Independent Review of ACC Privacy and Security of Information

23 March 2012

Contents

1.1	Background	1
1.2	Roles and Responsibilities	1
1.3	Review Objectives	2
1.4	Review scope and approach	2
1.5	Review protocols	5
1.6	Review timing	5
1.7	Review deliverables	6

1.1 Background

The Accident Compensation Corporation's (**ACC**) Board and Office of the Privacy Commissioner (**OPC**) have requested an independent review of ACC information security policies and practices as a result of an incident that occurred in August 2011.

On 5 August 2011, an ACC manager within the Recovery Independence Service (**RIS**) Team, during normal communications with an Auckland client, included in an email, a spreadsheet containing information about other ACC clients.

The information related to the review status with Dispute Resolution Services Limited (**DRSL**) of 6,748 ACC Clients.

ACC was notified of the alleged breach on 1 December 2011, when two senior area managers met with the recipient of the information to discuss the client's individual case. During the meeting on 1 December 2011 the client who had received the information advised that she had been sent a spreadsheet by ACC which contained a list of ACC clients.

In March 2012 ACC consulted with the OPC around the breach which appeared to have contravened the Privacy Act 1993. ACC proposed to contract an appropriate and independent organisation to conduct an investigation into the circumstances of the privacy breach.

Further discussions resulted in ACC's commitment to extend the investigation to encompass ACC's overall information policies and practices to assess the adequacy of ACC in complying with the relevant Legislation and Codes of Practice in the health sector.

In conjunction with the OPC, the ACC Board has commissioned KPMG and Integrity Solutions Pty Limited (**IIS**) led by Mr Malcolm Crompton to conduct an independent review around the circumstances of the breach and the overall information security policies and practices at ACC.

1.2 Roles and Responsibilities

(i) The OPC will:

- In conjunction with the ACC Board, commission the independent review
- Approve the Terms of Reference for the independent review
- Participate in the selection of independent third party(s) to complete the independent review
- Appoint an OPC representative to act as an observer on the Steering Group
- Receive the final report and provide comments on the findings and recommendations.

(ii) The ACC Board will:

- In conjunction with the OPC, commission the independent review
- Appoint the Chair of the Audit and Risk Committee and Chief Executive to the Steering Group
- Approve the Terms of Reference for the independent review
- Receive and act on the independent review findings and recommendations.

(iii) Independent Parties (KPMG and IIS) will:

- Provide input to the development of the Terms of Reference for the independent review
- Complete/undertake the independent review, documenting all findings and making recommendations as required to the OPC and the ACC Board
- Participate in the Steering Group.

1.3 Review Objectives

The objectives of the independent review are to:

1 Investigate the circumstances of the privacy breach including the cause(s) and the ACC's response.

2 Determine if ACC's policies and practices relating to security of information are:

- Appropriate (including comparability with private sector practices, consistent with good practice in the public sector and the health sector, appropriateness in terms of the risk related to the nature of the client data/information maintained by ACC)
- Effective (in the context of addressing staff and clients need for access to information, maintaining confidentiality and privacy, communication, compliance, monitoring and culture of the organisation).

3 Make recommendations to the OPC and the ACC Board to restore and increase public confidence in ACC's current and future client information handling policies and processes.

1.4 Review scope and approach

The scope of the independent review, in conjunction with the mandatory requirements of the Privacy Act 1993, Health Information Privacy Code 1994 (including the Health and Disability Code of Practice), will involve three coordinated and concurrent work streams:

1 Investigation of the unauthorised release of information by RIS Team and subsequent actions.

2 An assessment of ACC's policies, processes, culture and practices to manage client information.

3 An assessment of ACC's privacy and security policies, practices, processes, staff training and safeguards (as they relate to client information and sensitive claims) including both IT and physical security.

At the completion of the independent review, a written report will be produced on the findings along with any relevant recommendations to enable ACC to better comply with best practice policy and processes, together with requirements of the Privacy Act 1993, the Health Information Privacy Code 1994 and/or relevant codes of practice.

1.4.1 Work Stream One – Auckland privacy breach

Work Stream One will involve an investigation into the circumstances of the privacy breach by RIS Team on or about 5 August 2011, specifically to:

- Ascertain the cause of the information release by RIS Team to an ACC client.
- Assess the privacy practices used or other steps taken at RIS Team for or related to the management of information covered by the Privacy Act 1993, including without limitation, their effectiveness in achieving compliance with the Privacy Act 1993 or recognised Health Sector practices relating to client (patient) information.
- Assess ACC's response or actions taken upon being made aware of the privacy breach:
  - (i) On or after 5 August 2011; *and*
  - (ii) On or about 1 December 2011; *and*
  - (iii) In March 2012.

1.4.2 Work Stream Two – Privacy management policies, processes and practices

Work Stream Two will contribute to the assessment of ACC's policies and practices relating to the privacy of information by a review of:

- Roles and responsibilities relating to the security and privacy of client information
- Policies and procedures relevant to the information held by ACC
- Information collection practices
- Access to and correction of information
- High profile claims management (i.e. sensitive claims and other high profile individuals)
- Compliance with relevant legislation and Codes of Practice
- Approach to staff training in privacy and security
- The strength of the staff culture and attitude to privacy and security.

1.4.3 Work Stream Three – Security

Work Stream Three will contribute to the assessment of ACC's policies and practices relating to security of information by a review of:

- The overall security governance
- Operational security considerations and practices
- Technical security considerations and practices
- Third party management of ACC and client information
- Internet communications and accessibility
- Mobile computing usage including portable data
- Systems development considerations including testing
- Data transfers by electronic means
- Incident management practices
- Data destruction processes and conformation
- Physical security accessibility
- Compliance with legislation and Codes of Practice
- Staff training in security practices.

1.4.4 Review Methodology

The investigation and assessment will be performed through a combination of:

- Reviewing relevant legislation, codes of practice, and relevant ACC policies, standards, processes, procedures and practices
- Reviewing information/reports prepared by ACC in connection with the breach
- Undertaking interviews with relevant personnel
- Evaluating the design effectiveness of the controls, taking into account good practice, regulatory requirements, risk assessment
- Undertaking targeted detailed testing to confirm the operating effectiveness of the controls.

Relevant KPMG methodologies will be used to complete the information gathering and analysis, and ensure the robustness and quality of the findings and report. These include the KPMG Global Investigation methodology and the KPMG Internal Audit methodology. The engagement will be undertaken in accordance with recognised project management methodologies relevant to a project of this nature.

1.5 Review protocols

Due to the significance of the review and a strong desire to ensure transparency in ACC's approach, a Steering Group is to be formed. The role of the Steering Group will be to:

- Validate the investigation and review Terms of Reference
- Monitor the progress of the investigation and review
- Provide appropriate direction to the Review Team
- Provide timely updates to the OPC and the ACC Board as may be required
- Discuss any issues arising with the investigation and review process
- Review the draft report and provide feedback prior to finalising the report.

The Steering Group will comprise of both internal and external stakeholders. The Steering Group members are:

- **Mr John Meehan** – Chair, Audit and Risk Committee Chair (Steering Group Chair)
- **Mr Malcolm Crompton** – IIS (Privacy expert)
- **Mr Mike Flahive** – Assistant Commissioner (Investigations), OPC [Observer]
- **Mrs Souella Cumming** – Responsible KPMG Partner
- **Mr Ralph Stewart** – Chief Executive.

1.6 Review timing

The independent review will commence on 28 March 2012. A detailed project scope and timeline will be developed and confirmed once the Terms of Reference has been finalised. The timeline below is indicative of the review process. Achievement of the timetable is subject to availability and access to relevant personnel and documentation.

Activity	March 2012	April 2012	May 2012	June 2012
Planning, including agreement of TOR				
Fieldwork				
Reporting				

1.7 Review deliverables

- Timely and relevant updates to the Steering Group, as may be required
- Draft and final report consisting of:
  - Findings relating to the privacy breach investigation
  - Findings relating to the review of information security policies and practices
  - Recommendations for action by ACC.