recipient recognised at least 10 people on the lists.

The sensitive claims unit is a special unit containing ACC's most sensitive claimants, including sexual abuse and rape victims.

Before the warning to ACC management, ACC's board and former ACC minister Nick Smith were told about systemic failures of the corporation's processes for respecting the privacy rights of claimants.

The board was given an example of a branch medical adviser who covertly communicated with an ACC assessor providing false information to manipulate a medical report in ACC's favour.

A board member was sufficiently alarmed by the allegations to raise the matters at a higher board level, which

The Dominion Post
Tuesday, March 13, 2012
Page : 1
Section :
Edition :
Region : New Zealand Metropolitan

Circulation : 98,326
Area Of Clip : 421.39 sqcm
Clip ID : 3715919

resulted in a meeting between the recipient of the information and ACC management in December.

At that meeting, the recipient and their advocate told ACC's national manager of recovery independence services, Philip Murch, that ACC had potentially caused the biggest privacy breach in New Zealand's history.

ACC was told that its own staff emailed the recipient sensitive details of thousands of claims, which could result in thousands of complaints because of incompetent privacy management practices. ACC was told it would be horrified to know what material it had fired off.

But in spite of the general warning to the board and the explicit disclosures in December – including a formal written complaint – ACC management have not investigated the privacy breach with the recipient.

The same details also appear to have been sent to more than 50 ACC managers, most of them not from the sensitive claims unit, raising questions about the security of information supplied to the unit.

Personal information held by the unit is not supposed to be divulged to anyone outside the unit without the permission of the client.

The recipient, an ACC client, did not want to be named because they feared being swamped by telephone calls from other ACC clients concerned their details have been distributed nationwide.

The recipient blacked out all personal details of claimants when providing documents to *The Dominion Post*.

Privacy Commissioner Marie Shroff said if the emailed data involved personal details of thousands of people the breach was likely to be one of New Zealand's most serious.

She expected government agencies to adhere to her office's notification guidelines, which include contacting those whose privacy has been breached, getting the information back, minimising harm and making sure it did not happen again.

New Zealand laws are behind other jurisdictions in not providing for mandatory reporting of data privacy breaches and her office is developing a view on the need for there to be consequences for data breaches.

An ACC spokeswoman said the corporation took all privacy complaints "extremely seriously" but it had received no formal complaint.

ACC had implemented several safeguards to "ensure all client information is protected and managed correctly".

In 2010, ACC apologised after it admitted sending up to 2000 companies private information about workers' accidents that should have gone to other employers.

The information included names, descriptions of accidents, injuries, treatment and ACC payments.

A Petone business owner blew the whistle after she was sent private details about a Whanganui man she did not know, who had suffered a fall.

phil.kitchin@dompost.co.nz