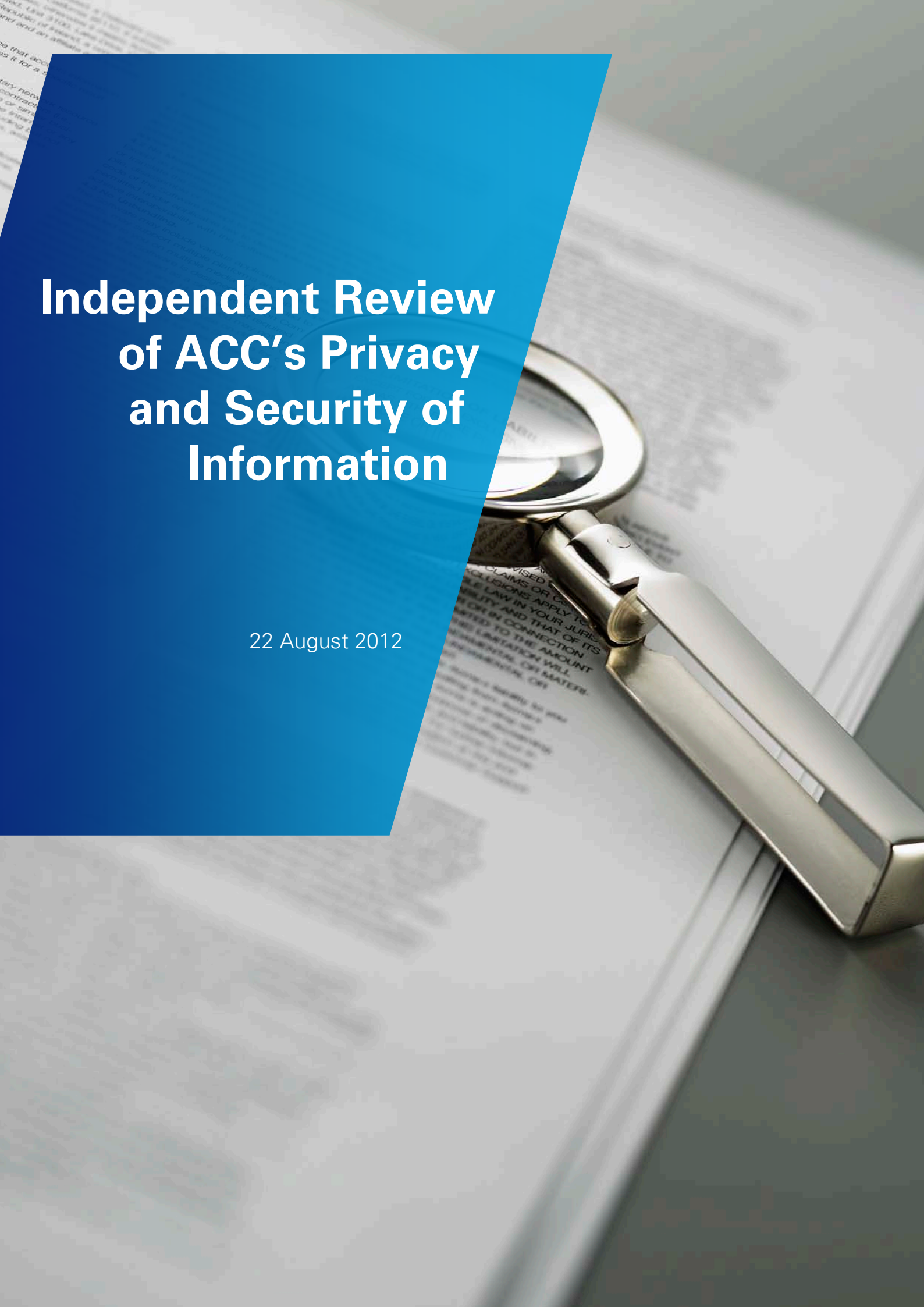
Independent Review of ACC's Privacy and Security of Information

22 August 2012



KPMG Centre
10 Customhouse Quay
P.O. Box 996
Wellington
New Zealand
Telephone: +64 4 816 4500
www.kpmg.co.nz

Level 3
53 Balfour Street
Chippendale NSW
PO Box 978
Strawberry Hills NSW 2012
Australia
Telephone: +61 2 8303 2438
www.iispartners.com

Privacy Commissioner
Office of the Privacy Commissioner
109-111 Featherston Street
Wellington 6143

Interim Chairperson
Accident Compensation Corporation
PO Box 242
Wellington 6140

22 August 2012

Independent Review of ACC's Privacy and Security of Information

We have completed our work in relation to the Independent Review of Accident Compensation Corporation's Privacy and Security of Information in accordance with the Terms of Reference dated 23 March 2012.

We appreciate the commitment and co-operation from Accident Compensation Corporation staff and management. We would also like to thank the external stakeholders and other organisations that contributed to the Independent Review.

We would be happy to answer questions relating to our report, or provide more information about our Independent Review, at your convenience.

Yours sincerely

Souella Cumming
Partner
KPMG

Malcolm Crompton
Managing Director
Information Integrity Solutions Pty Ltd

Contents

Disclaimers

Our report was prepared solely in accordance with the specific terms of reference set out in the engagement letter agreed between ourselves, the Office of the Privacy Commissioner ("OPC") and the Accident Compensation Corporation ("ACC") Board, and for no other purpose. Other than our responsibility to the OPC and the ACC Board, neither KPMG, Information Integrity Solutions ("IIS") nor any member or employee of KPMG or IIS undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility. KPMG and IIS expressly disclaim any and all liability for any loss or damage of whatever kind to any person acting on information contained in this report, other than the OPC and the ACC Board.

The report is based upon qualitative information provided by ACC. KPMG and IIS have considered and relied upon this information. KPMG and IIS believe that the information provided was reliable, complete and not misleading and has no reason to believe that any material facts have been withheld. The information provided has been evaluated through analysis, enquiry and review for the purposes of this report. However, KPMG and IIS does not warrant that these enquiries have identified or verified all of the matters which an audit, extensive examination or due diligence investigation might disclose.

The statements and opinions expressed in this report have been made in good faith and on the basis that all relevant information for the purposes of preparing this report has been provided by ACC and that all such information is true and accurate in all material aspects and not misleading by reason of omission or otherwise. Accordingly, neither KPMG, IIS nor their partners, directors, employees or agents, accept any responsibility or liability for any such information being inaccurate, incomplete, unreliable or not soundly based, or for any errors in the analysis, statements and opinions provided in this report resulting directly or indirectly from any such circumstances or from any assumptions upon which this report is based proving unjustified.

The report dated 22 August 2012 was prepared based on the information available at the time. KPMG and IIS have no obligation to update our report or revise the information contained therein due to events and transactions occurring subsequent to the date of the report.

1 Executive summary

1.1 ACC in the 21st Century

Historically, the assets of a company could easily be quantified by numbers on a balance sheet, or physical assets. In the information age, this is no longer the case. Information is arguably the most critical asset in any organisation. Keeping it safe and preserving its value is one of the most difficult challenges. Personal information makes the challenge more complex with rising community expectations and legal and regulatory factors impacting on an organisations' activities.

The value and risks involved in handling personal information are now changing very rapidly. In the words of a report to the World Economic Forum, "the explosive growth in the quantity and quality of personal data has created a significant opportunity to create new forms of economic and social value." By the same token "individual perceptions of harm and powerlessness versus organisational feelings of control and ownership" have meant that individuals "are beginning to lose trust in how organisations and governments are using data about them…"[1].

One significant implication of these developments is the emergence of data breaches as a fact of life globally. Some of the breaches have been massive. In 2007, the UK Department of Revenue and Customs lost a CD containing personal details of virtually every child in the UK. In 2006, a laptop belonging to the US Department of Veterans' Affairs was stolen containing the names, dates of birth and social security numbers of about 26.5 million active duty troops and veterans. Data breaches in the private sector have compromised personal information of more than 100 million individuals at a time. The lesson for all organisations, large and small; government or business is to be on their guard and manage a rapidly increasing risk, both to minimise the possibility of data breaches and have sound response strategies when they do occur.

The Accident Compensation Corporation ("ACC") is a large organisation which provides New Zealanders with personal accident insurance cover. It deals with a range of short and long term claims some of which are very complex in nature, requiring a substantial amount of health related and personal information to be collected and assessed. Personal information is one of the most significant assets ACC has to manage. In agencies such as ACC, whose interaction with people and personal information is critical and central to their function, effective privacy management and a culture of respecting personal information must be a clear priority and given appropriate strategic importance.

The impact of the information revolution on ACC means that the value of the personal data in its custody is increasing rapidly, with a commensurate impact on the risk exposure of ACC both in regards to data breach and the respectful management of personal data. Both point to the need for a renewed emphasis on governance of personal data including its risk management.

1.2 Context to the Independent Review

The Office of the Privacy Commissioner ("OPC") in conjunction with the ACC Board requested an independent review of ACC's practices in relation to privacy and security of information as a result of a significant data security breach that occurred on 5 August 2011 and that became public in March 2012 ("Auckland Privacy Breach" or "the Breach"). The Breach involved the unauthorised disclosure of details of 6,748 clients.

[1] See the World Economic Forum Report *Rethinking Personal Data: Strengthening Trust* and the related report *Personal Data: The Emergence of a New Asset Class* which are available at www.weforum.org/issues/rethinking-personal-data/

KPMG and Information Integrity Solutions Pty Limited ("IIS"), led by former Australian Privacy Commissioner Malcolm Crompton, were appointed as the Independent Review Team to conduct the Independent Review.

The Independent Review was conducted in the context of ACC dealing with the consequences of the Breach, both for its affected clients and for its own management and practices. As the seriousness of the Breach became apparent ACC's Board, Chief Executive and Executive Management commenced a number of internal reviews and ACC has already made a number of changes in its privacy management approach and structures.

1.3 Objectives of the Independent Review

The Independent Review was constituted and guided by the Terms of Reference which is set out in Appendix 1. The Terms of Reference require the Independent Review to make an independent assessment of ACC's Privacy and Security of Information and to specifically report back on:

- The circumstances of the Breach including the cause(s) and ACC's response.
- The appropriateness of policies and practices (including comparability with private sector practices, consistency 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).
- The effectiveness of policies and practices (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).
- 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.

The Independent Review Team has made its assessment based on information at the time of the Independent Review (April to August 2012). The Independent Review Team sought input from a range of internal and external stakeholders. Comparative analysis was completed with a number of other organisations on their approach to, and delivery of, privacy programmes from the perspective of risk management, compliance and accountability.

The scope and approach to the Independent Review is set out more fully in Section 3.

1.4 Overall assessment

Data is pervasive throughout all levels of business from the initial contact with the customer, through to the information and reports that the Board and Chief Executive rely on to make decisions. An organisation's data needs to be protected by thorough and effective risk mitigation strategies to the same (or higher) levels as other vital assets. Without these strategies in place, the organisation is at risk of significant reputational damage. The nature of ACC's operations, the number of complex and long-term claims, combined with the manual nature of many of its processes and technology systems, has resulted in ACC having a history of privacy breaches and complaints.

The Independent Review Team concluded that the Breach that occurred was a genuine error but that errors are able to happen because of systemic weaknesses within ACC's culture, systems and processes. The subsequent "response process" could also have been better if appropriate policies, practices, escalation protocols and the "right culture" were in place to allow for transparency of breach handling at the appropriate levels, in an appropriate manner. A similar incident is much more likely to happen again in the current environment if the issues identified in this Independent Review are not addressed systematically and systemically.

The Independent Review Team found that there are critically important areas of privacy management and better privacy practice which, if adopted, should strengthen ACC's ability to meet its compliance obligations, to better protect its clients' privacy and improve customer service. The recommendations in this report will support delivery of ACC's 2012-2015 Business Plan objectives which place a renewed emphasis on customer service and privacy. The recommendations are also consistent with the Government's priorities as outlined in the Service and Purchase Agreement 2012-2015.

1.5 Auckland Privacy Breach – findings

The sequence of events leading up to and arising from the Auckland Privacy Breach is set out in some detail below, in light of the considerable public interest in the Breach. The Independent Review Team bases this chronology on the evidence of the materials available to it and interviews it conducted. These developments are considered in more detail in Section 4 of this report while Appendix 4 sets out a more detailed chronology of events.

On 5 August 2011 the manager of the Northern Region Recover Independence Services Team (the "RIS Manager") was drafting an email response in reply to one received four days earlier from an Auckland based ACC client (the "Client"). In the course of drafting, the RIS Manager inadvertently clicked and dragged an unrelated email so that it became an attachment to the email being drafted.

The unrelated email included a spreadsheet containing information about 6,748 ACC clients including the Client. The information related to the status of clients' reviews with Dispute Resolution Services Limited ("DRSL"). DRSL is an independent company, which manages facilitation, mediation and review hearings for ACC clients who are unhappy with a decision or outcome relating to their claim. The DRSL information is included in a monthly management report distributed by the National Manager RIS to the regional RIS managers.

The Independent Review Team ascertained from interviews that the RIS Manager, rather than the Client's normal case manager, was involved in responding to the Client in this particular circumstance because the Client was requesting a response to a complaint previously made by the Client regarding a medical advisor. The RIS Manager had been reviewing the monthly management report containing the DRSL information around the same time as responding to the Client although it was not directly relevant to the response. This could be viewed as a hazard of multi-tasking in this instance. The Independent Review Team has ascertained from interviews that ACC has informal guidance discouraging working on more than one client file at a time.

The Client was one of the 6,748 ACC clients included on the spreadsheet. The Client informed the Independent Review Team that it was not until 26 October 2011 that the Client became aware of the extent of personal detail about other ACC clients included in the 5 August 2011 email response from the RIS Manager.

The Independent Review Team ascertained the following from the information reviewed, interviews with the Client and the Senior Advisor, Integrity at the State Services Commission ("SSC"):

- On 26 October 2011, the Client forwarded the 5 August 2011 email to the SSC. This email included the original attachments because most email systems, by default, will include any attachments when forwarding email as opposed to replying. The purpose of the email was to inform the SSC about the circumstances surrounding the Client's claim with ACC. The Client did not inform the SSC about the Breach at that time. The Client informed the Independent Review Team that it was only after sending the 26 October 2011 email to the SSC that the Client looked in detail at the spreadsheet containing the personal information about other ACC clients. The SSC was not aware that it had received the spreadsheets containing the personal information until 23 March 2012, shortly after the Breach became public. The Senior Advisor, Integrity informed the Independent Review Team that "*This email was one of 18 emails containing 65 attachments sent [from the Client to the SSC] within a 90 minute period*".

By December 2011 the Client had been a client of ACC for nearly nine years and has had a number of interactions with ACC that do not form part of this Independent Review. The events that the Independent Review Team consider most relevant between 5 August 2011 and 1 December 2011, began with the Client contacting a member of ACC's Board. That initial contact, which resulted in a meeting between the Client and an ACC Board member, set off a series of events leading up to the 1 December 2011 meeting in which the Breach was discussed.

- On 1 September 2011 the Client contacted a member of ACC's Board by email to arrange a meeting to discuss "*… a number of issues regarding ACC – compliance and personal*". The Client met that Board member on 14 September 2011 to discuss the Client's concerns with the way ACC was handling claims and managing personal information and specifically the Client's claim. The Client did not mention anything about the Breach at this meeting, as the Client informs the Independent Review Team the Client was unaware of it at that time. Later that same day the Board member sent an email to the Chair of the Board about the meeting with the Client and the issues raised by the Client. This led to ACC setting up a meeting with the Client, which was arranged for 1 December 2011. ACC understood that the purpose of the 1 December 2011 meeting was to listen to the Client's concerns regarding the Client's rehabilitation with the view to agreeing a way forward.

ACC was first notified of the Breach on 1 December 2011 during the course of a meeting between two ACC Managers and the Client. The Client made a voice recording of the meeting without the knowledge of the ACC Managers. While the Independent Review Team was not given a copy of this recording, four members of the team were given permission and listened to the recording of the 1 December meeting on 28 June 2012 and again on 9 August 2012. The following was ascertained:

- Those present at the meeting included the Client, the Client's support person, the Northern Area Manager and the National Manager RIS. A list of 45 alleged breaches by ACC of legislation, guidelines and codes was prepared by the Client prior to the meeting on 1 December 2011. The list, which included reference to the Breach as one of the 45 alleged breaches, was referred to several times during the meeting; however, the ACC Managers did not receive the list until the end of the meeting. This was because it was not the intention of the Client to address each and every alleged breach on the list at the meeting, but to discuss a proposal for a way forward with regard to the Client's own claim.
- During the course of the meeting, the ACC Managers were informed that the Client had received an email sent in "*error by one of your staff*". The email "*contained thousands of elements of highly sensitive health information*". One of the ACC Managers asked if the Client "*still had the email*" and if it had been deleted. The Client confirmed "*I've got every email since the day my claim started*", that the email included personal information about the Client "*plus about six and a half thousand other claimants, and names and claim numbers and conditions and details*".
- When the Breach came to the attention of the ACC Managers at the meeting, the Northern Area Manager asked "*Are we aware of that [the Breach]?*". The ACC Managers were told by the Client "*No*". The National Manager RIS stated, "*if there's a privacy breach that has originated from ACC, then absolutely we should be aware of it. Because if it relates to other people, then we need to make them aware that there has been a privacy breach*". Later the National Manager RIS stated, "*one of the things we clearly want is to get hold of that*". The Client's support person agreed to this stipulation and stated "*that it's never going to be used.*" Neither ACC Manager explicitly requested at the meeting that the information related to the Breach be returned.

The Independent Review Team did not find any evidence that ACC was aware of the Breach prior to the 1 December 2011 meeting. As a consequence of not being aware of the Breach until this date, ACC did not take any action on or after 5 August 2011, the date the Breach actually occurred.

Upon being informed of the Breach the ACC Managers responded as follows:

- At the meeting the ACC Managers asked if ACC were aware of the Breach and if the Client had deleted the email containing the Breach information.
- After the meeting the Northern Area Manager emailed the National Manager Claims and the Board and Corporate Secretary[2] advising them of what occurred at the meeting. The email communication included the following in reference to the list of 45 alleged breaches… " *They also gave us a list of alleged breaches by ACC of the Code, ACC legislation and other legislation*".
- After the meeting the National Manager RIS performed a search of his email communications with the Client and the Client's support person because he inferred from what was said at the meeting that he was responsible for sending the email that caused the Breach. It later transpired that this search was not sufficiently broad enough when it was determined he had not been the one who had sent the email that caused the Breach.
- A letter was sent to the Client on 9 December 2011 which included a formal request to return the personal information.

A request for the return of the information related to the Breach was not made before the 9 December 2011 letter to the Client. The Client did not return the personal information to ACC as requested by this letter.

Between the letter sent on 9 December 2011 and when the Breach was made public by the media on 13 March 2012, ACC took no further action in relation to the Breach or in relation to the other 44 alleged breaches by ACC of legislation, guidelines or codes.

Subsequent to the Breach being made public, ACC immediately contacted the Client; again requesting that the Breach information be returned and destroyed. The Client returned the file by forwarding a copy of the original email to ACC on 13 March 2012, and provided assurances that the information on her computer had been destroyed by an independent third party. ACC also established a response team to manage the Breach and inform those affected.

On 23 March 2012 the OPC, in conjunction with the ACC Board, announced an independent review of ACC's information security policies and practices and published the Terms of Reference.

In light of these events, the Independent Review Team finds that the immediate cause of the Breach was human error. A mistake happened in August 2011, ACC were not aware of it until 1 December 2011. After being made aware of the Breach they asked for its return in writing from the Client. While in hindsight an error in judgement, ACC did not appreciate the significance of the Breach until it was made public in March 2012 but the Independent Review Team found that ACC could have done more to follow through on the information provided by the Client on 1 December 2011. The Independent Review Team further considers that in light of being advised of the extent of the Breach information and being presented with a list of 45 alleged breaches, these issues should have been escalated to the Privacy Officer and/or the Office of the Complaints Investigator soon after the 1 December 2011 meeting. ACC should also have made a more concerted effort to have the Breach information returned and undertaken a more extensive internal investigation into how the information was sent to the Client.

Analysis of the events and steps taken by ACC highlighted systemic issues that increased the likelihood of the Breach occurring including the use of dual monitor screens, extensive use of spreadsheets for management reporting, a variable culture in regards to the importance of dealing carefully with personal information and a lack of clear accountability for addressing privacy issues.

[2] The Board and Corporate Secretary is the title of a member of the Executive at ACC. Refer to the Glossary for further information.

These systemic issues were explored further as part of the privacy and security practices assessments discussed below.

1.6 Privacy and Security Practices Assessment – findings

The Independent Review Team found that ACC had a range of controls in place to meet its obligations under the Privacy Act 1993 (the "Privacy Act") and the Health Information Privacy Code (the "HIPC") to protect the privacy of clients, and its practices, including the training associated with its privacy programme.

However, given the Breach and previous privacy breaches and complaints, the Independent Review Team finds that ACC's current arrangements need to be strengthened if they are to deliver a sustainable approach to protecting personal information.

The Independent Review Team considers that there needs to be clear recognition that reducing privacy breaches begins with addressing all aspects of information governance starting with data collection and moving through all the Information Privacy Principles ("IPPs") and Health Information Privacy Rules ("HIPRs"). This includes processes for ensuring data quality and accuracy; access to data, reporting systems and through it all, a culture that emphasises respect for individuals and the personal information that is collected, stored and used by ACC.

Risks associated with the collection and management of personal information were not a core part of ACC's risk management framework and historically privacy has not been a standing item on the agenda of the ACC Board and its sub-committees. The Board was aware that ACC's approach to privacy training and its standing against other public sector organisations compared favourably and therefore from the ACC Board's perspective there was no information that caused them to have any specific concerns about how personal information was managed by ACC. Privacy management was focused on responding to breaches rather than actively managing personal information in line with the IPPs. Resourcing has also reflected this with privacy being part of people's roles rather than having a core team of full time resources devoted to the privacy programme. The Privacy Officer is supported by a small team and dealt mainly with issues escalated from the branch network, rather than acting as a central co-ordination point for all privacy related matters across ACC. There is no comprehensive privacy programme in place and accountability is not clear, including responsibility for escalating and resolving issues. A consequence of this was that monitoring and reporting of privacy related matters was limited (for example the ACC Board did not receive regular reports relating to privacy issues or performance, privacy risk management, privacy breaches and "near misses", which is the discovery of privacy breaches before they are exposed externally, until May 2012).

While ACC defines privacy as everyone's responsibility the design of current systems and processes does not support a culture where the importance of personal information is valued and managed consistently and appropriately through the organisation. Current work practices and the wide range of policies and procedures have led to an ad hoc approach to managing personal information. Some work practices (physical file copying and distributing physical files in response to access requests) and system design (such as open access to the majority of client data once you have access to the claims management system) can result in inappropriate disclosure of personal information when not reinforced by a culture where the importance of personal information is understood, where all staff feel both supported in their work and also individually responsible, where staff are aware of the risks, and where sound management is appreciated and the consequences of not managing personal information appropriately are clearly defined. Business processes and systems would benefit from a comprehensive review to ensure privacy is built-in not built-on, and advances in technology (such as information portals) can be used to make personal information available to individuals while still ensuring high standards of access and protection on how the information is accessed and used.

The importance of culture was reinforced by the external stakeholders where the overwhelming feedback was for client and client personal information to be treated with respect. Stakeholders reported varied experiences of ACC's practices relating to personal information management over many years but consistent themes emerged through the stakeholder meeting regarding multiple instances where personal information was not updated on a timely basis, information not relevant to the claim was held on file, and frequent occurrences of information related to other claimants being retained on file and/or released to other claimants. Stakeholders reflected that while these instances were regrettable (and they acknowledged that errors occur from time to time), what concerned them most was the attitude of the organisation in dealing with their personal information. For stakeholders this pointed to a cultural issue and was the single biggest aspect that stakeholders wanted to see addressed as an outcome of the Independent Review.

The comparison of ACC's privacy practices with other organisations indicated a difference in approach to managing privacy issues particularly in the determination and response to legislative risks through process management. Notably, ACC compares more than favourably with other organisations around its education, training, complaint management and resolution processes. However it has a different approach to process risk management, compliance and the cultural elements, leadership and consequence management. This points to an opportunity for ACC to take a more comprehensive approach to compliance throughout the organisation.

The Independent Review Team's findings impact every stage of the information governance life cycle. The findings start with "tone at the top" and the setting of strategy, the implementation of that strategy through an integrated privacy programme, appropriate organisational and supporting business practices and complete the cycle with findings relating to monitoring and lines of accountability.

1.7 Recommendations

ACC needs to put in place clear policies that create a positive privacy mindset as part of rebuilding customer trust and establishing a "firm but also seen as fair" image in the minds of the public. As part of achieving these objectives, ACC also needs a coherent strategy and process to mitigate privacy risks; to monitor performance for compliance, and to ensure that there is adequate resources and capacity to respond to incidents. The current mechanisms and approaches need to be reassessed to assist ACC to protect personal information in the current and future planned operating environment.

In making its recommendations the Independent Review Team emphasises the significance of a culture and environment where personal information is valued. This must be supported by an approach to compliance with the privacy principles that is embedded within governance, leadership, and business processes and systems.

The full body of Recommendations is set out in Section 2. In summary, the Independent Review Team recommends that ACC:

- Strengthen Board governance of personal information management by reflecting the importance of privacy and protection of personal information in the weighting given to privacy in the risk management framework and the ACC Board's focus on privacy; and actively participate in the development of a vision for privacy within ACC which is to be the basis for a privacy strategy. A plan to implement the privacy strategy should also be developed and an independent privacy audit of ACC's adherence to its privacy strategy undertaken in consultation with the Privacy Commissioner. The ACC Board should review the privacy strategy every two years in light of the privacy audit.

- Strengthen privacy leadership and strategy by strengthening ACC's "three lines of defence model" for privacy including consideration of privacy compliance as part of a broader compliance framework; ensuring a member of the Executive is accountable for privacy and is responsible for providing leadership on implementing ACC's privacy strategy; developing a privacy strategy for ACC for adoption by the ACC Board; and considering how it will involve stakeholders in developing the strategy.
- Enhance its privacy programme, consistent with its privacy vision and strategy by ensuring that the Privacy Officer position has a formally documented role. This and other specialist privacy roles should be adequately resourced. The role of Privacy Champions should be reviewed and clarified and criteria for the appointment of Privacy Champions set out and consistently applied. Privacy policies and procedures should be reviewed and staff supported to implement ACC's privacy vision and to comply with the Privacy Act with appropriate privacy education and training. A privacy risk management framework should be developed. Consistent systems and processes for recording, monitoring and reporting all near misses, privacy breaches and privacy complaints under ACC's Claimants Code of Rights (the "Code") or the IPPs and the HIPRs should be developed. Privacy complaint processes, whether made under the Code or the IPPs, should be integrated. A formal security governance structure should be developed with appropriate processes, complemented by a formal security assurance programme and restructured security training programme.
- Strengthen the organisational culture to emphasise respect for individuals and the personal information that is collected, stored and used by ACC by aligning its privacy culture to the broader culture of the organisation to ensure that the operating framework within ACC is integrated with customer centric objectives and provides clear external commitment to clients of ACC's focus on customer care; developing consistent messages that balance privacy, customer service and efficient and effective management so that "firm is also seen as fair" by ACC and its external clients and stakeholders; incorporating stakeholder views on appropriate processes for continuous engagement with interest groups and individuals; and ensuring that staff are encouraged to report and resolve privacy breaches or near misses in a supportive environment.
- Strengthen privacy accountability across the whole organisation by ensuring that staff roles and responsibilities for privacy are clearly identified; identifying and implementing a set of key criteria/Key Performance Indicators ("KPIs") for driving and assessing ACC's privacy management performance; ensuring that ACC leadership monitor performance against the identified criteria/KPIs so that ACC can change tack if needed; ensuring there are processes in place to evaluate third parties against ACC's expectations, either at the start of a contract, or on an ongoing basis; and establishing clear reporting requirements to Board level and also report publicly on ACC's privacy performance via the annual report or other appropriate channels.
- Review and update business processes and systems by undertaking an end-to-end process review of the claims management process; re-engineering processes as needed, adopting "privacy by design" and/or "privacy by redesign" principles; reviewing processes by which clients and others on whom ACC holds personal information are able to access, review and challenge or even update that information; reviewing information exchange practices with employers and ACC's health service providers to introduce a requirement that any one report or exchange of information contains personal information relating to only one person or client; reviewing of all business processes that create compilations of personal information about clients other than the actual Electronic Claims Management System ("EOS") record, with a view to ceasing them or de-identifying the data and replacing identifying information such as names with random identifiers; and implementing data loss protection software.
- Provide additional resources to clear backlogs on privacy related processes including access requests and complaints.

In addition to implementing the above recommendations there are a number of short-term initiatives (such as addressing system access, reviewing the use of spreadsheets that contain personal information and addressing the back-log of paper files that need to be electronically scanned) that need to be addressed (with appropriate resources applied) to reduce the likelihood of privacy breaches occurring.

2 Review Recommendations

The Independent Review Team makes the following recommendations to the ACC Board. The recommendations have been developed on the basis of the findings in Section 8 of the report. The recommendations include indicative timeframes for implementation.

In making its recommendations the Independent Review Team emphasises the significance of a culture and environment where personal information is valued. This must be supported by an approach to compliance with the privacy principles that is embedded within governance, leadership, and business processes and systems.

Recommendation 1 – Board governance	Indicative timeframe for implementation
The Independent Review Team recommends that the ACC Board takes the following steps to strengthen the governance of privacy within ACC:	
1.1. Reflect the importance of privacy and protection of personal information in the weighting given to privacy in the risk management framework and the ACC Board's focus on privacy through the following measures: a. Co-ordinate and structure privacy as part of the risk management framework in the medium to long term in order to make privacy management effective across ACC. b. Lead by example at Board and Audit & Risk Committee level by setting clear expectations and communicating them to Executive Management. c. Assess privacy risks against ACC's risk appetite and tolerances with consistent reporting. d. The ACC Board commits to the provision of resources to fully embed privacy risk management within ACC with a programme of risk management activities.	3 months - 1 year
1.2. Actively participate in the development of a vision for privacy within ACC which is to be the basis for a privacy strategy and which: a. Defines the ACC Board's risk appetite with regards to compliance with the Privacy Act and related codes and principles. b. States that privacy is a key risk management issue for ACC and is likely to increase in importance over time. c. Recognises that striving for "zero acceptance" of data breaches begins by minimising risks at all stages in the information management life cycle through best practice implementation of all of the Information Privacy Principles ("IPPs") and Health Information Privacy Rules ("HIPRs"). d. States the critical importance of a culture of respect for client privacy and good management of information about clients, to the wellbeing of ACC clients and to achieving community trust in ACC. e. States the ACC Board's strong commitment to achieving the vision.	2 months
1.3. Initiate the development by ACC of a privacy strategy for adoption by the ACC Board which implements the vision for privacy and which covers compliance with privacy law including all the IPPs/HIPRs, implementation of best practice privacy and a culture of respect for client privacy (see Recommendation 4).	4 months

Recommendation 1 – Board governance		Indicative timeframe for implementation
1.4.	Ensure a cycle of continuous accountability to the ACC Board by ACC leadership in regards to privacy risks.	Immediately
1.5.	Include "privacy" in the Terms of Reference for those Committees that have responsibility for privacy oversight and monitoring. Individuals within the selected governance committees and groups should be made aware of the nature and scope of personal information collected by ACC.	3 months
1.6.	Follow up on the Independent Review Team's recommendations.	1 year
1.7.	Ensure that every two years ACC, in consultation with the Privacy Commissioner, commissions an independent privacy audit of ACC adherence to its privacy strategy including compliance and best practice elements.	2 years
1.8.	Ensure that the report of the independent privacy audit is given to the Privacy Commissioner and published on the ACC website.	2 years
1.9.	Ensure that the ACC Board reviews the privacy strategy every two years in light of the independent privacy audit.	2 years

Recommendation 2 – Leadership and privacy strategy		Indicative timeframe for implementation
The Independent Review Team recommends that ACC takes the following steps to strengthen its privacy leadership:		
2.1.	Strengthen the "three lines of defence model" that will allow privacy to be embedded in decision-making assisting to create a culture where everyone has ownership and responsibility for protecting personal information and doing the "right thing". This should include consideration of a comprehensive compliance programme to strengthen ACC's second line of defence.	6 months
2.2.	Ensure a member of the Executive is accountable for privacy and is responsible for: a. Providing leadership on implementing the ACC privacy strategy. b. Ensuring that appropriate resources are allocated. c. Ensuring that other key privacy targets are being met.	Immediate
2.3.	Develop a privacy strategy for ACC for adoption by the ACC Board which covers the following matters: a. The ACC Board's privacy vision for ACC. b. The values and principles that ensures that the culture within ACC supports the privacy strategy. c. The structure of responsibility and accountability for top to bottom implementation of privacy compliance and best practice within ACC – including a means of drawing upon the views of, and reporting to, key stakeholders and interest groups such as: i. ACC clients, their carers and advisers ii. Privacy Commissioner iii. ACC employees.	3 months

Recommendation 2 – Leadership and privacy strategy	Indicative timeframe for implementation
d. The mechanisms for identifying privacy compliance and risks and the way this fits within ACC's wider risk assessment approach. e. Mechanisms for ensuring that privacy best practice and compliance is built into all new systems products and services. f. The benchmarks or KPIs for Executive Management and ACC as a whole in achieving compliance with the law and best practice privacy. g. Philosophy governing, and mechanisms for, training staff in privacy compliance and best practice. h. Mechanisms for ensuring third party contractors to ACC comply with ACC's privacy strategy. i. Mechanisms for measuring progress in implementing and compliance with the privacy strategy including internal and external monitoring and audit. j. Mechanisms for reporting to the ACC Board and external stakeholders of progress in implementing and compliance with the privacy strategy taking into account the Independent Review's recommendations relating to Board governance. k. Expression of the privacy strategy in an integrated privacy programme.	
2.4. Develop a plan for engaging stakeholders in developing the strategy.	3 months

Recommendation 3 – Privacy programme	Indicative timeframe for implementation
The Independent Review Team recommends that ACC enhance its privacy programme, consistent with its privacy vision and strategy and should:	
3.1. Formally document the role of the Privacy Officer position to include, in addition to the roles set out in the Privacy Act (unless these roles are clearly allocated elsewhere): a. Developing ACC's privacy strategy and programme, in conjunction with the ACC Board, Executive Management and other ACC Managers. b. Providing day-to-day leadership of the privacy programme, in particular to the Privacy Champions, ensuring that they are able to operate as a virtual team. c. Providing advice on development of ACC systems and programmes, based on Privacy by Design principles and use of privacy impact assessments. d. Developing and reviewing privacy policies and procedures and systems and tools to ensure compliance with privacy principles and ACC's privacy vision and strategy. e. Developing or providing input into privacy awareness, training activities and guidance for all staff. f. Monitoring and reporting to Executive Management, the ACC Board and other stakeholders on ACC's compliance performance and its performance against agreed privacy benchmarks and KPIs. g. Investigating and/or providing advice on privacy complaints and complaint handling and monitoring privacy breaches or near misses to ensure systemic issues are being identified and dealt with.	2 months

Recommendation 3 – Privacy programme		Indicative timeframe for implementation
	h. Supporting continuous improvement in privacy practices including actively keeping abreast of developments in privacy approaches internationally as well as in New Zealand, by participating in OPC forums and undertaking development as a privacy professional.	
3.2.	Review and clarify the role of Privacy Champions and develop criteria for the appointment of Privacy Champions and ensure that it is consistently applied. If ACC decides that Privacy Champions should be expert privacy advisers, they should receive training at an appropriately technical level and given recognition as privacy professionals.	6 months
3.3.	Ensure ACC has an effective suite of privacy policies and procedures, based in the first instance on an audit of current personal information holdings and addressing all the IPPs/HIPRs which: a. Are comprehensive, up-to-date and easy to access and apply. b. Are reviewed regularly with input from staff to ensure they provide relevant and accessible answers to staff questions. This should be led by the Privacy Officer.	1 Year
3.4.	Ensure the Privacy Officer and other specialist privacy roles, including the possibility of a specialist privacy team reporting directly to the Privacy Officer, is adequately resourced, taking into account best practice benchmarks or advice from an independent Human Resource specialist.	4 months
3.5.	Support staff to implement ACC's privacy vision and to comply with the Privacy Act with appropriate privacy education and training for all staff which is comprehensive, has an appropriate maturity model based on staff experience in their role and which: a. Takes account of staff feedback that training should: i. be more scenario-based and practical ii. be operational and use work related examples iii. include dealing with clients in difficult and stressful situations empathetically and effectively iv. be more targeted to job area especially for Privacy Champions, HR and front-line staff. b. Ensures that staff are receiving regular detailed feedback on privacy incidents and their resolution and provides regularly updated case studies or similar tools to assist staff to refine their understanding of ACC's privacy approach. c. Is integrated with ACC's overall staff development programme as a visible demonstration that privacy is an integral part of the development of the complete ACC member of staff.	Visible to staff in 6 months, fully embedded 12 months
3.6.	Develop a privacy risk management framework that: a. Is an integral part of ACC wide risk management approach. b. Reflects ACC's view of its appetite for privacy risks. c. Addresses risks against all of the IPPs/HIPRs. d. Can take account of management information on near misses, privacy breaches and privacy complaints under ACC Claimants Code of Rights (the "Code") or the IPPs/HIPRs and identify and respond to any underlying systemic issues.	1 year

Recommendation 3 – Privacy programme	Indicative timeframe for implementation
3.7. Establish appropriate and consistent systems and processes for recording, monitoring and reporting all near misses, privacy breaches and privacy complaints under the Code or the IPPs/HIPRs, to facilitate improvements in policies and practices and identification of and response to systemic privacy issues. Privacy incident statistics might include: a. Business areas where incident occurred. b. Incident frequency by IPP and nature of the incident. c. Complaint outcome with categories both for matters substantiated and not substantiated. d. Improvements identified to minimise further incidents. e. Timeframe to resolution.	1 year
3.8. Complete a holistic review of the personal information provided to clients via all channels and at all stages in their interactions with ACC to ensure that: a. It is consistent. b. Provides sufficient detail to inform their decisions and actions. c. Takes account of current best practice in privacy notices, for example using layered notices and giving "just-in-time" privacy prompts.	Visible to clients within 6 months, fully embedded within 1 year
3.9. Establish clear processes for managing near misses and privacy breaches that take account of all the IPPs/HIPRs, as well as matters raised under the Code, have clear escalation paths, consider risks to the clients concerned and client notification in appropriate circumstance and incorporate review to identify and respond to underlying systemic issues.	4 months
3.10. Integrate privacy complaint processes, whether made under the Code or the IPP/HIPR ensuring that: a. The connection between privacy rights under the Code and under the IPPs and the HIPRs is clear. b. Clients are clearly aware of their rights to lodge a complaint about their privacy rights under the Code or the IPPs/HIPRs with ACC or the OPC. c. Privacy complaints are treated consistently and in accordance with best practice dispute resolution, whether made under the Code or the IPPs/HIPRs. d. Privacy issues raised through all channels are captured and fed into breach management and the risk management processes.	Within 1 year, earlier if possible, integrate with short term peak response plan
3.11. Develop a formal security governance structure and processes to support the effective information management of security which: a. Treats security as a business issue, rather than an IT issue, with security owned by a member of senior management (outside of the IT function). b. Establishes a governance group to provide direction and oversight of the security practices and processes – this could consist of, for example, the General Managers with security responsibilities. c. Establish a security management group to operationalise security, made up of the different senior staff with operational security roles from the different business units and functions, including representation from within the IT, property, privacy, human resources and information management functions. d. Applies risk management approach to managing security.	6 months

Recommendation 3 – Privacy programme	Indicative timeframe for implementation
3.12. Develop a formal security assurance programme. This should take a structured and comprehensive risk-based approach to security and focus on ensuring that: a. Sufficient feedback mechanisms are implemented within the business-as-usual activities performed by IT and the other business units with security responsibilities. b. Formal assurance mechanisms are implemented within project-based activities. c. Periodic independent assessments of security are performed, to provide an objective view of the effectiveness of the security in place.	6 months
3.13. Restructure the security training programme to ensure that: a. Regular broad compulsory security training is provided to all employees and contractors. b. Targeted, more detailed security training is provided to those employees and contractors with key security responsibilities. c. The completion of security training is tracked and monitored. d. The security training is reinforced by regular structured communications about relevant security topics.	Visible to staff in 6 months, fully embedded 12 months

Recommendation 4 – Culture	Indicative timeframe for implementation
The Independent Review Team recommends that in addition to the other recommendations that will influence the culture to ensure it supports respect for privacy. ACC should:	
4.1. Align its privacy culture to the broader culture of the organisation to ensure that the operating framework is integrated with customer centric objectives and provides clear external commitment to clients of ACC's focus on customer care.	Visible within 6 months, fully embedded within 1 year
4.2. Develop consistent messages that balance privacy, customer service and efficient and effective management so that "firm is also seen as fair" by ACC and its external clients and stakeholders.	Visible within 6 months, fully embedded within 1 year
4.3. Incorporate stakeholder views on appropriate processes for continuous engagement with interest groups and individuals.	Within 1 year
4.4. Ensure that staff are encouraged to report and resolve privacy breaches or near misses in a supportive environment supported by a sound compliance framework.	Visible within 6 months, fully embedded within 1 year
4.5. Develop measures, including key statistics, feedback from clients and other external stakeholders and staff and management surveys that will allow ACC to test that its culture supports respect for client privacy and to take remedial steps as needed.	1 year

Recommendation 5 – Accountability	Indicative timeframe for implementation
The Independent Review Team recommends that ACC take the following actions to strengthen privacy accountability across the whole organisation:	
5.1. Ensure that staff roles and responsibilities for privacy are clearly identified and documented with expectations and accountabilities apparent and measurable.	Within 6 months and 1 year
5.2. Identify and implement a set of key criteria/KPIs for driving and assessing ACC's privacy management performance for the Executive, ACC Managers and staff, and for ACC as a whole that: a. Reflect ACC's privacy vision and objectives for customer satisfaction as well as efficient and effective privacy management. b. Are consistent with ACC's risk settings on privacy. c. Allow it to measure compliance with all the IPPs/HIPRs and other agreed privacy indicators.	Within 1 year
5.3. Ensure that ACC leadership monitor performance against the identified criteria/KPIs so that ACC can change tack if needed.	Ongoing
5.4. Ensure there are processes in place to evaluate third parties against ACC's expectations, either at the start of a contract, or on an ongoing basis.	1 year
5.5. Establish clear reporting requirements to Board level and also report publicly on ACC's privacy performance via the annual report or other appropriate channels.	Interim 6 months, 1 year

Recommendation 6 – Business processes and systems	Indicative timeframe for implementation
The Independent Review Team recommends that ACC should:	
6.1. Undertake an end-to-end process review of the claims management process, including EOS functionality and other information management systems with a particular focus on privacy risk to: a. Ensure they are consistent with ACC's obligations under the IPPs/HIPRs, including in relation to the extent of personal information collected and best practice in seeking consent. b. Ensure process controls are effective. c. Identify high risk processes, both manual and electronic. d. Implement an "enter once" policy for any data entry or reporting system. e. KPI and reporting processes are automated outputs and by-products of other processes rather than requiring additional manual effort.	1 year
6.2. Re-engineer processes as needed, adopting "privacy by design" and/or "privacy by redesign" principles to minimise risks and improve effectiveness for ACC and its clients.	6 months

Recommendation 6 – Business processes and systems		Indicative timeframe for implementation
6.3.	Review processes by which clients and others on whom ACC holds personal information are able to access, review and challenge or even update that information, drawing on best practices available in other New Zealand government departments and agencies such as the Inland Revenue Department, with a view to implementing an online portal for clients to enable them to access and manage information about themselves online.	6 months
6.4.	Review information exchange practices with employers and ACC health service providers to introduce a requirement that any one report or exchange of information contains personal information relating to only one person or client, supported by appropriate ICT services and processes (such as templates and processes that deliver these requirements for reports on consultations, assessments, discharge summaries etc).	1 year
6.5.	Undertake a systematic review of all business processes that create compilations of personal information about clients other than the actual EOS record, with a view to ceasing them or de-identifying the data and replacing identifying information such as names with random identifiers. In particular: a. Establish a policy and supporting processes to ensure that research, actuarial and similar work streams are never conducted on raw, identifiable information. b. Consider the value in establishing a "de-identification" programme or unit with the responsibility for producing de-identified data for all purposes other than direct interaction with clients and case management, drawing on best practices from around the world.	1 year
6.6.	Develop and implement a strategy to reduce the reliance on the use of email as a business tool to communicate with staff, clients and business partners.	1 year
6.7.	Implement data loss protection software to reduce the likelihood of sensitive information being inadvertently "leaked" through email or other similar internet based communication.	1 year

Recommendation 7 – Backlogs and establishment of the new Business as Usual		Indicative timeframe for implementation
7.1.	The Independent Review Team recommends that ACC should provide additional resources to clear backlogs on privacy related processes including the back-log of paper files that need to be electronically scanned, access requests and complaints, in order for ACC and clients to regain trust and feel that a fresh start is under way as soon as possible.	3 months

IPP/HIPR Compliance Recommendations

The Independent Review Team has made a series of supplementary recommendations. These recommendations are primarily intended to assist ACC in implementing the broader recommendations for ACC's overall management of its privacy obligations but also raise issues that have not been considered elsewhere in the review. The supplementary recommendations are cross-referenced to the main recommendations.

Principle	Recommendation
IPP/HIPR 1	ACC should review its policy and procedures for the collection of personal or health information, taking account of the Privacy Commissioner's inquiry into the collection of medical notes by insurers to ensure that its staff, clients and providers are quite clear on the steps it will take when it receives medical reports or other information that might not be relevant in the processing of a claim or other circumstances. ACC should ensure the policy is promulgated to staff and that it also provides detailed guidance to assist in decision-making. ACC should monitor its collection practices at least yearly and take other steps as needed, including liaison with providers and further amending policies and procedures. (See also Recommendations 3 and 6)
IPP/HIPR 2	ACC should review its processes and forms for seeking consent to collect and disclose information to ensure that they are consistent with best legal and privacy practices and take account of ACC's clients' interests. ACC should establish processes to allow for detailed ongoing stakeholder consultation on the development and implementation of consent processes. Subject to the above, ACC should make its forms and consent processes: ■ As specific as possible to a claimant's circumstances. ■ Address the need to renew consent from time to time. ■ Consider the circumstances in which consent may be withdrawn (for future disclosures) and the consequences. ■ Not cover collection or disclosure of personal information where ACC does not need consent and instead provide information about such collection or disclosure in appropriate language, formats, and locations. (See also Recommendation 3 and 6)
IPP/HIPR 3	ACC should review the way in which it provides privacy information to its clients as required by IPP/HIPR 3 and best practice, to ensure it is consistent across forms and channels, is comprehensive and takes account of client's different information needs at different points in their claims process. Unless it can meet best practice other ways ACC should adopt a layered notice approach and should develop a detailed privacy policy on all aspects of its privacy commitment, its handling of personal information and its privacy complaint handling processes and make this generally available to clients and members of the community. (See also Recommendation 3 and 6)
IPP/HIPR 4	ACC should monitor the community perception of its collection processes and undertake detailed stakeholder consultations and address any issues identified in its privacy culture, recruitment, training or policies and procedures. (See also Recommendations 2, 3 and 4)

Principle	Recommendation
IPP/HIPR 5	In developing its response to this report and to its approach to its privacy management obligations, ACC should ensure that it addresses the security issues identified in this report or in other feedback from the review process. (See also Recommendation 3 in Section 8)
IPP/HIPR 6	ACC should review its "copy file" processes to ensure that it is able, including through IT sweeps and collation of information from all units, to provide all the information requested. ACC should also engage with claimant groups to ensure that its processes are meeting their needs and assist them to target requests as appropriate. ACC should review its processes for collating and providing "copy files" with specific reference to limiting risk of security breach or unauthorised disclosure. Within legal requirements, ACC should set and measure benchmarks, including processing times, for responding to requests for access under IPP/HIPR 6 and it should ensure that the same benchmarks apply to accredited employers. (See also Recommendation 6)
IPP/HIPR 7	No Recommendations made.
IPP/HIPR 8	In developing its response to this report and to its approach to its privacy management obligations, ACC should ensure that it has developed benchmarks for accuracy and that it addresses the risks to accuracy identified in this report or in other feedback from the review process. (See also Recommendation 6)
IPP/HIPR 9	ACC should review its practices in relation to the retention of personal information to ensure that: ■ Retaining identified client information for 75 years after the last interaction is appropriate. ■ Claimants and the community are aware of the practice. ■ It has identified and addressed the security risk in keeping personal information in identified form for such an extensive period. ■ It has in place strict governance and other arrangements to ensure that claimant information is only used for new purposes following detailed consideration including wide public consultation and that decisions are taken at least to Board or Executive level.
IPP/HIPR 10	In developing its response to this report and to its approach to its privacy management obligations, ACC should ensure that it considers the issues in relation to use of personal information identified in this report. (See also Recommendation 2 and 3)
IPP/HIPR 11	In developing its response to this report and to its approach to its privacy management obligations, ACC should ensure that it addresses the disclosure risks identified in this report, in particular, that it provides clear instructions and training to staff to ensure that only needed and appropriate information is disclosed in the context of claims processing. (See also Recommendation 2, 3 and 6)
IPP/HIPR 12	No recommendations made.

3 Introduction and Review objectives

3.1 Introduction

ACC is the Crown entity set up under the Accident Compensation Act 2001 ("AC Act"), to deliver New Zealand's accident insurance scheme ("the Scheme"). The purpose of the Scheme is to deliver no-fault personal injury cover for everyone in New Zealand, including overseas visitors.

The OPC in conjunction with the ACC Board requested an independent review of ACC's practices in relation to privacy and security of information as a result of a significant data security breach that occurred on 5 August 2011. An ACC Manager within the Recover Independence Services ("RIS") Team sent an email to an Auckland based client that included a spreadsheet containing information about 6,748 other ACC clients. The information related to the status of the clients' reviews with the Dispute Resolution Services Limited ("DRSL"), which is an independent company, who manage facilitation, mediation and review hearings for ACC clients who are unhappy with a decision or outcome relating to their claim. ACC was first notified of the Breach on 1 December 2011 during the course of a meeting scheduled with the Client to discuss various aspects relating to the status of the Client's claim.

The matter became public through the media on 13 March 2012. ACC then consulted the OPC about the matter that appeared to have contravened the Privacy Act.

KPMG and IIS were appointed as the Independent Review Team to conduct an independent review of the privacy breach and ACC's privacy policies and practices.

The Independent Review was conducted in the context of ACC dealing with the consequences of the Breach, both for its affected clients and for its own management and practices. As the seriousness of the Breach became apparent ACC's Board, Chief Executive and Executive Management commenced a number of internal reviews and have already made a number of changes in its privacy management approach and structures.

Personal information has always been one of the most significant assets ACC has to manage. Personal information is not only a critical part of its business but its management goes to the trust and confidence the community has in the agency.

However, in the words of a report to the World Economic Forum, "the explosive growth in the quantity and quality of personal data has created a significant opportunity to create new forms of economic and social value." By the same token "individual perceptions of harm and powerlessness versus organisational feelings of control and ownership" has meant that individuals "are beginning to lose trust in how organisations and governments are using data about them…".[3]

The impact on ACC is that the value of the personal data in its custody is increasing rapidly with a commensurate impact on the risk exposure of ACC both in regards to data breach and the respectful management of personal data. Both point to the need for a renewed emphasis on governance of personal data including its risk management.

During the period of the Independent Review there were some changes within ACC which affects the environment into which the review report will be delivered. These include:

[3] See the World Economic Forum Report *Rethinking Personal Data: Strengthening Trust* and the related report *Personal Data: The Emergence of a New Asset Class* which are available at www.weforum.org/issues/rethinking-personal-data/

- The Chair, Deputy Chair and three other Board Members' first term (of three years) expired on 31 March 2012. The Minister asked, and all agreed to remain on the Board while the Minister considered the Membership of the Board as the Minister was only appointed as Minister for ACC on 12 December 2011.
- On 12 June 2012 the Minister decided to not reappoint the Chair, Deputy Chair and one other Member for a second term (of three years). The Minister asked, and all agreed to remain on the Board until 30 June 2012.
- The Minister also offered a second term on the Board to the two other Board Members' whose terms expired on 31 March 2012. One Board Member accepted the reappointment and the other Board Member tendered his resignation effective from 31 July 2012. The Minister accepted his resignation on 21 June 2012.
- On 13 June 2012, following the departure of the Chair, Deputy Chair and one other Board Member, the Chief Executive decided to step down. The Board accepted his resignation on 18 June 2012; however the Chief Executive departure date has not been agreed with the Board.
- In June 2012, the Minister for ACC and ACC signed a Service and Purchase Agreement 2012-2015 outlining the quality and quantity of services to be provided by ACC. The Agreement reflected the Government's priorities for ACC.

The Independent Review Team has made its assessment on the basis of information about systems, policies and processes available at the time of the Independent Review (April to August 2012). It acknowledges the steps that have been taken to date in response to the Breach and that some of the changes it recommends may already be underway.

3.2 Review objectives and scope

3.2.1 Review Steering Group and Terms of Reference

As part of the review process and due to the significance of the review and a strong desire to ensure transparency in ACC's approach, a Steering Group was formed comprising both internal and external stakeholders. The Steering Group members are listed in the Terms of Reference in Appendix 1.

The role of the Steering Group was to:

- Validate the investigation and review Terms of Reference.
- Monitor the progress of the investigation and review.
- Provide appropriate direction to the Independent 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 Terms of Reference in Appendix 1 was prepared with input from KPMG and IIS and approved by the OPC and ACC Board.

3.2.2 Review objectives

The objectives of the Independent Review as set out in the Terms of Reference were to:

1. Investigate the circumstances of the privacy breach including the cause(s) and ACC's response.
2. Determine if ACC's policies and practices relating to security of information are:
    a. 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).
    b. 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.

3.2.3 Review scope

The scope of the Independent Review, in conjunction with the mandatory requirements of the Privacy Act and guidance provided within the HIPC, involved three co-ordinated and concurrent work streams:

1. Investigation of the unauthorised release of information by RIS and subsequent actions.
2. An assessment of ACC's policies, processes and practices to manage client information.
3. An assessment of ACC's security policies, practices, processes and safeguards (as they relate to client information and sensitive claims) including both IT and physical security.

3.3 Approach to the Independent Review

The Independent Review Team used a selected set of methodologies to complete the information gathering and analysis and to ensure the robustness and quality of the findings and report. These included the KPMG Global Investigation Methodology ("GIM"), KPMG's Internal Audit Methodology ("IAM") and IIS' approach to privacy breaches and investigations.

KPMG's GIM is used globally for investigative services. The methodology is the culmination of worldwide leading practices and is used by KPMG professionals as guidance when delivering investigative services. The methodology ensures the application of proven investigative techniques and processes. The use of KPMG's GIM also means a consistent and reliable approach is applied to all investigations.

KPMG's IAM is a proven methodology, used globally for internal audit services. KPMG's IAM is a risk-based process-focused methodology that helps the auditors understand an organisation's core business and objectives, the risks that threaten those objectives, and the relationships between those risks and the controls in place to mitigate the risks. The engagement was undertaken in accordance with recognised project management methodologies relevant to a project of this nature.

The IIS Methodology for a privacy review of an organisation's existing operations goes beyond simply compliance with privacy law and addresses wider privacy challenges and opportunities including allocation of risks and individual trust. The IIS methodology:

- Takes account of the guidance material prepared by the New Zealand and other Privacy Commissioners internationally, including Personal Information Protection and Electronic Documents Act Self-Assessment Tool published by the Office of the Privacy Commissioner of Canada and the Privacy Audit Manuals published by the Privacy Commissioner of Australia.

- Draws on privacy best practice including the concept of Privacy by Design developed by the Information and Privacy Commissioner Ontario, Canada.
- Applies the IIS "Layered Defence" approach which recognises that effective privacy protection is multi-dimensional and applies a number of possible tools at layers relevant to an organisation including "business as usual" good practice, application of the law, technology, governance and safety mechanisms including easily accessible and responsive complaints mechanisms.

The Independent Review Team made its assessments against the requirements of the Privacy Act including the IPPs, the HIPRs in the HIPC and current best practice in management generally and in privacy management. The framework used to assess privacy management practices is set out in section 3.4.

The investigation and assessment was performed through a combination of the following activities.

3.3.1 Reviewing relevant legislation, codes of practice, and relevant ACC policies, standards, processes, procedures and practices

The Independent Review Team familiarised itself with ACC's role and functions, its regulatory obligations, its organisational structures and its policies and procedures for handling personal information. This background information informed the targeting of further work including the interviews conducted and the testing of privacy controls.

3.3.2 Undertaking interviews with relevant personnel

The Independent Review Team conducted over 150 interviews with ACC staff throughout the organisation over the period of the Independent Review. The interviews were designed to gather information about ACC's role and functions and its practices in collecting and handling personal information. They also contributed to the assessment and to the confirmatory testing of practices and approaches.

The approach was to cover a comprehensive range of business units throughout a selection of ACC locations nationwide. This included certain business areas viewed as having higher access to personal information due to the nature of their functions or the volume of claimant information they handle. The interviews covered a mix of varying levels of staff and management both at the Corporate Office, the Sensitive Claims Unit, six branches from various locations across the North and South Island and two Service Centres. This covered the multiple teams involved in the end-to-end claims management process for the various categories of claims.

Interviews were also conducted with a number of non-client facing staff from the Corporate Office including members of the Executive Management. The areas interviewed included the Government Services team, Research, Legal, Risk, Injury Prevention, Assurance Services, Business Intelligence, Actuarial, the Office of the Complaints Investigator and the Investigations team.

These areas were targeted to provide insight into the access levels and the use of claimant information by staff not involved in claimant rehabilitation and case management. For a detailed summary of the business units covered and the number of staff and external stakeholders interviewed during the review process, refer to Appendix 3.

3.3.3 Undertaking consultation with other external stakeholder interests

During the review the Independent Review Team also sought input from a range of external stakeholders including claimants, advocates and associates. Input was sought as appropriate by correspondence, interview and a workshop with external stakeholders.

3.3.4 Evaluating the design effectiveness of the controls, taking into account good practice, regulatory requirements, risk assessment

In this phase the Independent Review Team evaluated ACC's privacy management and compliance approach when handling personal information with a focus on system design and controls and drawing on the information obtained through its interviews with ACC staff. In undertaking its evaluation the Independent Review Team considered:

- ACC's risk management framework and its management of privacy breaches and complaints.
- Policies, procedures and practices relevant to the security and privacy of claimant information.
- The roles and responsibilities of ACC staff in relation to the security and privacy of claimant information.
- Approach to compliance with the IPPs and the HIPRs including the privacy information provided for clients on forms, in guidance material and on its website.
- The adequacy of the training and other privacy related resources available and how effectively these were being utilised by staff.
- The general attitude and strength of staff culture in relation to privacy and security of information.

3.3.5 Undertaking targeted detailed testing to confirm the operating effectiveness of the controls

To assist in making its assessments the Independent Review Team performed walkthroughs of the following systems and processes:

- ACC's EOS – processes observed included the registration process, uploading of emails containing client information, logging contact with clients, and monitoring work load/jobs to be completed.
- The systems for front-end scanning of hard copy documents for uploading to EOS and the current backlog of scanned documents.
- InFact, a reporting tool currently in the final stages of development. This is already being widely used throughout the organisation to reduce the need to circulate management reports via email.
- LiMe, ACC's learner management system, where online training modules are available, for example, "Privacy and Managing Requests for Information" and "Information Security".
- Action Remedy, the system used by Government Services and the Chief Executive's office to record privacy complaints.
- The process followed by the Office of the Complaints Investigator in undertaking an investigation.
- Responding to requests from clients under IPP 6/HIPR 6 and/or the Code for access to personal information ACC holds about them (within ACC called a "Copy File" request) including to a request for an "IT sweep", where an organisation is called upon to review all of its electronic systems to identify comprehensively all personal information held about an individual.

3.3.6 Comparison with other organisations

The task of the Independent Review Team included assessing whether ACC's privacy management practices were appropriate and effective, including how they compared to the risk management and compliance cultures of similar private and public sector organisations, and if its practices equated to good privacy practice from these perspectives.

Comparisons were completed with a number of organisations on their privacy programmes. The survey group included two major banks, a DHB, two insurance companies and three large data handling government agencies. The analysis focused on structures, education and training, breach and complaint management and resolution, responsibilities and reporting around privacy.

3.4 Privacy management good practice framework

In making its assessments the Independent Review Team drew on its combined experience of good practice and also on privacy good practice advice developed in New Zealand and a number of other international jurisdictions. The Independent Review Team has represented the framework it applied in Diagram 1 below. The key concepts underpinning the diagram include:

- The Independent Review Team's view that privacy should be driven by the "tone at the top" and embedded through models such as KPMG's three lines of defence where business owners are the first line of defence, standard setters are the second line of defence, and assurance providers are the third line of defence. Through this process the importance of privacy would be continuously communicated and modelled, with a focus on consistent messaging.
- Privacy by Design ("PbD") – a strategic approach to privacy pioneered by Dr Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, which has evolved into a comprehensive approach to embedding privacy-sensitive thinking into all aspects of an organisational or system-wide initiative, starting with three foundational aspects:
  - Accountable business practices
  - Information technology that preserves or enhances privacy
  - Physical design and infrastructure of premises that contain personal information[4].
- Guidelines prepared by the Office of the Privacy Commissioner of Canada
  - *PIPEDA Self-Assessment Tool, Personal Information and Electronic Documents Act* and
  - *Getting Accountability Right with a Privacy Management Programme*[5].

Privacy management good practice framework

Diagram 1

[4] More information about PbD is available at http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/ and http://www.privacybydesign.ca

[5] The documents are available from the Office of the Privacy Commissioner of Canada website at http://www.priv.gc.ca/information/index_e.asp

At the centre of a good practice privacy framework is a strong Culture for respecting individual clients and their personal information. The Board and Executive demonstrate commitment to privacy management by combining governance and oversight with appropriate tools and resources that will help drive and foster a culture of protecting personal information. An effective leadership structure, supported by a privacy programme and accountability measures will embed privacy in decision-making thereby assisting to create a culture where everyone has ownership and responsibility for protecting personal information and doing the "right thing".

Surrounding and supporting a good practice privacy framework are the fundamental enablers of People, processes and systems in the organisation. All three of these factors are critical for ensuring that respect for privacy is an integral feature, embedded in the organisation's mindset and business-as-usual activities. Effective Communication is required throughout the organisation for effective privacy management. This includes effective reporting protocols to management and the Board, as well as the Board effectively communicating their strategic vision and values to the organisation.

The role of Board Governance is to establish the values of the organisation and a consistent strategic vision that sets an appropriate tone and culture of respecting privacy and personal information within the organisation. The Board also clearly defines their risk tolerance and appetite in relation to privacy management. The Board ensures that they communicate their expectations clearly to leadership and that their approach aligns to privacy, risk and compliance functions. Independent assurance activities should be undertaken and oversight maintained with a focus on privacy management and security of information, looking at current business processes, systems and practices and ensuring a clear eyed view of the future.

An appropriate Leadership structure is implemented and maintained to ensure there are defined levels of responsibility and accountability for privacy management within the organisation. The leadership structure should ensure a clear line of responsibility for developing a well defined privacy strategy within the Executive, reflecting the overall strategic direction established by the Board. This includes ensuring privacy management is visible throughout all areas of the organisation and promoting a culture where respecting personal information is a clear priority. The importance of privacy management should be reflected in the weighting given to privacy in recognition and reward structures, and the establishment of an effective compliance framework, all of which should lead to an effective compliance culture.

The Privacy Programme represents the implementation of the strategy set by the Board. The Privacy strategy must be articulated into a plan, with adequate resources and effective monitoring of performance against plan. Appropriate tools and resources that support privacy and personal information include comprehensive policies, training and education and clearly defined roles and responsibilities of privacy resources. The programme will be led by a Privacy Officer who is accountable to the Executive with responsibility for privacy and be given the responsibility for the delivery of strategic responsibilities including the authority of oversight, design, implementation, monitoring and reporting of privacy policies and ensuring appropriate compliance systems and control measures are in place. "Privacy by design" for new programmes and "privacy by redesign" should be a fundamental part of developing business processes and verified by Privacy Impact Assessment ("PIA"). The programme should focus on all of the IPPs/HIPRs, recognising that all contribute to managing the risk with associated client personal information and in particular minimising the risk of data breach. The Privacy Programme needs to be reviewed and its functionality assessed regularly.

Accountability is essential to complete the cycle in order to ensure that the programme is being delivered as intended, undertake systematic root cause analysis to expose and address systemic issues, to provide insight to where change or adaptation might be needed and to hold all levels of the organisation to account. Accountability measures for delivery of the privacy programme should be consistent with overall organisation performance and should include KPIs for all staff. Client satisfaction surveys are some of the most essential metrics to include in the suite of accountability measures. Effective accountability depends on roles and responsibilities of staff members reflecting the broader privacy strategy and being clearly defined within the privacy programme. To be effective, accountability measures will need to be supported by appropriate, consistent systems and processes for recording, monitoring and reporting privacy breaches.

4 Auckland Privacy Breach – findings

4.1 Investigation of the unauthorised release of information

The Independent Review Team investigated the circumstances of the Breach by the RIS Team on or about 5 August 2011, specifically to:

- Ascertain the cause of the information release by the RIS Team to the Client; and
- Assess ACC's response or actions upon being made aware of the Breach:
  - i. On or after 5 August 2011
  - ii. On or about 1 December 2011
  - iii. In March 2012.

The findings of this investigation detailed below are based on information obtained from, and meetings with, the Client, relevant ACC staff and other parties, external from ACC, who may have held information relevant to the investigation. A large amount of information was provided to, and considered by, the Independent Review Team with regard to the Breach. The information referred to in this section is that which the Independent Review Team considers to be most critical to address in accordance with the Terms of Reference for the Independent Review.

4.2 What happened

On 1 August 2011, the Client sent an email to the RIS Manager. The purpose of the email was to follow up on a complaint previously made by the Client regarding a medical adviser at ACC.

The RIS Manager was involved in responding to the Client in this particular circumstance because the complaint was an HR issue and not an operational issue regarding the Client's claim which would have been handled by the Client's case manager.

On 5 August 2011, the RIS Manager was drafting a response to the Client. At the same time, the RIS Manager was reviewing an internal monthly management report which had been distributed via email by the National Manager RIS to the regional RIS managers. The management report related to the status of reviews with DRSL of RIS clients. In the course of the drafting, the RIS Manager inadvertently clicked and dragged the email containing the management report such that it became attached to the response email being drafted by the RIS Manager and sent to the Client. The management report contained two embedded spreadsheets, that contained personal information about 6,748 ACC clients. A detailed explanation of the information contained in the spreadsheets is attached as Appendix 5.

The RIS Manager was not aware the internal email was attached to the Client response until being asked to search all correspondence with the Client by the National Manager RIS when the Breach was made public on 13 March 2012. At that time, the RIS Manager did not know how the internal "FW: Monthly review report" email was attached to the email response to the Client. Given that on 5 August 2011, the RIS Manager was reviewing the internal monthly management report at the same time as composing the response to the Client on two independent monitors, the most likely explanation is that the internal email was inadvertently dragged from the inbox into the Client response email sometime during its drafting and before sending.

In summary, the reason for the unauthorised release of personal client information was human error. ACC was not aware at the time that the Breach had occurred on 5 August 2011. No actions were therefore taken by ACC at that time.

On 16 August 2011 the Client emailed a response to the RIS Manager which was copied to the OPC and the Ombudsman's Office. The email of 16 August 2011 to the RIS Manager did not mention the Breach, and as discussed later below, the Client advised the Independent Review Team of not being aware of receiving the Breach information until 26 October 2011. In the email thread was the original email sent by the Client to the RIS Manager dated 1 August 2011 and the RIS Manager's response dated 5 August 2011. There were no attachments to the email and there was no evidence of an attachment being sent by the RIS Manager to the Client in the email dated 5 August 2011. During an interview with the Independent Review Team, the Client stated the reason for copying the OPC and Ombudsman's Office was because the Client thought ACC was refusing a request to access the Client's own personal information. The reason for copying the OPC and Ombudsman's Office therefore had nothing to do with the Breach.

The OPC and the Ombudsman's Office have confirmed receipt of the email dated 16 August 2011. They also confirmed the email did not contain any attachments or mention any privacy breach by ACC. As a result no further action was taken by the OPC or the Ombudsman's Office.

On 1 September 2011 the Client contacted a member of ACC's Board by email to arrange a meeting to discuss "*… a number of issues regarding ACC – compliance and personal*". The Client met that Board member on 14 September 2011 to discuss the Client's concerns with the way ACC was handling claims and managing personal information and specifically the Client's claim. The Client did not mention anything about the Breach at this meeting, as the Client was unaware of it at that time. Later that same day the Board member sent an email to the Chair of the Board about the meeting with the Client and the issues raised by the Client. This led to ACC setting up a meeting with the Client, which was arranged for 1 December 2011.

The Chair forwarded the email he received from the Board member to the Board and Corporate Secretary on 16 September 2011. On or around 4 October 2011, the Board and Corporate Secretary asked the Northern Area Manager, who at the time was the Acting National Manager ACC Claims Management Network ("Acting National Manager Claims") to organise a meeting with the Client to discuss the issues raised during the 14 September 2011 meeting.

On 14 October 2011 the Client sent an email to the Board member she met on 14 September 2011 and copied in the Chair and the Board and Corporate Secretary. The email raised concerns about ACC's alleged lack of respect for client rights and for not complying with the Code. This email was forwarded to the Acting National Manager Claims on 17 October 2011. A meeting was then arranged to be held on 1 December 2011 at the premises of Johnson and Associates (Chartered Accountants), 202 Ponsonby Road, Auckland.

On 26 October 2011 the Client forwarded the email received from the RIS Manager to the State Services Commission ("SSC") including the monthly management report. The purpose of the email was to inform the SSC about the circumstances surrounding the Client's claim with ACC. The Client did not inform the SSC about the Breach. The SSC was not aware that it had received the spreadsheets containing the personal information until 23 March 2012. The Senior Advisor, Integrity at the SSC informed the Independent Review Team that "*This email was one of 18 emails containing 65 attachments sent [from the Client to the SSC] within a 90 minute period*".

The Client informed the Independent Review Team that it was only after sending the 26 October 2011 email to the SSC that the Client looked in detail at the attachment to the 5 August 2011 email from the RIS Manager noting the extent of the personal information included in the spreadsheets embedded into the attached monthly management report. The Client advised the Independent Review Team that this was the first the Client became aware of the Breach.

The Client considers that there were two possible occasions before 1 December 2011 when ACC could have identified the Breach. The first was when the email of 5 August 2011 was printed and scanned into the EOS and the second was when the Client made a Privacy Act request and was

provided with a copy of the 5 August 2011 email that had been scanned into the EOS. The Independent Review Team found that only the 5 August 2011 email was scanned into the EOS but not the embedded spreadsheets that were attached to that email (which included the personal information). As such the Breach was not discovered, and nor could it reasonably have been discovered, on either of these occasions by ACC.

The Independent Review Team has found no evidence that ACC was aware of personal client information being sent to the Client until the meeting held between the Client and two senior ACC Managers on 1 December 2011.

ACC was first notified of the Breach on 1 December 2011 during the course of a meeting between two senior ACC Managers ("ACC Managers") and the Client. The Client made a voice recording of the meeting without the knowledge of the ACC Managers. While the Independent Review Team was not given a copy of this recording, four members of the team were given permission and listened to the recording of the 1 December 2011 meeting on 28 June 2012 and again on 9 August 2012.

Those present at the meeting included the Client, the Client's support person, the Northern Area Manager and the National Manager RIS. A list of 45 alleged breaches by ACC of legislation, guidelines and codes was prepared by the Client prior to the meeting on 1 December 2011. The list, which included reference to the Breach as one of the 45 alleged breaches, was referred to several times during the meeting; however, the ACC Managers did not receive the list until the end of the meeting. This was because it was not the intention of the Client to address each and every alleged breach on the list at the meeting, but to discuss a proposal for a way forward with regard to the Client's own claim.

ACC understood that the purpose of the 1 December 2011 meeting was to listen to the Client's concerns regarding the Client's rehabilitation with the view to agreeing a way forward.

In addition to discussing the Client's rehabilitation, at the meeting the ACC Managers were informed that the Client had received an email from ACC containing personal information relating to the Client "*plus about six and a half thousand other claimants…*"[6]. This was the first time the Client had informed ACC about receiving the personal information.

The Northern Area Manager asked whether ACC was aware of the Breach to which the Client answered "*No*". The National Manager RIS stated later, "*If there's a privacy breach that has originated from ACC, then absolutely we should be aware of it. Because if it relates to other people, then we need to make them aware that there has been a privacy breach*".

The Client informed the ACC Managers that the Breach information consisted of "*…about six and a half thousand other claimants, and names and claim numbers and conditions and details*". The ACC Managers were informed that the Client received the information via email but were not given any other information that would have helped identify the source such as specifically who had sent the information or the date the information was sent. The ACC Managers did not ask for any further details either. However, the National Manager RIS told the Independent Review Team that he inferred from what was said at the meeting that he was involved in emailing the personal information to the Client.

The National Manager RIS asked if the Client had deleted the email. The Client answered, "*I don't delete any emails. I've got every email since the day my claim started…*". Later the National Manager RIS stated "*…one of the things we clearly want is to get hold of that*". The Client's support person agreed to this stipulation and stated "*that it's never going to be used*".

[6] This is the number referred to in the interview with the Client. The actual number was 6,748.

Towards the end of the meeting the ACC Managers were given a list, prepared by the Client, of 45 alleged breaches of legislation, guidelines or codes that the Client considered ACC had made in dealing with the Client. Following the meeting, the ACC Managers reviewed and discussed the issues listed, noting that they were general in nature and did not contain any detail or evidence to support the Client's allegations. The Client informed the Independent Review Team during an interview that the second item on the list, "Extensive disclosure of other claimant's information to [the Client]" referred to the personal information received by the Client on 5 August 2011.

A reporter from The Dominion Post contacted ACC's lead media advisor on 9 March 2012 and advised that the newspaper was going to publish a story regarding a large privacy breach and requested a response from ACC. The Client informed the Independent Review Team in an interview that a portion of the information related to the Breach, with all personal information redacted, was provided to a reporter at the Dominion Post on 1 March 2012.

Ten minutes following receipt of the email from the Dominion Post, the lead media advisor forwarded the information request to ACC's Privacy Officer, copied to ACC's General Manager People and Communications, the Board and Corporate Secretary and the Chief Executive.

In an interview with the Independent Review Team, the ACC Chief Executive said that he requested the media team to investigate the request made by the reporter. As a consequence, the National Manager RIS was forwarded the email that had come from the reporter. The National Manager RIS responded by confirming he had previously searched his email correspondence but did not find anything and that a request had been made to have the information returned. A response was provided to the reporter from the Dominion Post.

On 13 March 2012, an article was published in The Dominion Post publicising that ACC had emailed the details of 9,000[7] claims to a person who should not have received them. The information referred to was the information the RIS Manager emailed to the Client on 5 August 2011.

During his interview with the Independent Review Team, the National Manager RIS said that on reading the article he realised that he was wrong to have inferred from what was said at the 1 December 2011 meeting that he was the source. He phoned the RIS Manager on the morning of 13 March 2012 and requested the RIS Manager to check all correspondence with the Client to try and find the information.

In an interview with the Independent Review Team, the RIS Manager confirmed receipt of a phone call from the National Manager RIS asking to search correspondence with the Client for information the Client was not supposed to receive. It was during this search that the RIS Manager located the email sent to the Client that contained personal information of other ACC clients. The RIS Manager phoned the National Manager RIS and told him what had been found. The email was forwarded to the National Manager RIS.

The Client forwarded the email that was received from the RIS Manager dated 5 August 2011 to ACC's Internal Legal Counsel on 13 March 2012. The Internal Legal Counsel forwarded the message to the General Manager, Claims Management and the National Manager Claims also copying the Board and Corporate Secretary. This is the first evidence the Independent Review Team found of the Client providing to ACC full details about the personal information received on 5 August 2011.

[7] This is the figure reported by the Dominion Post.

4.3 ACC response to the Breach

As previously discussed, based on the balance of evidence, the Independent Review Team determined that ACC were unaware of the Breach prior to 1 December 2011. In an interview with the Independent Review Team the Client confirmed that ACC was not informed directly by the Client about the personal information received on 5 August 2011 until the meeting on 1 December 2011.

The Independent Review team noted that the ACC Managers took five actions during and following the 1 December 2011 meeting related to the Breach.

1. During the 1 December 2011 meeting, the ACC managers asked if ACC were aware of the breach and if the Client had deleted the email containing the Breach information. The Client gave assurances at the time that the email was still in the Client's possession and that it had not been shown to anyone else. However, the Client had forwarded the Breach information to the SSC on 26 October 2011, although the Client says they were not aware the email contained the Breach information at the time it was sent.
2. At the end of the meeting, the National Manager RIS gave an undertaking to respond to what was raised in the meeting by 9 December 2011.
3. The Northern Area Manager, following the meeting, sent an email on 1 December 2011, informing the National Manager Claims and the Board and Corporate Secretary of what happened at the meeting. This email included the fact that they had received a list of alleged breaches by ACC of legislation, guidelines and codes. The Northern Area Manager also had a discussion with the National Manager Claims regarding the meeting on the afternoon of 1 December 2011.
4. Following the meeting, the National Manager RIS, in response to the fact that he inferred from what was said at the meeting that he was the source of the email to the Client, performed a search of his emails with the Client and the Client's support person that may have contained the personal information. The search did not find any such emails.
5. The National Manager RIS drafted a letter to the Client, which was reviewed by the Northern Area Manager and National Manager Claims. The letter to the Client, sent on 9 December 2011, addressed some of the issues the Client raised in the meeting regarding her rehabilitation. The letter contained the following paragraph which asked for the personal information the Client had received to be returned.

   > *"At the meeting you state 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".*

The National Manager RIS confirmed that this was the only time that ACC requested in writing that the information be returned by the Client. We have not found any evidence to the contrary.

The Independent Review Team was advised that there was an intention by ACC to request more information from the Client regarding the list of 45 alleged breaches so they could be investigated. However, ACC's immediate focus was responding to the issues raised in the meeting on 1 December 2011 regarding the Client's rehabilitation. This was done in the letter sent to the Client on 9 December 2011. Communication with the Client regarding her rehabilitation continued through 22 December 2011 and again on 21 February 2012 and 22 February 2012. However, none of these communications after 9 December 2011 referred to the personal information related to other ACC clients (i.e. the Breach).

Between the letter sent on 9 December 2011 and when the Breach was made public by the media on 13 March 2012, ACC took no further action in relation to being informed that the Client had been sent an email with personal information relating to "*... about six and a half thousand other*

claimants..." or in relation to the other 44 alleged breaches by ACC of legislation, guidelines or codes. It should also be noted that the Client did not return the personal information to ACC during this time, but did forward a copy of the original email to ACC on 13 March 2012.

Following the Breach being made public on 13 March 2012, ACC immediately conducted an internal review to understand the cause of the Breach, and to understand ACC's file access, file management and file selection systems.

In addition, the following actions were taken:

- On 13 March 2012 ACC's Manager, Legal Services was asked to contact the Client's lawyer to request the information be returned to ACC and destroyed, and then verify that all electronic information was erased from the Client's computer system. On 13 March 2012 the Client returned the file to ACC and provided an assurance that the information had been destroyed that day by an independent third party IT specialist who removed all related computer records from the Client's computer. On 14 March 2012 the independent third party IT specialist provided verification of this via a certificate of destruction.
- An incident team was formed to manage the Breach. The team's first task was to establish a call centre to contact all the people who had been affected.
- A free-phone number was established for people to call if they were concerned about whether they may be affected by the Breach.
- The structure of the management report was changed so that it is no longer possible to connect the classification Sensitive Claims Branch with an individual client name and reference number, to further protect the privacy of sensitive claims clients.
- A process was started to update ACC's email system so that whenever an electronic file is sent out of ACC the system will request authorisation from the sender before it is sent. The update was fully implemented in July 2012.
- The footer on ACC's emails was updated to make it clear to advise ACC if the recipient receives any information they should not have, and it is the recipient's responsibility for doing so.
- The reporting lines for privacy issues were changed to the Board and Corporate Secretary who reports to the Chief Executive daily on activity. The information the Chief Executive now receives is status of open and closed privacy issues, status change by day, status change by week and root cause analysis.
- A meeting of all the Privacy Champions of ACC was held in Wellington during the week beginning 19 March 2012 to discuss ideas for improving ACC's management of privacy.
- All staff were asked to complete an online privacy training module and were required to pass the associated test with a required pass rate of 90%.

The Chief Executive also wrote a report to the Minister for ACC dated 16 March 2012 which contained an explanation of how the Breach occurred and ACC's response. This report was published on ACC's website.

On 23 March 2012, the OPC in conjunction with the ACC Board advised the media that an independent review of ACC's information security policies and practices was being conducted following the Breach, and published the Terms of Reference of the review.

The ACC Board and management also commenced a process of considering the structure and resourcing of the privacy team and assessing the longer term impacts of the Breach and other privacy related issues which have led to changes in the way in which privacy will be managed going forward.

4.4 Appropriateness of response

The Independent Review Team considered ACC's response from three perspectives:

1. The release of unauthorised information to the Client on 5 August 2011.

   ACC did not take any action as it was not aware of the Breach until 1 December 2011.

2. The meeting on 1 December 2011.

   At the meeting the ACC Managers were advised that the Client had received an email containing personal information relating to the Client "*plus about six and a half thousand other claimants…*". However it was only following the meeting, in a letter sent to the Client on 9 December 2011, that an explicit request was made for the return of this information to ACC and assurances that the no one else had copies of the information.

   At the meeting the ACC Managers were provided with a list of 45 alleged breaches which they discussed and reviewed subsequent to the meeting. However no specific action was taken to investigate these alleged breaches.

   After the meeting on 1 December 2011, ACC's initial focus was on progressing the Client's rehabilitation. The Independent Review Team was advised that the Client's rehabilitation took precedence for two reasons. Firstly, the ACC Managers believed the meeting was arranged to progress the Client's rehabilitation and were therefore focused on that. Secondly, ACC did not have enough information to begin an investigation because the Client did not give ACC sufficient details about the personal information received or the other 44 alleged breaches.

   The Independent Review Team was advised that ACC's intention was to ask for further details of the Breach once the Client's planned rehabilitation was agreed, but this did not occur prior to the Breach being made public by the media.

   The Independent Review Team considers that in light of being advised of the extent of the Breach information and being presented with a list of 45 alleged breaches, these issues should have been escalated to the Privacy Officer and/or the Office of the Complaints Investigator soon after the 1 December 2011 meeting. ACC should also have made a more concerted effort to have the Breach information returned and undertaken a more extensive internal investigation into how the information was sent to the Client.

3. The actions following the media release.

   On becoming aware of the full extent of the Breach on 13 March 2012 ACC's response was appropriate in terms of escalation, investigation and putting in place a process to contact all those potentially impacted by the Breach. Significant senior resources, including involvement of the ACC Board and Chief Executive, were actively involved in responding to and managing the impact of the Breach.

   ACC in consultation with the Privacy Commissioner also established an independent review and has demonstrated its commitment to addressing the issues raised by the Independent Review Team. Given the seriousness of the privacy issues ACC's response was appropriate.

4.5 Systemic issues arising from the Breach

The Independent Review Team has concluded that the Breach was caused by human error. However, there are certain systemic issues as well as contributing factors that led to the Breach and if not rectified could lead to additional occurrences of significant privacy breaches. These are summarised as follows:

- Technology and business practice issues, including extensive use of spreadsheets for management monitoring and reporting purposes and desktop configuration that allows multiple monitors to be open at any one time.
- Culture where the importance of personal information and respecting individual's personal information is not consistent and is often de-emphasised over dealing with the management of the claim/claimant.
- Privacy management, including lack of clear accountability for addressing privacy issues when they are raised (including investigating/following up on issues) and for ensuring that client issues, including privacy matters, are dealt with in a holistic way.

These issues have been considered more fully in Section 8 of the report and a number of recommendations made to ensure these issues are addressed.

5 Overview of ACC's approach to privacy

5.1 ACC's privacy management approach

ACC has in place a range of measures and strategies to meet its Privacy Act and HIPC obligations. The key elements are outlined briefly here as a background to the Independent Review Team's findings and recommendations in Section 8 of the report.

5.1.1 ACC Board

ACC's governance and management arrangements start at the ACC Board and Executive Management level. At this level there is general oversight on privacy, for example yearly assessments of privacy compliance for external audit processes and high-level consideration of privacy in ACC's risk processes.

The Executive Management has set specific direction on certain privacy related matters, such as steps to be taken following a privacy breach.[8]

5.1.2 Privacy Officer role

As required by Section 23 of the Privacy Act, ACC has appointed a Privacy Officer; the role has been given to the Manager of Government Services. The role reports to the General Manager of Governance, Policy and Research. The Privacy Officer role is not formally defined, other than as set out in the Privacy Act. The Privacy Officer indicated that her key privacy responsibilities are:

- Handling privacy complaints received directly from claimants, referred by the Privacy Commissioner or escalated from the branches and corporate office.
- Developing privacy policies and privacy input to policies.
- Providing input to the development of privacy training.
- Supporting the Privacy Champions' network.

The Privacy Officer also provides some advice on privacy matters to Privacy Champions, branch staff, management and Executive Management; this is often in the context of a privacy breach.

The Privacy Officer receives reports on privacy breaches via the Privacy Champions. From time to time the reports have been collated and analysed, however there is currently no regular process to provide feedback to units and branches. Recently the role has included reporting to the Executive Management and the ACC Board.

The Privacy Officer's duties are supported by the staff in her team. Government Services currently has a team of 17.3 FTE staff, with approximately 5% of their time being dedicated to privacy related issues.

5.1.3 Privacy Champions

ACC has had a network of Privacy Champions established within various business units throughout the Corporation since 2005. Traditionally these have been within the client-facing areas of the business, however since the Breach there has been a drive to ensure every business unit in the organisation has a Privacy Champion. The Privacy Champions are expected to give advice and

[8] *Steps to be taken following release of claims documents to unauthorised parties* ACC 2009

guidance on privacy matters and actively promote privacy to staff within their area. Their responsibilities also include maintaining a risk register and submitting monthly reports to the Privacy Officer detailing all breaches and near misses.

Privacy Champions attend an annual workshop that is run by Government Services, outlining their role and responsibilities, including case studies of privacy breaches that have occurred.

5.1.4 Privacy training

Since 2004, as part of the induction programme, all new staff joining ACC have been required to complete a privacy module on "Privacy and Managing Requests for Information". The module focuses on ensuring staff understand their key legislative accountabilities and responsibilities under the Privacy Act, the Official Information Act 1982 ("OIA") and the HIPC.

Following the Breach, ACC has made it a requirement for all staff to re-sit an annual refresher course on "Privacy and Managing Requests for Information". The refresher online privacy training is the same as the induction module, however there is a work plan to have a further eight privacy modules developed and rolled out over the next two years. The initial module will focus on increasing Privacy Principle awareness.

Security training covering broad IT security practices is provided to all staff; reliance for security awareness training is primarily placed on online training which is carried out when a new staff member joins ACC. This training is not required to be repeated on a periodic basis. As part of their induction programme, staff are also required to complete the "Information Security" online module.

5.1.5 Privacy breach management

Throughout ACC a "privacy breach" is commonly defined as the unintentional disclosure of personal information to a third party. ACC has in place a system of managing breaches, or near misses where ACC becomes aware of an incident. ACC's current approach to breach management focuses on containing and recovering the material relating to the breach. General procedure following a privacy breach is for the staff member responsible to notify their manager, who will then contact the recipient of the information. The manager will aim to get assurance from the third party that the information will be destroyed or returned to ACC. The staff member responsible or their manager will also ring the claimant whose personal information has been disclosed and apologise for the breach. In some cases a letter may be sent in addition to this. There is also some additional guidance in place to refer breaches to the OPC.

5.1.6 Privacy complaints lodged by clients

Privacy complaints may be handled by ACC front line staff or by the Privacy Officer.

ACC also has an Office of the Complaints Investigator located in the Corporate Office. Functions include providing an impartial complaint investigation into complaints about service delivery to clients and for complaints made under the Code and representing ACC at reviews for decisions made under the Code.

ACC receives privacy complaints through a number of channels including:

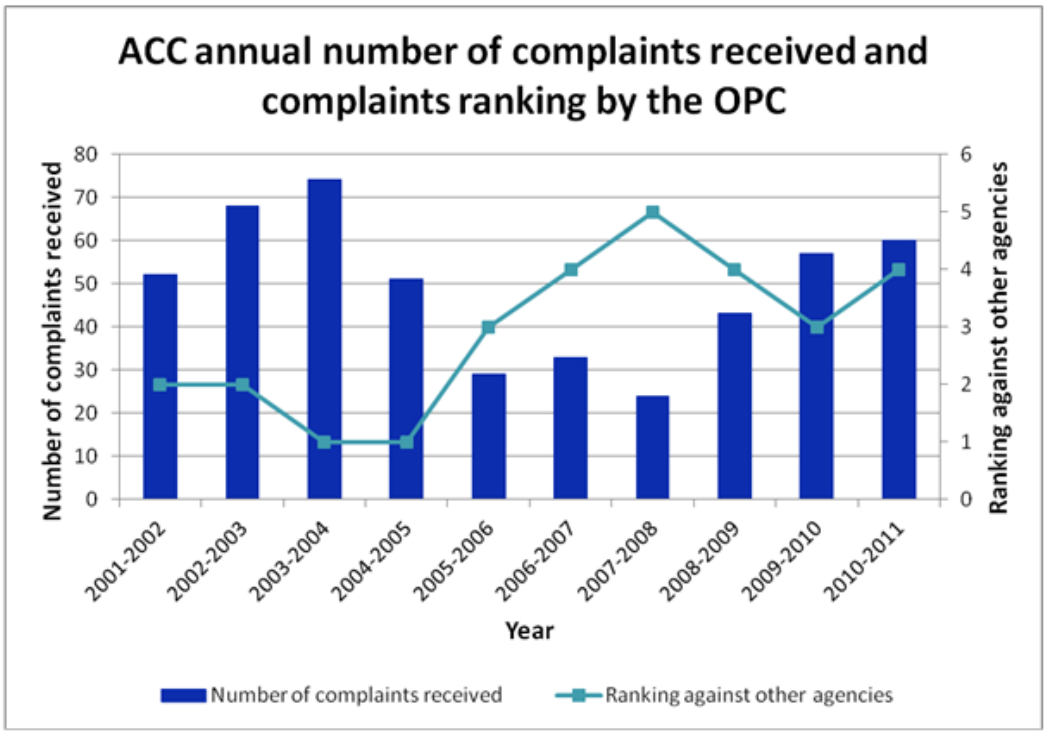
- Directly from claimants via the case manager or the Customer Service Support team, which could be about a possible breach of the IPPs or HIPRs, or the Code.
- Complaints made under Right 7 of the Code to the Office of Complaints Investigator.
- Complaints received by the Privacy Commissioner.
- Complaints to the Ombudsman.

Complaints received through the OPC or the Ombudsman are handled by the Privacy Officer, as well as any complaints or breaches escalated from the branches. Occasionally, claimants will also contact the Privacy Officer directly. Any complaints made under Right 7 of the Code will be independently investigated by the Office of the Complaints Investigator.

5.1.7 Complaints to the OPC and the Ombudsman

ACC is a complex organisation that handles very large amounts of personal information much of which is very sensitive to its clients. Like any organisation of similar size and complexity, it also has regular complaints about its handling of personal information in relation to privacy.

There are some measures of how the number of complaints received about ACC have trended in recent years. Of the few measures available, ACC has regularly been in the top five in the OPC's ranking of agencies by number of complaints received. This is not unexpected given the nature of its services and the type of information obtained about individual claimants. For example, in 2003–2004 they ranked number one, with 74 complaints[9]. However, ACC has KPIs aiming to reduce the number of privacy complaints and in 2010–2011 ACC ranked number four on the list with 60 complaints[10]. However, these figures must be treated with caution in the absence of meaningful comparative analysis about relative size and complexity and sensitivity of information in other organisations.



[9] *Annual Report of the Privacy Commissioner 2004* available at http://privacy.org.nz/annual-report-of-the-privacy-commissioner-2004/

[10] *Annual Report of the Privacy Commissioner 2011* available at http://privacy.org.nz/annual-report-of-the-privacy-commissioner-2011/

The table below sets out the ranking of the top 5 respondent agencies, according to the number of complaints received annually about them by the OPC.[11]

Agency	2006-2007	2007-2008	2008-2009	2009-2010	2010-2011
Ministry of Social Development	1	3	2	2	2
Department of Labour (Immigration)	2	1	5	5	5
NZ Police	3	2	1	1	1
ACC	**4**	**5**	**4**	**3**	**4**
Department of Corrections	5	4	3	4	3

Formal documentation relating to "Processing requests for Information" was first implemented by ACC in 2001. This arose following a complaint to the Ombudsman, after a fax sent to a claimant at work was picked up by a colleague, who proceeded to deliver it to the claimant. ACC was found to have breached the claimant's privacy and as a result of the Ombudsman's findings, the complainant requested that ACC be required to implement formal processes. ACC also introduced one training module on privacy as part of their induction programme following the complaint to the Ombudsman.

5.1.8 Privacy breach and complaint reporting

ACC does not have a centralised reporting system for recording privacy complaints making it difficult to collate and analyse information relating to breaches or near misses. Current mechanisms for recording of privacy breaches and complaints include EOS, spreadsheets, Action Remedy and email communication. The reporting available for complaints is at a very high level and does not include privacy complaints received by the Privacy Officer or by the branches. It does not provide sufficient information to identify trends, systemic issues and risk areas. Additionally there is limited information available of complaints (including privacy breaches and near misses) received and handled directly by branches.

5.2 Privacy and security policies and procedures

ACC currently has various policies relating to the privacy and security of personal information with the primary resource being the Privacy Policy. This is located on ACC's intranet which is accessible to all staff and contains links to various privacy related documents, including all relevant legislation. In addition, ACC has a dedicated "claims management resource" portal located on the intranet. This contains all process and policy documents relating to claims management, including various privacy related processes such as "completing information requests", "when to release personal information" and "gaining client consent".

[11] *Annual Report of the Privacy Commissioner 2002-2011* available at http://privacy.org.nz/corporate-reports/?start=0

5.3 ACC's current collection and handling of personal information

5.3.1 Collection of personal information

The AC Act Section 279 – provides that ACC may collect information for the following purposes:

1. The Corporation may collect information for the following purposes:
   a) to enable a comprehensive claims database to be maintained.
   b) to facilitate the monitoring of the operation of this Act.
   c) to monitor and evaluate the nature, incidence, severity, and consequences of injuries.
   d) injury prevention.
   e) the provision of appropriate rehabilitation and treatment.
   f) the provision of appropriate compensation.
   g) policy development under this Act.
   h) determining the cost to society of personal injury.
   i) levy setting.
   j) scheme management.
2. The Corporation must collect—
   a) such information as is prescribed for the purposes set out in subsection (1)(a) to (i) by regulations made under this Act.
   b) information for such of the purposes set out in section 287 that are prescribed by regulations made under this Act.
3. Information prescribed for the purpose set out in subsection (1)(a) must include information about the circumstances of the personal injury, the nature and severity of the personal injury, and its consequences.

Sources of personal information include:

- Initially from a health service provider.
- From the individual concerned.
- From employers.
- From a range of specialist medical providers about condition and/or rehabilitation. This includes counsellors, psychologists, physiotherapists, chiropractors and occupation/medical assessors.
- From other government departments such as the Ministry of Business, Innovation and Employment (formerly known as Department of Labour), Inland Revenue Department and Ministry of Social Development (Work and Income New Zealand and Child, Youth and Family).

Information collected includes:

- Details from "ACC45 Injury Claim Form".
- Medical notes relating to condition and/or rehabilitation of specific injury.
- Vocational independence assessment.
- Coroner's interim and final certificate of findings (for Accidental Death cases).

ACC's initial source of information is the "ACC45 Injury Claim Form" which is submitted to ACC either by the claimant or their health service provider. The information provided on this form includes personal, accident and employer details. The need to collect additional information to that provided on the ACC45 will depend on the nature of the injury. Over 90% of the claims received by ACC are medical only and minimal, if any, additional information is required.

Cases in which the claimant requires time off work or needs special assistance are managed in the branch network. These, more frequently, require the collection of additional information relating to the condition and the rehabilitation of the injury. This information is collected from a range of medical providers such as General Practitioners ("GPs"), hospitals, physiotherapists, chiropractors and other medical assessors. Additionally personal information may be collected from other government agencies such as the Ministry of Business, Innovation and Employment, Inland Revenue Department and Ministry of Social Development (Work and Income New Zealand and Child, Youth and Family). ACC may seek non-clinical assessments such as building assessments. This would occur in cases where claimant's injuries have seriously affected their mobility and require structural adjustments to their house and/or workplace.

Claimants who have been receiving weekly compensation for a total of greater than 912 days are managed by the RIS unit. Due to the longer timeframe and complexity of these cases, the amount of information collected and held by ACC about these claimants is generally substantially greater than for other categories of claimants. Additionally, it is common for case managers to seek assessments to assess the claimant's ability to return to work.

Within ACC there are various specialist units that deal with unique injuries and the information collected varies accordingly. The Sensitive Claims unit will often require reports from psychologists and counsellors and for claimants under the age of 16 there may be a need to obtain additional information from Ministry of Social Development (Child, Youth and Family) relating to the guardianship of the child. Other units that may require specialist information due to the nature of the injuries they deal with include the National Serious Injury Service, the Accidental Death unit and the Lump Sum unit.

5.3.2 Use of personal information

The following is a summary of some of the ways in which personal information is used by ACC. This is based on information gathered during the Independent Review process.

- In cases where a claim is being managed by the branches, the information collected by ACC is used by the case manager to assess the claimant's eligibility for treatment, rehabilitation, special assistance and other forms of compensation relating to their injury. In some cases this may include review of a claimant file by the branch medical advisor to provide expert medical opinion with regards to case management.
- ACC line managers are provided with various reports to manage and benchmark their performance against other areas of the organisation. These are prepared by the Business Intelligence team and circulated nationally. A reporting portal "InFact" is in the final stages of development and will be used to reduce the number of reports circulated by email.
- One of ACC's core functions is injury prevention and, as outlined in the AC Act, personal information that is collected may be used for research into injury prevention. In cases where personal details are provided to an external party, claimants are considered vulnerable, claimants are contacted as part of the research proposal and programmes where the claimant's clinical treatment/rehabilitation is varied from standard care, approval by ACC Research Ethics Committee is required prior to commencement.
- As a part of the investigations process, the Investigations unit will access information from claimants, providers and levy payers. This information may include personal information.
- ACC receives a large amount of Official Information requests, which are handled by the Government Services team. This may include requests for statistics involving claimant personal information. The Government Services team is responsible for ensuring that any information provided does not include identifiable claimant information.

5.3.3 Disclosure of personal information from ACC

Disclosure of information includes but is not limited to:

- The client gives consent for ACC to collect and disclose information initially when they sign the "ACC45 Injury Claim Form". This includes any information necessary to determine cover and/or assess entitlement to compensation, as well as for the purposes of research into injury prevention and effective assessment and rehabilitation. If the claim is transferred to the branches to be managed by a case manager, the claimant will be required to sign an "ACC167 Authority for the collection and disclosure of information". This covers collection and disclosure of information for the same purposes outlined in the ACC45, with the main difference being that the ACC167 is a single purpose form. In the case of disclosure to lawyers/advocates and other external parties the claimant must give at least verbal consent, however in most cases signed written consent is preferable. This is recorded on the claimant's file in EOS.
- For the majority of claims ACC has minimal need to disclose information for case management purposes. As outlined in "Collection of Information" above, the amount of active case management required varies significantly depending on the nature of the injury. Accordingly the need to disclose personal information varies greatly depending on the complexity of the case. In particular factors such as the level of special assistance/services required and the period of time the claimant will require weekly compensation are relevant. For example to assess claimant eligibility for a lump sum payment, the claimant's information is provided to a lump sum assessor who gives the claimant a rating which corresponds to a set amount to be paid by ACC.
- Disclosure of information is typically to medical providers and other assessors for rehabilitation or to provide the assessment required by ACC. Information may be provided to other government departments such as the Ministry of Business, Innovation and Employment (formerly known as Department of Labour), Inland Revenue Department and Ministry of Social Development (Work and Income New Zealand and Child, Youth and Family).
- Additionally ACC discloses employer claims history reports to employers, detailing injuries that have occurred at their work place. The employer claims history report has the claimant's name, claim number, the accident date, and a description of the accident, recent costs and total costs.
- Claimants who are unhappy about a decision or the outcome of their claim, have the option to dispute the decision to the DRSL. When claims go to the DRSL a copy of the claimant file is prepared for the claimant and another for the DRSL. The DRSL returns their copy of the file following the completion of the review. In the event the claimant is still dissatisfied with the outcome, they have the option of taking their case to the District Court and thereafter to the Court of Appeal if still not satisfied with the outcome. In these instances the original copy of the file is provided to the Court, a copy is provided to the DRSL and the claimant also receives a copy. Following the completion of the case the Court and DRSL copies are returned to ACC.

5.3.4 Access to personal information

ACC has processes in place to respond to clients' request for access to personal information held about them. The process for providing "copy files" of the information held about them for clients is generally the responsibility of case managers. ACC does not limit the number of "copy files" requested.

Since 2005 ACC has been using EOS for claims management. Information received by ACC relating to the management of a claim will be kept on EOS. Information held on EOS is either at "Party level", the level at which all general claimant information is recorded, or at "Claim level", the level at which all information specific to the injury/claim is recorded. Since December 2010, all email correspondence relating to claim management has been uploaded to EOS. If claimants want access to the emails sent in relation to them prior to this period, they must specifically request an IT sweep.

For claims that originate prior to 2005 a physical file will exist as well as the electronic file held on EOS. Producing a copy file involves printing all documents held on EOS as well as photocopying the

physical file, which can be an onerous task as some files may have multiple volumes. This is generally tasked to the case manager. However, some branches employ temporary staff to manage the workload and others have the option of using third party contractors. ACC holds some physical files containing documents from before the Privacy Act was enacted. These documents often contain personal information of other claimants and such information must be removed prior to a copy file being provided to the claimant. It is a requirement throughout the branch network that all outgoing copy files receive a privacy check prior to being sent to the claimant.

5.3.5 Accuracy and correction

While ACC has many sources of claimant information, the majority of information collected and held comes from medical experts. A high level of reliance is placed on the providers to provide complete and full information.

When a claimant requests the correction of personal information relating to their personal details such as address or phone number, their details will be updated on EOS by the case manager. If the claimant is requesting a correction of a provider report, ACC will request the claimant provides a Statement of Correction outlining the disputed areas of the report. ACC will then provide this report to the provider. If the provider accepts the corrections, an amended report will be provided and uploaded into EOS, with the original report being deleted. If the provider does not agree with the changes, the Statement of Correction will be uploaded into EOS as part of the original report.

5.3.6 Storage and security

ACC has a focus on the security of its IT systems and data, including client information. This is reflected in the policies, standards and security practices in place.

Information relating to general claims can be accessed by any ACC staff member with EOS access. There are three classifications of claims which impose a restriction on access to claimant information. These are claims designated as VIP claims, sensitive claims and staff claims.

Formal policy allows for the VIP status to be allocated to the following categories, namely the Governor-General, Members of Parliament, Members of the Judiciary, ACC Board members and members of their immediate family.

Sensitive and staff claims are identified at registration through their injury code. Staff claims are transferred to Catalyst, an external party, for management of the claim. Sensitive claims are managed by the Sensitive Claims unit once registered.

6 Stakeholder input

During the review the Independent Review Team sought input from a range of internal and external stakeholders. Internal stakeholders included ACC Board members, managers and staff. External stakeholders included claimants, advocates, associates etc. A list is included in Appendix 3.

6.1 Internal stakeholders

Feedback from ACC personnel is reflected throughout the report and is consistent with a diverse employee group whose experience in handling personal information reflects a range from direct frontline responsibility through handling complaints to monitoring and reporting on risk at a Board level.

Handling personal information is an intrinsic part of ACC's interaction with clients. Staff appear more focused on managing high workloads and achieving performance targets which can take priority over the importance placed on protecting personal information.

6.2 External stakeholders

The overwhelming feedback from external stakeholders was for clients and client's personal information to be treated with respect.

Stakeholders reported varied experience of ACC's practices relating to personal information management over many years but consistent themes emerged through the stakeholder meeting regarding multiple instances where personal information was not updated on a timely basis, information not relevant to the claim was held on file and frequent occurrences of information related to other claimants being retained on file and/or released to other claimants. Stakeholders reflected that while these instances were regrettable (and they acknowledged that errors occur from time to time), what concerned them most was what they saw as an almost "cavalier" attitude with which they and their personal information were dealt with by ACC personnel. In many instances stakeholders felt as though they were just another transaction rather than an individual and the attitude adopted by ACC personnel reflected this. For stakeholders this pointed to a cultural issue and was the single biggest aspect that stakeholders wanted to see addressed as an outcome from the Independent Review.

The feedback from stakeholders can be grouped around a number of themes:

- Communication. Stakeholders cited a number of examples where changes were made within ACC that gave rise to concerns by claimants from a privacy perspective. One example is the recent change in the management of sensitive claims. In the past these were managed centrally but the change has seen such claims allocated to claims advisors throughout the country. From the perspective of the stakeholders this gave rise to concerns that their often complex, and always sensitive, claims were being dealt with by staff with less experience in such claims and that their personal information would be treated with less sensitivity. There was also the view that this was done as a cost saving measure by ACC.

  The reason for the change from ACC's perspective was to assist with more timely management of such claims and the reallocation throughout the country was made to experienced claims advisors.

  This is a situation where proactive and direct communication with claimants about the rationale for the change (and how personal information would be managed) would have gone a long way to ensuring claimant concerns about their sensitive and personal information could have been addressed upfront and such concerns alleviated.

Stakeholders raised the issue of claimants classified as VIPs. There was inconsistent understanding of the reason for this category but it was generally interpreted to mean that such claimants got "special" treatment. Again this is an area where a simple fact sheet or FAQ on ACC's website could ensure that ACC's policy and practices are clear. For example in current policies and practices the only difference between the treatment of VIP and general claims is that the access of VIP claims is limited to a selection of ACC staff.

- Personal information management. A number of issues were discussed ranging from the definition and use of personal information through to its storage and updating.

  Stakeholders felt that ACC's lack of distinction between health-related (clinical) information and administrative (name, address, etc.) information contributed to all information being dealt with less care than health information maintained by other agencies (for example the DHBs).

  Many people consider their health information to be highly sensitive. ACC does not distinguish between health information and general administrative information about a claimant (the current EOS does not have such functionality) nor does it always return information to medical professions where medical information not directly relevant to the current claim is provided by a medical professional. Stakeholders would like to see higher standards set around filing and access to clinical information and only information relating to the current claim maintained on file.

  A key area of concern in this regard is the "ACC167 Authority for the Collection and Disclosure of Information Form" which is used to obtain consent from individuals for the collection and use of personal information. The form has been the subject of much discussion by stakeholder and advocacy groups over a number of years and the area of contention relates to the use of the term "etc" with reference to obtaining and using health information. Stakeholders consider that this gives ACC complete freedom to obtain and use information and that this authority is "abused" by ACC when dealing with some claimants to whom it wishes to deny or cease compensation payments. Stakeholders stated that various attempts had been made to discuss the form with ACC over the years but stakeholders felt their input had not been listened to.

  Stakeholders also expressed concern that ACC often collected more medical information than was needed to assess the specific claim and that such information had been used in some circumstances as grounds for denying compensation inappropriately.

  Stakeholders cited examples where they had requested information to be updated but this had not been done in a timely way and as a result the information sent by ACC to clinicians, as the basis for assessing their claim, was not always correct and accurate. In addition not all information was retained on the file (for example emails). As stakeholders described the process it appeared to be cumbersome and time consuming and would often generate additional requests for access to information due to claimant suspicion that the file did not contain accurate information. Stakeholders felt the onus was on them, rather than ACC to ensure the information on file was accurate.

  Another area of concern was the extent to which employers accredited under the Accredited Employer Scheme were adhering to the privacy principles and whether their practices were robust. While this aspect is covered in the periodic audits of employers the results are not published or communicated and this is something that could be considered.

  Timeliness in responding to requests for information was a concern in connection with requests to both ACC and Accredited Employers.

- Personal information practices. Stakeholders noted a lack of consistency of treatment in relation to personal information practices around the country and in resolving issues. Reference was made to Building Effective Relationships Training ("BERT"), an approach for working with claimants to resolve issues, as a good practice approach.

- Technology. Stakeholders had a range of views about the technology used by ACC including the reliance on email and spreadsheets and the exchange of physical files when dealing with claims. Most would like to see more interactive technology solutions and systems that are more reflexive.

  The "open access" to claimant information allowed by EOS was also cited as a major issue and inconsistent with practices of other agencies dealing with sensitive client information.

Attendees at the stakeholder meeting were keen to offer up a number of potential solutions including:

- Addressing the culture and attitudes of all ACC personnel when dealing with claimants and their personal information.
- Reviewing policies and practices to ensure that only information relevant to the claim is collected and/or retained on file and distinguishing between medical and other information.
- Reviewing ACC's approach to stakeholder engagement, communication and consultation to ensure it is meaningful and enables:
  - timely and appropriate communication with stakeholders about changes that impact on personal information relating to the claimant (communication)
  - effective input into the design of systems and processes, for example obtaining feedback on ACC167 form (consultation).
- Addressing technology including:
  - developing a "portal" type approach to enable claimants to directly access their own information (as now provided by the Inland Revenue Department)
  - limiting access to information to those who need it based on role, rather than open access for all
  - linking corrections to information to the base information held in EOS.

These have been considered as part of the recommendations set out in Section 8.

7 Comparison with other organisations

Comparative analysis was completed with a number of other organisations on their approach to, and delivery of, privacy programmes from the perspective of risk management, compliance and accountability. The survey group included two major banks, a DHB, two insurance companies and three government agencies. All handle significant volumes of transactions and customer data. The analysis focused on structures, education and training, breach and complaint management and resolution, responsibilities and reporting around privacy.

All of the participating organisations indicated that privacy was treated, for the large part, as just one of a number of operational and legislative risks managed under their structures and process, albeit with specific training and resolution processes.

The benchmarking analysis indicated a significant difference in approach to managing privacy issues particularly in the determination and response to legislative risks through process management. Notably, ACC compares more than favourably with other organisations around its education and training processes, complaint management and resolution. However, it has a significantly different approach to process risk management and compliance and the cultural elements, leadership and consequence management.

The organisations pointed to their successes being achieved through creating a culture of compliance where it was easier to comply than not. The essence of their approach is to identify the key risks to manage, embed risk treatments aligned to strategy in their processes and technology and then ensure that employees comply with the processes through a compliance framework.

The next most significant key contributor to success that each organisation had in common was the existence of a compliance framework and function to support a coherent, co-ordinated and consistent approach to maintain compliance.

Culturally, the significant difference was a leadership position of "how we do things here" rather than the ACC management position that privacy and legislative compliance is carried out by employees elsewhere in the organisation.

The key learnings were that while ACC is now focused on the right areas of concern it has some critical decisions to take regarding risk appetite, tolerance and what structures it requires going forward. It should be noted that all but one organisation still encountered privacy breaches and near misses but the impact of those was lessened by the approach adopted and actions taken as a result.

Currently ACC's risks around handling of high value or sensitive information is not matched by the controls it exercises in the processes to manage that information. The relative proportions depend on the type and sensitivity of the information however, where the surveyed organisations have clearly considered the risks and their treatment, ACC does not appear to have.

Each of the organisations surveyed were able to demonstrate that a risk appetite and tolerance were decided for a number of operational and legislative risks. This in turn was reflected in the investment in processes that they had adopted. Examples included how client information was treated whether in storage or in remittance. Similarly system access, logging, monitoring and reporting all reflected identified and prioritised risks.

Nearly all talked about creating a culture of compliance which was supported by a clear strategic focus and a compliance framework. Relying on the embedding of risk responses into processes to manage the risks, the focus for leadership and management is ensuring that employees understand what successful performance looks like, what the desired culture to achieve it is and that the right processes are in place to achieve it.

Each organisation had clear and definitive business rules and guidelines to ensure that responsibilities and consequence management are well understood.

Responsibility for privacy activities was shared in most organisations. The role of the privacy officer was normally to co-ordinate activities relating to the OPC and manage formal complaints while providing advice to the business. The privacy officer role is supported by some form of compliance function that ensured that processes are being managed and followed, monitoring and reporting is accurate and meaningful and trends analysed and acted on.

The more structured the organisation around processes (banks, insurers, large agency) the more stringent the compliance functions. It was one part of a multi faceted approach to managing business risk.

It is clear that a well performing compliance function is a strong contributor to a culture of doing the right things in the right way at the right time – a culture of compliance. The reason is twofold; employees follow the processes more closely when they know that there are appropriate checks in place, and the role of the compliance function is to communicate, inform and educate as much as ensuring discipline to process. An essential element is the feedback loop to allow processes to be improved as soon as issues or trends are evident.

The compliance functions also included complaint resolution and investigation within the same business group to provide a co-ordinated and consistent approach to whole of organisation issues and provide feedback and independent advice quickly to process owners.

A comparison of training approaches shows that ACC has one of the more sophisticated and through approaches to awareness and general principle training. All organisations had a degree of privacy specific training in their induction programme. However, the difference between ACC and other organisations is the amount of specialised training that occurs around critical or task specific processes after induction and ensuring that they are followed. Again this is an "all risk" approach rather than just privacy.

Every organisation reported to executive level to one degree or another, certainly on trends, breaches and complaints. Most reported more on the basis that there is a heightened sensitivity by customers to privacy issues rather than an increasing risk rating or process failure.

8 Privacy and security practices review – findings and recommendations

The Independent Review Team concluded that the Breach that occurred was a genuine error but that errors are able to happen because of systemic weaknesses within ACC's culture, systems and processes. The subsequent "response process" could also have been better if appropriate policies, practices, escalation protocols and the "right culture" were in place to allow for transparency of breach handling at the appropriate levels, in an appropriate manner. A similar incident is much more likely to happen again in the current environment if the issues identified in this review are not addressed systematically and systemically.

The Independent Review Team's task was to determine if ACC policies and practices relating to security of information are appropriate and effective taking account of comparable best practice and its risk environment.

ACC has a complex and challenging role. It must manage the Scheme in a cost-effective, outcome-focused way that ensures the Scheme is financially sustainable for future generations.

ACC's role brings it into contact with people at times when they are vulnerable and might be severely traumatised or suffering diminished ability to look after their affairs. The organisation deals with a range of short and long term claims some of which are very complex in nature. ACC necessarily collects and processes vast amounts of very sensitive personal and health information about Scheme clients. Privacy should therefore be a paramount consideration.

As noted in the introduction, ACC is also operating in a fast-changing digital environment where personal information is an increasingly valuable asset with a commensurate impact on the risk exposure of the Corporation. In turn this impacts on what might be appropriate approaches to risk management, associated governance, business processes and technology platforms.

The Independent Review Team found that ACC had a range of controls in place that are intended to meet its obligations under the Privacy Act and the HIPC to protect the privacy of clients. However, given the Breach and previous privacy breaches and complaints, the Independent Review Team finds these do not provide a sufficiently strong and sustainable approach to protecting personal information.

The areas that the Independent Review Team has identified as needing to be addressed or strengthened fall into a number of clear themes.

- Board governance – privacy now needs to figure more prominently on the ACC Board agenda particularly when addressing organisation-wide risks. This in turn means that the ACC Board and ACC as a whole need to recalibrate the extent of risk faced in handling vast amounts of personal and health information (some of which is sensitive in nature) and the resources that need to be applied to managing/mitigating the risk.
- Leadership and privacy strategy – ACC will be in a better position to build trust and confidence with its stakeholders with a renewed emphasis on leadership, vision and strategy that demonstrates that privacy is an integral contributor to improved public trust and confidence and providing high quality services to clients consistent with meeting the key priorities identified by the government in the ACC Service and Purchase Agreement 2012-2015.

- Privacy programme – ACC has elements of a good privacy programme in place which now needs strengthening and co-ordinating and, in some cases, a step change; in particular new approaches are needed to risk management and to building privacy measures in at all stages of business processes.
- Culture – the "right culture" needs to be in place to implement the spirit of the IPPs, the HIPRs and the HIPC all the way through from the customer service desk, through complaints management to transparency of breach handling. This culture needs to be firmly based on respect for claimants and therefore their personal information.
- Accountability – there needs to be clearer responsibility for reporting and monitoring how personal information is managed, matched by suitable rewards and consequences.
- Business processes and systems – current manual processes and technology systems need redevelopment using a framework such as privacy by design so that staff are well supported in their work, excessive manual processing and double handling is eliminated and reporting systems are automated and the advantages and risks in the changing digital world are recognised.
- Backlogs and establishment of the new Business as Usual – a "surge" strategy is required to address backlogs in complaints, access requests, and finalise any document imaging and error correction. This may require additional resources through the establishment of a separate, temporary "backlog unit".
- Compliance with the IPPs and the HIPRs – the Independent Review Team undertook a high-level assessment of ACC's compliance with the IPPs/HIPRs and has made some specific recommendations that are included in this section of the report. These recommendations are to assist ACC in implementing the broader recommendations for ACC's overall management of its privacy obligations.

The Independent Review Team's recommendations are intended to deliver a systemic response from the ACC Board at the top all the way through to client facing staff, to improve compliance with the letter and the spirit of the law, meet client expectations and win back the trust of clients and other major stakeholders.

Finally the Independent Review Team recognise that for culture change to take effect within ACC it will take time with a focus on the long-term for real, sustainable results to be achieved. There are various short-term changes ACC can and has started to implement to improve its privacy management. It will also need to consider fundamental change to the design process of key systems, policies, processes and practices going forward, and will require substantial redesign of many current systems and processes.

8.1 Board governance

The Independent Review Team found that the ACC Board needs to give increased priority and focus to privacy and the protection of clients' personal information so that ACC's approach to managing privacy and its privacy culture is strengthened.

Historically, privacy has not been a standing item on the agenda of the ACC Board and its sub-committees. In addition, the ACC Board did not receive regular reports relating to privacy issues or performance, privacy risk analysis, privacy breaches and near misses. The ACC Board was aware that ACC's approach to privacy training and its standing against other public sector organisations[12] compared favourably and therefore, from the ACC Board's perspective, there was no information that caused them to have any specific concerns about how personal information was managed by ACC.

[12] *Annual Report of the Privacy Commissioner 2002-2011* available at http://privacy.org.nz/corporate-reports/?start=0

In this context the Independent Review Team infers that privacy was not "top of mind" and therefore lacked strategic focus at Board governance level. ACC does not have a strategic vision that aligns privacy with the corporate strategic direction of ACC. It also appears that the ACC Board may have not been sufficiently focused on the nature and extent of privacy risks faced by ACC until the Breach became public in March 2012.

However, since May 2012 reporting on privacy matters has been put in place. The ACC Board has expressed a "zero acceptance" approach to breaches. However, the Independent Review Team considers that the ACC Board could have more effectively communicated its expectations of privacy management to ACC in relation to its stance on privacy breaches. It appears there was insufficient effort on contextualising the application of this in practice, particularly with regards to whether staff would be provided with the appropriate resources, tools and systems to reach a level of zero acceptance. The Independent Review Team considers there needs to be a clearer recognition that reducing breaches begins with addressing all aspects of information governance starting with data collection and moving through all the IPPs/HIPRs including processes for ensuring data quality and accuracy, access to data, reporting systems and through it all, a culture that respects privacy.

The Independent Review Team found a varied understanding of ACC's risk appetite, risk framework and its application throughout the organisation. It also found disparate views on ACC's risk management framework and the Independent Review Team considered that risk management in general could be strengthened. Privacy is not part of ACC's risk management framework. It is currently seen in isolation from the framework and there is no formalised process for co-ordination, monitoring and reporting of privacy risks. This has contributed to a culture where it appears that respecting clients and protecting clients' personal information is not "top of mind".

Recommendation 1 – Board governance	Indicative timeframe for implementation
The Independent Review Team recommends that the ACC Board takes the following steps to strengthen the governance of privacy within ACC:	
1.1. Reflect the importance of privacy and protection of personal information in the weighting given to privacy in the risk management framework and the ACC Board's focus on privacy through the following measures: a. Co-ordinate and structure privacy as part of the risk management framework in the medium to long term in order to make privacy management effective across ACC. b. Lead by example at Board and Audit & Risk Committee level by setting clear expectations and communicating them to Executive Management. c. Assess privacy risks against ACC's risk appetite and tolerances with consistent reporting. d. The ACC Board commits to the provision of resources to fully embed privacy risk management within ACC with a programme of risk management activities.	3 months - 1 year
1.2. Actively participate in the development of a vision for privacy within ACC which is to be the basis for a privacy strategy and which: a. Defines the ACC Board's risk appetite with regards to compliance with the Privacy Act and related codes and principles. b. States that privacy is a key risk management issue for ACC and is likely to increase in importance over time. c. Recognises that striving for "zero acceptance" of data breaches begins by minimising risks at all stages in the information management life cycle through best practice implementation of all of the Information Privacy Principles ("IPPs") and Health Information Privacy Rules ("HIPRs").	2 months

Recommendation 1 – Board governance		Indicative timeframe for implementation
	d. States the critical importance of a culture of respect for client privacy and good management of information about clients, to the wellbeing of ACC clients and to achieving community trust in ACC. e. States the ACC Board's strong commitment to achieving the vision.	
1.3.	Initiate the development by ACC of a privacy strategy for adoption by the ACC Board which implements the vision for privacy and which covers compliance with privacy law including all the IPPs/HIPRs, implementation of best practice privacy and a culture of respect for client privacy (see Recommendation 4).	4 months
1.4.	Ensure a cycle of continuous accountability to the ACC Board by ACC leadership in regards to privacy risks.	Immediately
1.5.	Include "privacy" in the Terms of Reference for those Committees that have responsibility for privacy oversight and monitoring. Individuals within the selected governance committees and groups should be made aware of the nature and scope of personal information collected by ACC.	3 months
1.6.	Follow up on the Independent Review Team's recommendations.	1 year
1.7.	Ensure that every two years ACC, in consultation with the Privacy Commissioner, commissions an independent privacy audit of ACC adherence to its privacy strategy including compliance and best practice elements.	2 years
1.8.	Ensure that the report of the independent privacy audit is given to the Privacy Commissioner and published on the ACC website.	2 years
1.9.	Ensure that the ACC Board reviews the privacy strategy every two years in light of the independent privacy audit.	2 years

8.2 Leadership including privacy strategy

8.2.1 Privacy leadership

At the time of the Independent Review, it was evident that Executive Management were placing a high importance on privacy, with a commitment to improving the way in which personal information is handled. However, many also expressed the view that privacy was not "top of mind" prior to the Breach being made public in March 2012. Privacy management did not feature regularly in Executive Management meetings, and the risk and value of protecting personal information did not appear to be fully appreciated.

The Independent Review Team found that there was no formal requirement for Executive Management to report on ACC's privacy risk profile or any significant changes in the privacy risk profile to the ACC Board, at the time of the Independent Review. Commitment for risk management was limited and there appeared to be a general lack of awareness of ACC's risk management framework with the belief that lower level staff were responsible for this activity.

The responsibility for implementing, promoting and driving privacy management was delegated below senior executive level to the Manager of Government Services and privacy was a small part of the responsibilities of the position. There was no Executive with a standing responsibility and accountability for the privacy strategy and setting an appropriate tone and culture towards protecting personal information. As a result, practices relating to protecting the privacy of personal information varied greatly throughout ACC.

Privacy management had a largely bottom-up approach where reaction from the top was based on privacy breaches that had occurred. At the same time, line management authority and responsibility for privacy management was unclear and generally staff had an ad hoc approach to identify, measure, monitor, and report on privacy risk, breaches and near misses. The Independent Review Team found that in some instances line management did not have a clear understanding of the extent of risk, breaches and near misses within their areas.

8.2.2 Privacy strategy

An integrated privacy strategy is critical to promote transparency and to leverage assurance processes. It incorporates board-level engagement, features regular reporting and aligns with risk oversight objectives.

The Independent Review Team found that ACC has a range of strategies and practices that would provide elements of an effective privacy strategy but that these need to be brought together into a coherent overarching strategy. While there are some indicators of a direction, which includes customer service and "zero acceptance" to privacy breaches, there is no clear statement that aligns to this direction and describes what this means to all stakeholders, both internal and external. Privacy also is not explicitly referenced in ACC's Programme of Delivery, although the Independent Review Team considers that a strong performance on privacy will be critical to also achieving "customer satisfaction".

It is important that ACC aligns each of its Government priorities with privacy and personal information as a key cornerstone. To enable organisation-wide change and a common understanding the following key principles will need to be incorporated during this transition phase namely:

- Conform to laws and regulations.
- Reflect a common culture and language around risk, including privacy risks.
- Be aligned to strategic objectives.
- Be well understood and visible across ACC.
- Be embedded within company policies and procedures.
- Be simple and sustainable and enable proactive management.

Recommendation 2 – Leadership and privacy strategy	Indicative timeframe for implementation
The Independent Review Team recommends that ACC takes the following steps to strengthen its privacy leadership:	
2.1. Strengthen the "three lines of defence model" that will allow privacy to be embedded in decision-making assisting to create a culture where everyone has ownership and responsibility for protecting personal information and doing the "right thing". This should include consideration of a comprehensive compliance programme to strengthen ACC's second line of defence.	6 months
2.2. Ensure a member of the Executive is accountable for privacy and is responsible for: a. Providing leadership on implementing the ACC privacy strategy. b. Ensuring that appropriate resources are allocated. c. Ensuring that other key privacy targets are being met.	Immediate

Recommendation 2 – Leadership and privacy strategy		Indicative timeframe for implementation
2.3.	Develop a privacy strategy for ACC for adoption by the ACC Board which covers the following matters: a. The ACC Board's privacy vision for ACC. b. The values and principles that ensures that the culture within ACC supports the privacy strategy. c. The structure of responsibility and accountability for top to bottom implementation of privacy compliance and best practice within ACC – including a means of drawing upon the views of, and reporting to, key stakeholders and interest groups such as: i. ACC clients, their carers and advisers ii. Privacy Commissioner iii. ACC employees. d. The mechanisms for identifying privacy compliance and risks and the way this fits within ACC's wider risk assessment approach. e. Mechanisms for ensuring that privacy best practice and compliance is built into all new systems products and services. f. The benchmarks or KPIs for Executive Management and ACC as a whole in achieving compliance with the law and best practice privacy. g. Philosophy governing, and mechanisms for, training staff in privacy compliance and best practice. h. Mechanisms for ensuring third party contractors to ACC comply with ACC's privacy strategy. i. Mechanisms for measuring progress in implementing and compliance with the privacy strategy including internal and external monitoring and audit. j. Mechanisms for reporting to the ACC Board and external stakeholders of progress in implementing and compliance with the privacy strategy taking into account the Independent Review's recommendations relating to Board governance. k. Expression of the privacy strategy in an integrated privacy programme.	3 months
2.4.	Develop a plan for engaging stakeholders in developing the strategy.	3 months

8.3 Privacy programme

A privacy programme can be considered as the set of activities, policies and procedures that organisations apply in delivering a privacy strategy aimed at meeting their privacy law obligations.

ACC does have a range of elements of a privacy programme including its Privacy Officer, a network of Privacy Champions, annual privacy training and a range of privacy related policies and procedures. However, the elements need to fit within a clear structure and have a clear focus. Further, ACC does not currently provide specific guidelines and responsibilities for business units and management and the programme is therefore limited in reach. The lack of a clear programme for ensuring compliance with the Privacy Act and the HIPC is clearly having an effect. For example, current privacy management practices are largely focused towards preventing disclosure of personal information to external parties and the other IPPs/HIPRs which will have a much greater impact on the regard in which ACC is held, are not given as much focus.

The Independent Review Team's observations about key elements of the current privacy programme are noted below.

8.3.1 Privacy Officer and privacy resources

An organisation's Privacy Officer will generally be the focus of privacy activities and the way in which this role is allocated and resourced will have a key impact on the effectiveness of a privacy programme.

As noted earlier, other than as set out in the Privacy Act, ACC's Privacy Officer does not have a formally defined role. The Privacy Officer's description of her role is clearly appropriate but is narrower than might be expected for an organisation the size of ACC and with its privacy risk profile. In particular, the role currently has limited involvement in advising on privacy in new systems or products, in risk assessments and, until recently, in reporting on privacy performance. There also do not appear to be strong links between the privacy function and ACC's Office of the Complaints Investigator.

The Independent Review Team also notes that the Privacy Officer has limited time and resources to carry out her responsibilities. The position is currently located in an area where there are high profile competing responsibilities. While the Privacy Officer has resources within the wider Government Services team, only approximately 5% of her time and her team's time is allocated to dealing with the range of privacy related matters. The Independent Review Team understands that ACC's specialised privacy resources, apart from the Privacy Champion network discussed below, amounts to approximately one FTE position.

The Privacy Officer receives reports on privacy breaches via the Privacy Champions. From time to time the reports have been collated and analysed, however there is currently no regular process to provide feedback to units and branches. Recently the role has included reporting to the Executive Management and the ACC Board.

The lack of a robust written privacy programme and infrastructure, coupled with the lack of a formal and communicated succession plan for the Privacy Officer, creates a potential "single point of failure" within the privacy function at ACC.

8.3.2 Considering privacy in new systems, products or services

The Independent Review Team considers that ACC should strengthen its focus on considering privacy impacts as it develops and implements new systems or processes. While there is some liaison with the Privacy Officer on these matters ACC could significantly improve focus and co-ordination by regular preparation of Privacy Impact Assessments and adopting a philosophy such as Privacy by Design ("PbD") so that there is a full understanding of the extent to which personal information is handled within the organisation, how it is handled and the impacts this may have on clients.

PbD is a strategic approach to privacy pioneered by Dr Ann Cavoukian, the Information and Privacy Commissioner of Ontario, Canada, which has evolved into a comprehensive approach to embedding privacy-sensitive thinking into all aspects of an organisational or system-wide initiative.[13]

[13] More information about PbD is available at http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/

The most significant concept in PbD is the importance of considering privacy issues right from the beginning and at all stages of developing and implementing processes and systems that handle personal information. More specifically the objectives of PbD — ensuring privacy and gaining personal control over one's information and, for organisations, gaining a sustainable competitive advantage — may be accomplished by practicing seven Foundational Principles which are:

1. Proactive not Reactive; Preventative not Remedial.
2. Privacy as the Default Setting.
3. Privacy Embedded into Design.
4. Full Functionality — Positive-Sum, not Zero-Sum.
5. End-to-End Security — Full Lifecycle Protection.
6. Visibility and Transparency — Keep it Open.
7. Respect for User Privacy — Keep it User-Centric.

8.3.3 Privacy Champions

ACC has had Privacy Champions embedded within business units since 2005. Since the Breach ACC has had a drive to add more Privacy Champions throughout the organisation; there are now 92. This is a positive step to promote privacy awareness.

Historically, the Privacy Officer has not had the budget or resources to fully support the Privacy Champions. Accordingly, the awareness and importance placed on privacy has varied throughout the organisation to reflect the Privacy Champion and Branch Manager's commitment to and awareness of privacy related matters, rather than the effectiveness of the resources they were provided with.

Feedback from the Government Services team and the network of Privacy Champions is that in the past there has not been sufficient support for the champion role to be fully effective. A number of Privacy Champions were new to the role and indicated they did not understand the full extent of what is required of them.

The issues the Independent Review Team identified were:

- Clear selection criteria are needed for being appointed into this role. While some business units selected Privacy Champions based on the importance of the role, others selected based on who volunteered for the role, while others selected based on the person who "had the most breaches".
- Staffs' view of the Privacy Champion role currently and the support they can provide needs to be aligned to the Privacy Champions' expertise. Champions are viewed in branches as a resource for technical privacy issues, but most have not received "expert" technical training or do not have the knowledge to provide this form of advice.
- Current training is geared towards increasing awareness of Privacy Champions rather than gaining technical expertise and more "expert" technical training is needed for Privacy Champions, including a documented programme for on-going training and development as privacy professionals.
- Privacy Champions need more clearly defined support mechanisms, as far as tools, training, checklists etc and access to information and expertise.
- The reporting lines of the Privacy Champions need to be clarified so that it is clear to whom they are accountable to and for what, i.e. Line management reporting versus reporting to the Privacy Officer.

8.3.4 Privacy training

A key element in an effective privacy programme is ongoing privacy training for all staff. The Independent Review Team considers that ACC's baseline privacy training is generally good; it includes Induction training and Online modules. Privacy Champions are also encouraged to offer regular reinforcement of privacy messages. The Independent Review Team found staff were keen for improvements in the following areas:

- More scenario/practical based training.
- More operational and work related examples.
- More unit specific training.
- More training targeted to job area especially for Privacy Champions, HR and front-line staff.
- More frequency of training e.g. follow up on identified issues.
- Training content more engaging, relevant and frequently updated.
- Training on dealing with clients in difficult and stressful situations empathetically and effectively.

In addition, the Independent Review Team observed that there could be more consistent monitoring and reporting of privacy training compliance. The Learning and Development group is responsible for executing the annual privacy training programme (as required by Privacy Management's procedures). This needs to be supported by identifying a function or department, possibly the Privacy Officer and her team, within ACC accountable for monitoring or reporting to management on privacy training compliance.

Security training covering broad IT security practices is provided to staff, however the training programme is not comprehensive. Reliance for security awareness training is primarily placed on online training, however the completion of the online training is not compulsory for contractors and there is no monitoring to ensure that staff complete the training. Similarly, the information management training module is not compulsory. The online training is performed when a new staff member joins ACC, however it is not required to be repeated on a periodic basis to ensure that sufficient awareness continues to be maintained. Outside of the online training, staff are provided limited training beyond the physical security training related to health and safety.

Communication to staff about security is generally ad-hoc.

8.3.5 Privacy policies

ACC has a suite of policies, procedures and guidelines that generally cover privacy management. ACC has recently reviewed this material and has identified the following:

- Disparate policy documents that give no single source of reference and that create the potential for uncoordinated or incoherent views of expectations for privacy.
- The policy framework is viewed as less of a live resource and information base and more of a passive publication set.

The Independent Review Team largely agrees with the above comments. It also found the need for some clearer or additional policy in relation to collection of relevant health information. The Independent Review Team's view is that ACC does not currently fully understand the nature of the personal information it holds and how it handles this information. It also finds that some areas of ACC is not clear on its responsibilities relating to maintaining confidentiality versus its obligations for privacy.

8.3.6 Privacy complaint handling

ACC clients have privacy rights that arise under the Code as well as under the IPPs/HIPRs. As outlined earlier a privacy complaint may be made under the Code via the Office of the Complaints Investigator and also through direct contact with Government Services, a Customer Service Centre or to Branch management. A complaint about the IPPs or HIPRs could also be raised through these channels or by a direct complaint to the Privacy Commissioner.

The Independent Review Team considers that there is some potential for clients to be confused or unaware of which channel to pursue and for the response to a complaint to vary depending on the channel used. The Independent Review Team found that:

- ACC's website information on complaints does not mention privacy, the IPPs or the HIPRs specifically and directs claimants to the Office of the Complaints Investigator.
- ACC's website privacy statement provides information (including timeframe) for clients seeking access to personal information but does not, as best practice would suggest, give at least general information about ACC's information handling practices, or about complaints under the IPPs/HIPRs generally.
- The Code (handled by Office of Complaints) states "all claimants" have the right to have their privacy respected, which includes compliance with legislation and granting all claimants access to their information in accordance with legislation" – while this is right it appears to cover the same territory as the IPPs/HIPRs (handled by Privacy Officer or branches) there appears to be some room for clarification from a client and organisation perspective.
- There are process instructions for staff on handling complaints but it appears there is not a detailed set of instructions on complaint handling and resolution.
- The Government Services team does have some instructions – the Independent Review Team considers these are useful but could be expanded by emphasising interactions with the client and conflict resolution practices and also on identifying and dealing with underlying systemic issues.

8.3.7 Privacy complaints and breaches – reporting

ACC has a significant focus on privacy, near misses and breaches (defined as inappropriate disclosure of information). There are clearly documented procedures and staff are encouraged to proactively report breaches. There is a positive emphasis in the procedures on alerting clients who may have been affected by a privacy breach.

However, the Independent Review Team finds that the current processes are possibly too narrowly focused. They appear to be aimed at preventing disclosure of personal information to external parties and the other IPPs/HIPRs are not given equal focus. They are not set up to capture and respond to underlying systemic issues and risks. While the breach management process includes a generic privacy risk register that covers fairly extensive risk identification, it focuses primarily on IT physical security and disclosure. The register provides practical solutions to identified risks but does not seem driven towards eradicating risks and/or addressing the underlying cause. The risk register appears to be used by the branch network, including by Privacy Champions but there is less evidence that it is used by corporate teams.

The Independent Review Team sees a need for the more co-ordinated capture and recording of privacy issues/breaches and near misses across ACC. It notes that:

- There are separate recording systems depending on the complaint channel, for example:
  - complaints received via the Complaints "0800" number are recorded in EOS under the "Complaints" tab.
  - privacy issues, breaches and near misses being recorded on spreadsheets, both manual and electronic.

- the Government Services team uses a system called Action Remedy, rather than EOS, to manage the complaints it handles (primarily those referred by the OPC).
- the Office of Complaints Investigator does not provide any breakdown of complaints received under Right 7 of the Code.

- The Government Services team are only aware of those breaches that are escalated through to them resulting in limited central co-ordination of privacy breaches and inconsistency of reporting through the channels. Processes are now being formalised to give effect to a recent requirement that all breaches and near misses are to be reported to the Government Services team.
- Given reporting requirements, the branches expressed interest in receiving feedback on the general nature of privacy breaches and how they are being dealt with.
- There has been a requirement for line management operational reporting of breaches for a number of years, but it appears that there needs to be a clearer focus on identifying and resolving systemic issues.

The Independent Review Team also sees a need for reporting functionality to be an automatic part of systems. A manual monthly reporting process has been established (since May 2012) and that is providing greater visibility of near misses and breaches, underlying causes and management of complaints. This approach has the potential to increase disclosure risk if it results in personal information being included in spreadsheets and other information and information exchange systems.

A centralised reporting system for privacy complaints will make it easier to collate and analyse data. Current reporting available for complaints has limited details and does not include privacy complaints received by the Privacy Officer or by the branches. Additionally, there is limited overview of complaints including privacy breaches and near misses received and handled directly by branches.

8.3.8 Security practices

Security practices relate to the processes and controls in place to manage the confidentiality, integrity and availability of the information systems and the data contained within them, and the physical security over ACC's information systems and premises.

ACC has a focus on the security of its IT systems and data, including client information. This is reflected in the policies, standards and security practices in place.

Although there is a focus on security, the security is not as effective as intended, due to:

- The lack of formal governance structures over security.
- The absence of a structured and comprehensive security assurance programme.
- Security training not being sufficiently comprehensive.
- Information management processes not always being robust.

Formal organisational governance structures are not in place to manage security. The different business functions that perform security management related roles perform their operational roles in isolation, and have no direct linkages to ACC's privacy practices. This has been recognised by ACC, and management are currently evaluating which security governance structure would be the most effective.

A structured and comprehensive security assurance programme is not in place to evaluate the ongoing design and operating effectiveness of the security controls implemented. While a range of assurance activities are performed, both within IT and within the wider business, these are not sufficiently structured or comprehensive to provide ACC with the comfort that their security practices are both designed and operating effectively.

Some of the information management practices do not support robust security. Specifically:

- Subsets of production data from the EOS claims management system are provided to ACC's third party developer, and are used in test and development systems. This increases the likelihood that unauthorised or inappropriate access will be gained to client data.
- Quarterly reviews are intended to be performed over the system access provided to users however, the process is not effective and confirmation often not received from managers to confirm that access continues to be correct. Similarly, there are no mechanisms to proactively identify unusual system access within EOS.
- There is a limited understanding and no clear ownership of unstructured data on shared drives. It is estimated that the volume of unstructured data is significant with, for example, 14 terabytes of unstructured data on shared drives. As there is a limited understanding of the data, ACC does not have a clear understanding to whether the security implemented over the data is effective.
- The information classification framework in place is based on the broad Government classification system. As most of ACC's data falls into one of the broad classifications, the security of data is generally treated the same regardless of its nature. Classifications based on the business nature of the data (e.g. client data or corporate data) are not in place. This increases the likelihood that the controls implemented over some types of data do not align with the risk posed.
- Clear desk practices are generally not followed. Clear desk guidelines are currently being developed and are intended to be distributed to all staff.

While these practices do not support robust security, it cannot be clearly determined if this has resulted in undue risk to client information due to limited evaluation of the operating effectiveness of security that occurs.

The Privacy programme recommendations are based on the Privacy management good practice framework, which the Independent Review Team used to makes its assessment against.

Recommendation 3 – Privacy programme	Indicative timeframe for implementation
The Independent Review Team recommends that ACC enhance its privacy programme, consistent with its privacy vision and strategy and should:	
3.1. Formally document the role of the Privacy Officer position to include, in addition to the roles set out in the Privacy Act (unless these roles are clearly allocated elsewhere): a. Developing ACC's privacy strategy and programme, in conjunction with the ACC Board, Executive Management and other ACC Managers. b. Providing day-to-day leadership of the privacy programme, in particular to the Privacy Champions, ensuring that they are able to operate as a virtual team. c. Providing advice on development of ACC systems and programmes, based on Privacy by Design principles and use of privacy impact assessments. d. Developing and reviewing privacy policies and procedures and systems and tools to ensure compliance with privacy principles and ACC's privacy vision and strategy. e. Developing or providing input into privacy awareness, training activities and guidance for all staff. f. Monitoring and reporting to Executive Management, the ACC Board and other stakeholders on ACC's compliance performance and its performance against agreed privacy benchmarks and KPIs. g. Investigating and/or providing advice on privacy complaints and complaint handling and monitoring privacy breaches or near misses to ensure systemic issues are being identified and dealt with.	2 months

Recommendation 3 – Privacy programme		Indicative timeframe for implementation
	h. Supporting continuous improvement in privacy practices including actively keeping abreast of developments in privacy approaches internationally as well as in New Zealand, by participating in OPC forums and undertaking development as a privacy professional.	
3.2.	Review and clarify the role of Privacy Champions and develop criteria for the appointment of Privacy Champions and ensure that it is consistently applied. If ACC decides that Privacy Champions should be expert privacy advisers, they should receive training at an appropriately technical level and given recognition as privacy professionals.	6 months
3.3.	Ensure ACC has an effective suite of privacy policies and procedures, based in the first instance on an audit of current personal information holdings and addressing all the IPPs/HIPRs which: a. Are comprehensive, up-to-date and easy to access and apply. b. Are reviewed regularly with input from staff to ensure they provide relevant and accessible answers to staff questions. This should be led by the Privacy Officer.	1 Year
3.4.	Ensure the Privacy Officer and other specialist privacy roles, including the possibility of a specialist privacy team reporting directly to the Privacy Officer, is adequately resourced, taking into account best practice benchmarks or advice from an independent Human Resource specialist.	4 months
3.5.	Support staff to implement ACC's privacy vision and to comply with the Privacy Act with appropriate privacy education and training for all staff which is comprehensive, has an appropriate maturity model based on staff experience in their role and which: a. Takes account of staff feedback that training should: i. be more scenario-based and practical ii. be operational and use work related examples iii. include dealing with clients in difficult and stressful situations empathetically and effectively iv. be more targeted to job area especially for Privacy Champions, HR and front-line staff. b. Ensures that staff are receiving regular detailed feedback on privacy incidents and their resolution and provides regularly updated case studies or similar tools to assist staff to refine their understanding of ACC's privacy approach. c. Is integrated with ACC's overall staff development programme as a visible demonstration that privacy is an integral part of the development of the complete ACC member of staff.	Visible to staff in 6 months, fully embedded 12 months
3.6.	Develop a privacy risk management framework that: a. Is an integral part of ACC wide risk management approach. b. Reflects ACC's view of its appetite for privacy risks. c. Addresses risks against all of the IPPs/HIPRs. d. Can take account of management information on near misses, privacy breaches and privacy complaints under ACC Claimants Code of Rights (the "Code") or the IPPs/HIPRs and identify and respond to any underlying systemic issues.	1 year

Recommendation 3 – Privacy programme	Indicative timeframe for implementation
3.7. Establish appropriate and consistent systems and processes for recording, monitoring and reporting all near misses, privacy breaches and privacy complaints under the Code or the IPPs/HIPRs, to facilitate improvements in policies and practices and identification of and response to systemic privacy issues. Privacy incident statistics might include: a. Business areas where incident occurred. b. Incident frequency by IPP and nature of the incident. c. Complaint outcome with categories both for matters substantiated and not substantiated. d. Improvements identified to minimise further incidents. e. Timeframe to resolution.	1 year
3.8. Complete a holistic review of the personal information provided to clients via all channels and at all stages in their interactions with ACC to ensure that: a. It is consistent. b. Provides sufficient detail to inform their decisions and actions. c. Takes account of current best practice in privacy notices, for example using layered notices and giving "just-in-time" privacy prompts.	Visible to clients within 6 months, fully embedded within 1 year
3.9. Establish clear processes for managing near misses and privacy breaches that take account of all the IPPs/HIPRs, as well as matters raised under the Code, have clear escalation paths, consider risks to the clients concerned and client notification in appropriate circumstance and incorporate review to identify and respond to underlying systemic issues.	4 months
3.10. Integrate privacy complaint processes, whether made under the Code or the IPP/HIPR ensuring that: a. The connection between privacy rights under the Code and under the IPPs and the HIPRs is clear. b. Clients are clearly aware of their rights to lodge a complaint about their privacy rights under the Code or the IPPs/HIPRs with ACC or the OPC. c. Privacy complaints are treated consistently and in accordance with best practice dispute resolution, whether made under the Code or the IPPs/HIPRs. d. Privacy issues raised through all channels are captured and fed into breach management and the risk management processes.	Within 1 year, earlier if possible, integrate with short term peak response plan
3.11. Develop a formal security governance structure and processes to support the effective information management of security which: a. Treats security as a business issue, rather than an IT issue, with security owned by a member of senior management (outside of the IT function). b. Establishes a governance group to provide direction and oversight of the security practices and processes – this could consist of, for example, the General Managers with security responsibilities. c. Establish a security management group to operationalise security, made up of the different senior staff with operational security roles from the different business units and functions, including representation from within the IT, property, privacy, human resources and information management functions. d. Applies risk management approach to managing security.	6 months

Recommendation 3 – Privacy programme	Indicative timeframe for implementation
3.12. Develop a formal security assurance programme. This should take a structured and comprehensive risk-based approach to security and focus on ensuring that: a. Sufficient feedback mechanisms are implemented within the business-as-usual activities performed by IT and the other business units with security responsibilities. b. Formal assurance mechanisms are implemented within project-based activities. c. Periodic independent assessments of security are performed, to provide an objective view of the effectiveness of the security in place.	6 months
3.13. Restructure the security training programme to ensure that: a. Regular broad compulsory security training is provided to all employees and contractors. b. Targeted, more detailed security training is provided to those employees and contractors with key security responsibilities. c. The completion of security training is tracked and monitored. d. The security training is reinforced by regular structured communications about relevant security topics.	Visible to staff in 6 months, fully embedded 12 months

8.4 Culture

Culture (behaviours and beliefs) determines how things get done in an organisation. In reviewing privacy practices at ACC the Independent Review Team considered the impact of ACC's culture on its approach to collecting, using, storing and disclosing personal information and on client perceptions of how the information about them was handled. This was not a fully comprehensive current state cultural assessment but the Independent Review Team felt it was important to understand the cultural environment.

As discussed earlier in the report, ACC is a large and complex organisation. Its history dates back to the establishment of a no-fault scheme for all New Zealanders in 1974. ACC's culture is shaped firstly by its founding principles (community responsibility, comprehensive entitlement, complete rehabilitation, real compensation, and administrative efficiency) and then by priorities, focus and leadership. Its culture is also influenced by the Crown operating model where accountability is shared between the government, board and management.

Successive governments have placed different emphasis on the implementation of the AC Act. Some have supported a strong social interpretation of the AC Act that has been seen to have led to more generous interpretation of the assistance available to claimants. Others have been mindful of the fiscal implications of the AC Act and have expected more conservative interpretations of its provisions. The fluctuations in overall scheme performance over the last 38 years in part reflect the different approaches. This has created ambiguity for staff in terms of customer service and managing claimant entitlements.

The Independent Review Team found evidence of a strong client focused culture in terms of dealing with clients – working with them to ensure they received the services/rehabilitation to which they were entitled. We observed a good awareness of privacy as an issue throughout the organisation, particularly in the branch network.

We found, however, that staff may not always be in a position to appreciate the risks associated with the management of personal information, in particular the consequences for the individual or the organisation. This has had an impact on the approach taken to some of the more challenging aspects of ACC's work. For example, although there are processes in place to check physical files prior to

them being sent to a client following a request for a copy of the file, these checks are not consistently followed or completed effectively. Copying files is often undertaken by staff who are not as aware of the importance of individual's personal information as the case manager directly involved with the client. Where near misses or breaches occurred there was often an inconsistent approach in terms of follow-up and consequences for those involved.

The variation in approach may well start with leadership and management expectations, how they are expressed and some of the very subtle aspects of "walking the talk". ACC defines privacy as everyone's responsibility yet the Independent Review Team found that the level of understanding of privacy varied. Staff within the Corporate Office saw privacy as more of a branch or client facing issue rather than as an organisation-wide issue, and branch staff tended to have a greater level of awareness of the privacy principles.

The Board, Chief Executive and Executive Management have a key role to play in leading the culture throughout the organisation including establishing a sound respect for privacy. The renewed focus on customer centricity, as outlined in the 2011 Strategic Plan, requires staff to be given more certainty over core operating principles. The Chief Executive considers that "*a consistent culture can be built if certainty can be given to staff over the appropriate attitude towards clients, the application of entitlements, and the balance between return to work performance and comprehensive rehabilitation. If consistency can be achieved the benefits will be to a culture conducive to the adoption of the privacy principles and to trust and confidence as clients experience a consistent ACC experience.*"

What this highlights is a need to develop a consistent culture where the importance of personal information is understood, where all staff feel both supported in their work and also individually responsible, where staff are aware of the risks, and where sound management is appreciated and the consequences of not managing personal information appropriately are clearly defined. This must be undertaken in the context of any broader cultural initiatives undertaken by ACC.

Recommendation 4 – Culture		Indicative timeframe for implementation
The Independent Review Team recommends that in addition to the other recommendations that will influence the culture to ensure it supports respect for privacy. ACC should:		
4.1.	Align its privacy culture to the broader culture of the organisation to ensure that the operating framework is integrated with customer centric objectives and provides clear external commitment to clients of ACC's focus on customer care.	Visible within 6 months, fully embedded within 1 year
4.2.	Develop consistent messages that balance privacy, customer service and efficient and effective management so that "firm is also seen as fair" by ACC and its external clients and stakeholders.	Visible within 6 months, fully embedded within 1 year
4.3.	Incorporate stakeholder views on appropriate processes for continuous engagement with interest groups and individuals.	Within 1 year
4.4.	Ensure that staff are encouraged to report and resolve privacy breaches or near misses in a supportive environment supported by a sound compliance framework.	Visible within 6 months, fully embedded within 1 year
4.5.	Develop measures, including key statistics, feedback from clients and other external stakeholders and staff and management surveys that will allow ACC to test that its culture supports respect for client privacy and to take remedial steps as needed.	1 year

8.5 Accountability

The Independent Review Team finds that the accountability framework at ACC needs to be integrated fully from the ACC Board setting expectations and calling to account "right" all the way through the organisation. This begins with clear lines of responsibility as set out in the earlier recommendations on the privacy programme. The accountability framework needs to embed accountability expectations consistent with these lines of responsibility.

The Independent Review Team also considers that current compliance assurance mechanisms should be strengthened to complement the "checklist" assessment for the annual attestation, by the Privacy Officer and ACC Board and Corporate Secretary, that ACC adheres to the Privacy Act. This could include independent assurance of compliance activities undertaken, particularly in relation to privacy and security of information and more line management involvement.

Identifying potential KPIs is an important driver in assisting management to focus their effort in areas that require improvement and will assist in identifying areas of non-performance.

In addition, there are a range of third party contractual agreements that include privacy considerations but no systemic monitoring and reporting on effectiveness of controls. There is no staff member with overall responsibility for ensuring contractual obligations are met. Issues include:

- Third parties management – although security expectations are communicated to third parties within contracts, no processes are in place to evaluate third parties against ACC's expectations, either at the start of a contract, or on an ongoing basis.
- Accredited partnership programme – we understand the contractual relationship and auditing process relating to the Accredited Partnership Programme refers to privacy, however with regard to the monitoring and follow up of privacy compliance, we are not aware of links between the results of the accredited audit and ACC privacy management policies.

Recommendation 5 – Accountability	Indicative timeframe for implementation
The Independent Review Team recommends that ACC take the following actions to strengthen privacy accountability across the whole organisation:	
5.1. Ensure that staff roles and responsibilities for privacy are clearly identified and documented with expectations and accountabilities apparent and measurable.	Within 6 months and 1 year
5.2. Identify and implement a set of key criteria/KPIs for driving and assessing ACC's privacy management performance for the Executive, ACC Managers and staff, and for ACC as a whole that: a. Reflect ACC's privacy vision and objectives for customer satisfaction as well as efficient and effective privacy management. b. Are consistent with ACC's risk settings on privacy. c. Allow it to measure compliance with all the IPPs/HIPRs and other agreed privacy indicators.	Within 1 year
5.3. Ensure that ACC leadership monitor performance against the identified criteria/KPIs so that ACC can change tack if needed.	Ongoing
5.4. Ensure there are processes in place to evaluate third parties against ACC's expectations, either at the start of a contract, or on an ongoing basis.	1 year
5.5. Establish clear reporting requirements to Board level and also report publicly on ACC's privacy performance via the annual report or other appropriate channels.	Interim 6 months, 1 year

8.6 Business processes and systems

Business processes and systems are one of the most significant levels at which it will be critical to recognise the impact of emergence of personal data as the new asset class and the importance of implementing PbD.

The Independent Review Team found a number of indications that there are systemic issues arising in ACC's handling of personal information that are not being addressed in a systematic and organisation-wide manner. The fact that there is no current requirement for privacy considerations and risks to be included as part of developing business processes could be a contributor here.

The Independent Review Team has not undertaken a root cause analysis of practices and it considers this would be needed in order to fully understand the sources of risks and options for management. Some of the practices that the Independent Review Team observed as particularly risky, and which ACC has also recognised, include:

- Email is used as a very common business tool to communicate and interact with claimants and third parties. This has resulted in a heightened inherent risk that information will be unintentionally disclosed from ACC. The use of email to interact with clients and business partners has increased over time. ACC has recognised that email is used extensively, and is currently developing a "portal strategy" (whereby access to information is accessed through web-based applications) to change how it communicates.
- Consistency of messaging and lack of, or limited understanding of:
  - systems functionality
  - allowing use of dual screens
  - ability to open multiple client files on EOS at a time
  - use of and distribution of information within ACC
  - file copy procedures
  - recording, monitoring and reporting of privacy issues and complaints
  - access to EOS not being regularly reviewed and monitored.

Section 8.8 below also points to some of the likely systemic issues that ACC may face in meeting it's obligations to comply with the IPPs and HIPRs and otherwise to meet client and community expectations.

Recommendation 6 – Business processes and systems	Indicative timeframe for implementation
The Independent Review Team recommends that ACC should:	
6.1. Undertake an end-to-end process review of the claims management process, including EOS functionality and other information management systems with a particular focus on privacy risk to: a. Ensure they are consistent with ACC's obligations under the IPPs/HIPRs, including in relation to the extent of personal information collected and best practice in seeking consent. b. Ensure process controls are effective. c. Identify high risk processes, both manual and electronic. d. Implement an "enter once" policy for any data entry or reporting system. e. KPI and reporting processes are automated outputs and by-products of other processes rather than requiring additional manual effort.	1 year
6.2. Re-engineer processes as needed, adopting "privacy by design" and/or "privacy by redesign" principles to minimise risks and improve effectiveness for ACC and its clients.	6 months

Recommendation 6 – Business processes and systems		Indicative timeframe for implementation
6.3.	Review processes by which clients and others on whom ACC holds personal information are able to access, review and challenge or even update that information, drawing on best practices available in other New Zealand government departments and agencies such as the Inland Revenue Department, with a view to implementing an online portal for clients to enable them to access and manage information about themselves online.	6 months
6.4.	Review information exchange practices with employers and ACC health service providers to introduce a requirement that any one report or exchange of information contains personal information relating to only one person or client, supported by appropriate ICT services and processes (such as templates and processes that deliver these requirements for reports on consultations, assessments, discharge summaries etc).	1 year
6.5.	Undertake a systematic review of all business processes that create compilations of personal information about clients other than the actual EOS record, with a view to ceasing them or de-identifying the data and replacing identifying information such as names with random identifiers. In particular: a. Establish a policy and supporting processes to ensure that research, actuarial and similar work streams are never conducted on raw, identifiable information. b. Consider the value in establishing a "de-identification" programme or unit with the responsibility for producing de-identified data for all purposes other than direct interaction with clients and case management, drawing on best practices from around the world.	1 year
6.6.	Develop and implement a strategy to reduce the reliance on the use of email as a business tool to communicate with staff, clients and business partners.	1 year
6.7.	Implement data loss protection software to reduce the likelihood of sensitive information being inadvertently "leaked" through email or other similar internet based communication.	1 year

8.7 Backlogs and establishment of the new Business as Usual

The Independent Review Team would be concerned if ACC's ability to establish an appropriate and effective approach to privacy is hindered by any continued complaint backlogs including in relation to requests for access. A "surge" strategy is required to address any such complaints, and to finalise any document imaging and error correction. This might require additional resources through the establishment of a separate, temporary "backlog unit".

Recommendation 7 – Backlogs and establishment of the new Business as Usual		Indicative timeframe for implementation
7.1.	The Independent Review Team recommends that ACC should provide additional resources to clear backlogs on privacy related processes including the back-log of paper files that need to be electronically scanned, access requests and complaints, in order for ACC and clients to regain trust and feel that a fresh start is under way as soon as possible.	3 months

8.8 Compliance with the IPPs and the HIPRs

This part of the report considers ACC's approach and performance specifically through the lens of the IPPs/HIPRs. The Independent Review Team has made a series of supplementary recommendations in this section. These recommendations are primarily intended to assist ACC in implementing the broader recommendations for ACC's overall management of its privacy obligations but also raise issues that have not been considered elsewhere in the Independent Review. The supplementary recommendations are cross-referenced to the main recommendations.

The Independent Review Team's detailed observations and analysis point to specific areas of risk and areas where there are opportunities to adopt better privacy practice. It considers there is a range of factors in ACC's approach to managing personal information, some minor and others very significant that, if not addressed, increase the risk of non-compliance with the IPPs/HIPRs.

Not unexpectedly, the Independent Review Team finds that the major areas of compliance risk arise in relation to security (IPP 5 and HIRP 5 – Storage and Security of personal information held by an agency or its contractors) and the related risk of unauthorised disclosure to third parties (IPP 11 and HIRP 11 – Disclosure for purpose subject to specific exceptions).

However, there is also room for significant change at the critical point of entry of personal information to ACC systems. ACC's practices in relation to the collection of personal information could be improved both in terms of communications with clients and in ensuring it only collects, or receives, information that is relevant and necessary for its functions and activities. ACC also needs to properly close the loop, ensuring it has a clear understanding on identifying and managing all underlying systemic issues and providing a comprehensive and accessible privacy complaints service.

Below is a discussion of the key areas of risk, or key opportunities, noted against IPPs/HIPRs. The risks and opportunities for better practice are described briefly rather than comprehensively. The intention is to complement the Independent Review Team's recommendations against its identified key themes to highlight areas of practice that should be addressed as a matter priority. Together these would be expected to create the environment and systems for an efficient and effective compliance regime.

8.8.1 IPP 1 and HIPR 1 – collection lawful and necessary

IPP /HIPR 1 is the first level of defence in the protection of personal information. It permits collection of personal information only where it is necessary for an agency's lawful functions and activities. The Privacy Commissioner considered the issue of the collection of medical notes by insurers in 2009. The inquiry was restricted to the activities of private insurers. The Privacy Commissioner's report noted "*I did not consider the position of ACC since, although the general principles about relevance and authorisation still apply, ACC's legislative environment creates some different issues*". The Independent Review Team encourages ACC to note the Privacy Commissioner's conclusion that "insurers that collect full medical notes – even for a specified period – are at risk of breaching the HIPC".[14]

While the AC Act does provide a broad remit for ACC to collect personal information to manage claims, prevent injuries, undertake research and other matters, the Independent Review Team found challenges for ACC in regards to the "necessary" collection of personal information.

[14] Collection of medical notes by insurers - Inquiry by the Privacy Commissioner June 2009 available at http://privacy.org.nz/collection-of-medical-notes-by-insurers-inquiry-by-the-privacy-commissioner/%20New%20Zealand%20Privacy%20Commissioner

ACC continues to receive reports from health providers that include information about more than one client, or which provide information about matters that are not relevant to a particular claim. In the former case, the challenge for ACC is to ensure that only personal information about client A is included on client A's file. ACC does takes steps to manage this internally and the Independent Review Team understands that ACC also works with providers to encourage reporting on a client-by-client, rather than a multiple client basis but that the problem persists, particularly in the hospital sector.

In cases where a claimant's injury is relatively simple or routine, judging whether information is relevant to the claim is fairly obvious. However as cases and injuries get more complex, making judgements on which information is irrelevant requires a certain level of medical expertise. ACC's front-line staff do not have the medical training or qualifications to make judgements on which information is irrelevant for the purposes of managing a claim, pertaining to a certain injury. Again, the Independent Review Team understands ACC works with providers in this area.

ACC's current policy regarding the handling of irrelevant information is unclear or in any event is inconsistently applied. In particular the Independent Review Team observed that while the relevant policy documents state that any irrelevant information should be returned to the provider, in reality there are inconsistent practices including:

- Some staff and managers took the view that ACC is not qualified to make decisions on what is relevant, rather it should rely on the providers to make this decision and so all information provided would be included on the client file.
- In some cases, if information is unrelated to the injury but is related to client, it is still uploaded to EOS.
- The whole report is sent back to the provider.
- The irrelevant sections are blanked out and then the document is uploaded into the clients file on EOS.
- Information not relevant to the claim is destroyed.

ACC currently has no policies or processes regarding the privacy checking of information, prior to it being uploaded to EOS. Any irrelevant information is normally discovered once documents or copy files have been printed and receive a privacy check, prior to being disclosed to an external party.

8.8.2 IPP 2 and HIPR 2 – collect from the individual or with consent

IPP/HIPR 2 promotes the privacy concept of individuals being "in control" of their personal information by encouraging agencies to collect directly from the individual concerned, or to seek their consent to collect from another party, unless there are other practical or public interest considerations.

ACC's general procedure is to seek a client's consent to collect personal information for specified purposes at the outset of claim processing, via the form "ACC 45 Injury Claim Form ("ACC 45")". Claimants who are managed in the branches are required to sign the "ACC 167 Consent to Collect and Disclosure Information ("ACC 167")" and are given additional publications detailing privacy related information, such as "Helping you get back to an everyday life".

The challenge from a privacy perspective is that the consent forms as currently worded are quite broad. Broadly worded consents tend to make it more difficult for individuals to understand what will happen to their personal information and therefore to make informed choices. The client stakeholders who participated in the Independent Review Team's consultation expressed this concern.

The issues identified by the Independent Review Team, ACC staff, or stakeholders include:

- The breadth of the consent form, particularly noting the use of "etc" when describing the bodies from whom personal information might be collected or to whom it might be disclosed so making it difficult to know with certainty who ACC might contact for information or to whom it might be provided.
- The general description of the nature of personal information collected or disclosed does not provide clients with a clear picture of what sort of information will be collected.
- ACC's policy on the "life" of a consent – essentially the life of the claim – and whether this is fair, and understood by ACC staff and clients.
- The process, if any, to withdraw consent.
- Some inconsistency in staff reports of the consent process and what they understand from the guidance provided on consent issues including:
  - if/how to discuss consent and nature of collection/disclosure process with clients
  - multiple consent, modified consents, consent for one claim, if or when applicable to another.
- Whether the consent should include the collection of information for research and statistics – this issue might be better dealt with separately from the consent process. ACC is authorised by the AC Act to use information for these purposes and so does not need consent, and moreover, the Independent Review Team understands it would primarily be using de-identified information for these purposes and the detailed use of identified information would be subject to ACC's ethics review process.

While the consent forms may be considered to comply – and this has been tested in at least one complaint to the Privacy Commissioner in 2001 – the Independent Review Team considers there is an opportunity for a better practice review. It strongly encourages ACC to consider detailed consultation with stakeholders as part of any review.

8.8.3 IPP 3 and HIPR 3 – tell people purpose of collection, usual disclosures rights and other specified matters

IPP/HIPR 3 also aims to put individuals in control of personal information about them. It requires agencies that are collecting information to take reasonable steps to make individuals aware of matters such as the purpose of collection. ACC provides the information required by IPP/HIPR 3 in a number of places:

- Privacy statement on website.
- ACC 45 – initial claim form.
- ACC 167 – Consent to collect and disclosure information.
- Personal information and disclosure statement (INPIS01).
- Staff discussions.
- Privacy warnings on inbound calls re voice recordings.
- Other claimant information publications.

The Independent Review Team has not identified significant compliance issues in respect to IPP/HIPR 3 although there appear to be some minor gaps in meeting its requirements. For example, the ACC 167 does not specifically identify information as being voluntary or mandatory or set out the consequences of not providing the information. In addition, the description of usual disclosures is very broad; it would be difficult for claimants to get a realistic picture of what disclosures will happen in their particular case. The form does not mention usual disclosures for data-matching, health system payments, other government interests or disclosures in the context of reviews or appeals.

Apart from these points, there is a range of other information that better practice privacy approaches would encourage including more detailed information on ACC's approach to privacy and how it collects, uses, holds and discloses personal information, in particular with relation to:

- ACC's general approach to handling personal information – often addressed in a detailed privacy policy.
- More specific information on what is collected when (this might take the form of fact sheets for different stages in process or guidance to staff to have regular detailed discussions with clients as their case proceeds).
- Data retention (see IPP/HIPR 9 discussion below).
- Circumstances in which personal information will be used or disclosed for statistics or research and the safeguards, including the ethics process and guidelines and when specific consent would be sought.
- Processes to have concerns heard or to make a privacy complaint.

The Independent Review Team also encourages ACC to consider how it is communicating privacy information to its clients and the community. There has been considerable research undertaken in this area, for example into the concept of "layered privacy notices", which recognise that individuals have different ways of absorbing information and need different levels of information at different stages in an interaction.[15]

8.8.4 IPP 4 and HIPR 4 – fair, not unreasonably intrusive collection

This principle focuses on the means of collection and protects individuals from unfair or unreasonably intrusive processes.

The Independent Review Team did not observe any specific issues in this area. However, it notes that the HIPC indicates that it would be inconsistent with HIPR 4 to adopt an "overbearing or threatening manner". It also notes that there is at least the perception amongst some in the community that ACC treats clients suspiciously or in a way that is considered to be "bullying". The Independent Review Team encourages ACC to regularly seek stakeholder feedback on this issue and to consider any reports of poor practice that may need to be addressed at least as a culture issue and possibly in recruitment, training, policies and procedures.

8.8.5 IPP 5 and HIPR 5 – Storage and Security of personal information held by an agency or its contractors

IPP/HIPR 5 requires agencies to protect personal information "by such security safeguards as it is reasonable in the circumstances to take" against loss, unauthorised access, access, use, modification, or disclosure and other misuse.

To perform its functions ACC must collect and hold extensive amounts of very sensitive personal information. The Independent Review Team was not convinced that ACC's approach to security is reasonable in these circumstances.

It found a wide range of persistent issues – some small, others more significant – that could lead to, contribute to, or have resulted in, breaches of IPP/HIPR 5. ACC branches maintain privacy risk registers which include most of the issues identified, however, the use of the registers varies amongst the branches from being an active resource to only being sporadically used.

The Independent Review Team considers that ACC's policy and procedures on its first level response – that is what to do if a breach or potential breach is found – could be strengthened in a range of

[15] This approach has been devised to deal with the issues noted above and draws on research conducted by Hunton & Williams Centre for Information Policy and Leadership (CIPL) and which was then endorsed by international Data Protection Commissioners conference at their 2003 Sydney and further refined in a multi party workshop in Berlin in 2003 – see the Center for Information Policy Leadership and www.privacyconference2003.org/resolution.asp and www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf

ways. It also considers that a key question is whether there are sufficient mechanisms for ACC to become aware of, and manage, the underlying systemic issues. Some of the issues observed are listed here to give a flavour of the matters identified and to flag priority areas for review and action:

- Managing "copy file" requests – there is a large volume of entirely legitimate requests by individuals for a copy of their files. Files can be in electronic or paper form and in the case of older claims could extend to many volumes. The Independent Review Team observed inconsistencies in guidance and practices, and there are many reported instances of information about another client mistakenly being included in the file copy provided.
- Scanning risk – ACC operates an electronic filing system and all hard copy documents it receives are scanned and uploaded to client files. Issues include pages from a document omitted or scanned to another client's record, and scanned documents about client A being uploaded to another client's record.
- Uploading electronic documents or emails – similarly, documents might be uploaded to the wrong file.
- Mailing risk – outgoing letters and documents may be misaddressed or mistakenly include material relating to other clients.
- Role based access particularly to sensitive claims – there are three classifications of claims which impose a restriction on access to claimant information. These are VIP claims, sensitive claims and staff claims.
- In practice claimants with VIP indicators include various high-profile (formal policy allows for the VIP status to be allocated to the following categories, namely the Governor-General, Members of Parliament, Members of the Judiciary, ACC Board members and members of their immediate family) people outside of this list. The only difference between the treatment of VIP and general claims is that the access of VIP claims is limited to a selection of ACC staff. All staff have the ability to put a VIP indicator on a claim, but only those with VIP access are able to remove the indicator.
- While ACC's approach to managing access to sensitive claims is role based, in practice there is very wide access to sensitive claims files. There are questions about how roles are defined, whether there are opportunities to move from an "all or nothing approach" to something more targeted to information needs and whether access management could be more robust, including proactive monitoring of file access.
- Extensive use of spreadsheets – ACC staff use spreadsheets for a range of reasons including work management, analysis, and management reporting and routinely email the spreadsheets, often containing identifiable personal information about multiple clients, to other ACC staff.
- Secure printing has been implemented but is not consistently used by all staff. When secure printing was introduced it was not adequately communicated to staff that it was one of many controls protecting the privacy of personal information, and that the other controls were still equally important. In some cases this resulted in less rigour in other areas of the copy file process.
- Practices relating to email usage both incoming and outgoing – ACC is increasingly moving to electronic communications and so email is currently an increasing and critical part of its communications. The Independent Review Team identified a range of risks in this area, and ACC gives direction to staff on a range of matters including encouraging use of direct contact by telephone, and is in the process of making a range of changes. The risks include: wrongly addressed emails, the content of emails, attaching information relating to other clients, and uploading emails to the wrong file.
- VIP claims management process is unclear with respect to who warrant "VIP status" and the resulting claims management processes.
- The watermarking of files released externally is not a common practice apart from the sensitive claims unit.

- Inconsistent and undocumented policies for ensuring an appropriate level of security for providers' method of receiving claimant information, in particular sending information to non-professional email addresses.

8.8.6 IPP 6 and HIPR 6 – individual access

IPP/HIPR 6 promotes an individual's control of personal information about them by giving them a right of access, in most circumstances, to all personal information an agency holds about them. The Independent Review Team's observation is that ACC is very aware of its client's rights and expects to be very responsive to them. As noted in the discussion of IPP/HIPR 5 above, the inclusion of information about another client in the response to an access, or "copy file", is a major security issue. Apart from this, the Independent Review Team was not able to get a clear picture of the extent to which ACC is meeting acceptable practice in this regard. Anecdotally, there are issues, however at this point the Independent Review does not have statistics available to it to assess the number of access requests, or the nature of complaints that may be made in this context, including failure to provide timely access.

Some possible issues in relation to the handling of access requests were observed including:

- Under Section 29 of the Privacy Act, ACC has the right to refuse a personal information request if they believe the information would be likely to prejudice the physical or mental health of that individual. This may only occur after consultation with the claimant's medical practitioner. Awareness of this right is not high throughout the organisation, with the exception of the Sensitive Claims Unit who on occasion will not release certain documents to the claimant on this basis.
- The risk that the information provided in the "copy file" will not contain all information held by ACC relevant to the claimant. For example, in EOS complaints are recorded at party level and "copy files" include information held at a claims level. Additionally, complaints handled directly by the Government Services team are recorded in Action Remedy not EOS, so are not included in "copy files" generated by branch staff.
- IT Sweeps – Prior to December 2010, ACC email interaction with claimants was not uploaded onto their EOS files. Claimants can request an IT sweep which will be a file of all emails sent about the claimant prior to this period. To date ACC had not developed guidelines or process on how to handle this and the Independent Review Team observed different practices, and was advised of some policy issues, in the branches it visited.
- As reported in the stakeholder meeting, the timeframe to get access to personal information from an accredited employer under the ACC Partnerships Programme can be significantly longer than getting access from ACC.

8.8.7 IPP 7 and HIPR 7 – correction or adding statement

Together IPP/HIPR 7 and IPP/HIPR 8 recognise the potential inconvenience or real harm to individuals if inaccurate information is acted upon. This principle gives individuals the right to seek to have inaccurate information corrected. The Independent Review Team observes that ACC has policy and processes in place to respond to requests. It did not find particular process issues in the context of the Independent Review.

8.8.8 IPP 8 and HIPR 8 – check accuracy before use

This principle obliges agencies to take reasonable steps to check the accuracy of personal information before it is used.

In discussions with ACC frontline staff, with managers and with corporate staff there was frequent mention of potential and actual risks to the accuracy of personal information. Some of these risks appear to be managed, others appear to not be getting detailed attention to identify and find solutions to the underlying problem. Sources of risk to personal information inaccuracy include:

- The Enterprise Data Warehouse runs daily and weekly updates – client details are part of the weekly component and so any updates do not take effect until after the weekend when the update is done.
- Scanning – as noted above, there is a risk that when documents are scanned they will end up on the wrong client's file; at this point the Independent Review Team cannot comment on ACC's record in this regard compared to similar organisations processing similar volumes of data.
- ACC relies on client information provided by its providers to send information to clients about a claim or in some cases to update its own records – there is a persistent problem of providers not updating details or otherwise providing incorrect details to ACC with the result that information may be provided to an ex-employer or sent to the wrong address.

8.8.9 IPP 9 and HIPR 9 – data retention only for purpose for which collected

IPP/HIPR 9 reflects the general approach from a privacy perspective is to keep personal information in identified form for the minimum time possible. The aim is to minimise the risk of use of older inaccurate information, security threats over time and the use of information for new purposes that were not contemplated at the time the information was collected.

ACC's Claims Record Retention and Disposal Schedule specifies that in the main records will be kept "75 years after the date of the last action ACC has recorded on the claim". There is no technical compliance issue here, however, from a privacy perspective there are issues to consider including:

- The extent of claimant/community awareness of the practice.
- The security risk in keeping personal information in identified form for such an extensive period.
- The potential for the personal information to be used for new purposes without the knowledge of the individuals concerned.

8.8.10 IPP 10 and HIPR 10 – Use for purpose, directly related purpose, authorised etc

IPP/HIPR 10 aims to keep personal information "under control" by permitting uses outside of the individuals likely expectations only with consent or where there are other public interests that need to be considered.

The Independent Review Team did not find indications or evidence that ACC's use of personal information prima facie would be inconsistent with the IPP/HIPR 10. There were some practices observed that suggest there is room for ACC to identify and review practices that may heighten the risks of inappropriate use or reuse (and which may also lead to security risks). The practices observed include:

- Management reports including New Zealand wide information – for example the weekly change of bank account report (a potential fraud indicator) – circulated to all managers.
- Reports generated by Business Intelligence do not specifically identify whether sensitive claims information has been included.
- Use of identified information for statistical analysis.
- Policy on use of voice recordings – we understand it is used only for training and performance review and are discarded after 6 weeks however, the Independent Review Team did not see specific policy or processes for this.

8.8.11 IPP 11 and HIPR 11 – Disclosure for purpose subject to specified exceptions

IPP/HIPR 11 is also about keeping personal information under control by specifying the circumstances under which agencies can disclose personal information to external parties. This prohibits the disclosure of information to external parties without appropriate consent from the individual. Exceptions include disclosures that are authorised by law, or which are necessary for the protection of the public revenue or enforcement of the criminal law.

Breaches of IPP/HIPR 11 are very often intrinsically linked with breaches of IPP/HIPR 5 so that they are often investigated or reported together. The Independent Review Team has not re-listed all of the issues noted under IPP/HIPR 5 that could be contributing to an unauthorised disclosure of personal information but draws attention to the link, for example issues in the handling of "copy files" (requests for access under IPP/HIPR 6) lead to compliance risks under IPP/HIPR 5 but equally raise risks in relation IPP/HIPR 11.

It is important to note ACC works on the basis that it has its clients' consent to disclose. The Independent Review Team supports the approach of seeking consent, provided that consent is appropriately targeted and informed (see discussion under IPP/HIPR 2 above). In addition the Independent Review Team considers that even where ACC has consent, from a best practice perspective it should be aware of and manage for the consequences to claimants of inappropriate or excessive disclosure. The areas that the Independent Review Team considers may need further development in policy and practice include:

- Disclosure of information to third parties or providers – for example, how much to disclose about a claim, what is relevant and what is not. While these matters are discussed in training, the Independent Review Team understands that generally ACC relies on frontline staff's judgement and does not provide guidance to staff.
- Addressing to employers – practice to address to company, not a specific person or role – could be opened by anyone – people not authorised to receive such information.
- Accidental death – there is not currently set templates for all of the letters that they have to send out, so they reuse saved letters. There is potential for a privacy breach if they do not change all of the details.
- Child and adolescent clients – legal guardian issues, sending information to caregivers.
- Disparity between call centres on whether a spouse has authority to have all information disclosed to them – complaints where information was given and now will not be given without consent. Where to find consent/add consent in EOS can be an issue.
- "ACC 45 Injury Claim Form" – considered as consent to disclose by work injury team in the context of payment disputes with employers – if employer requests a breakdown of payments, written consent must be given by employee.
- Release of information that does not include names but is identifiable – for example ACC has responded to media requests seeking information about rare or unusual accidents, such as a specific animal bite, which might allow the identity of the victim to be established. The Independent Review Team has not identified ACC guidelines to assist staff in making decisions about release of de-identified personal information.

8.8.12 IPP 12 and HIPR 12 – Unique Identifiers – only if necessary, disclosure required only for purpose

IPP/HIPR 12 recognises the power of unique identifiers in any process of accurately bringing together information about an individual collected in different contexts. The principle limits agency collection, use and disclosure of unique identifiers to specified circumstances. The Independent Review Team has not identified any issues in relation to IPP/HIPR 12.

IPP/HIPR Compliance Recommendations

Principle	Recommendation
IPP/HIPR 1	ACC should review its policy and procedures for the collection of personal or health information, taking account of the Privacy Commissioner's inquiry into the collection of medical notes by insurers to ensure that its staff, clients and providers are quite clear on the steps it will take when it receives medical reports or other information that might not be relevant in the processing of a claim or other circumstances. ACC should ensure the policy is promulgated to staff and that it also provides detailed guidance to assist in decision-making. ACC should monitor its collection practices at least yearly and take other steps as needed, including liaison with providers and further amending policies and procedures. (See also Recommendations 3 and 6)
IPP/HIPR 2	ACC should review its processes and forms for seeking consent to collect and disclose information to ensure that they are consistent with best legal and privacy practices and take account of ACC's clients' interests. ACC should establish processes to allow for detailed ongoing stakeholder consultation on the development and implementation of consent processes. Subject to the above, ACC should make its forms and consent processes: ■ As specific as possible to a claimant's circumstances. ■ Address the need to renew consent from time to time. ■ Consider the circumstances in which consent may be withdrawn (for future disclosures) and the consequences. ■ Not cover collection or disclosure of personal information where ACC does not need consent and instead provide information about such collection or disclosure in appropriate language, formats, and locations. (See also Recommendation 3 and 6)
IPP/HIPR 3	ACC should review the way in which it provides privacy information to its clients as required by IPP/HIPR 3 and best practice, to ensure it is consistent across forms and channels, is comprehensive and takes account of client's different information needs at different points in their claims process. Unless it can meet best practice other ways ACC should adopt a layered notice approach and should develop a detailed privacy policy on all aspects of its privacy commitment, its handling of personal information and its privacy complaint handling processes and make this generally available to clients and members of the community. (See also Recommendation 3 and 6)
IPP/HIPR 4	ACC should monitor the community perception of its collection processes and undertake detailed stakeholder consultations and address any issues identified in its privacy culture, recruitment, training or policies and procedures. (See also Recommendations 2, 3 and 4)
IPP/HIPR 5	In developing its response to this report and to its approach to its privacy management obligations, ACC should ensure that it addresses the security issues identified in this report or in other feedback from the review process. (See also Recommendation 3 in Section 8)

Principle	Recommendation
IPP/HIPR 6	ACC should review its "copy file" processes to ensure that it is able, including through IT sweeps and collation of information from all units, to provide all the information requested. ACC should also engage with claimant groups to ensure that its processes are meeting their needs and assist them to target requests as appropriate. ACC should review its processes for collating and providing "copy files" with specific reference to limiting risk of security breach or unauthorised disclosure. Within legal requirements, ACC should set and measure benchmarks, including processing times, for responding to requests for access under IPP/HIPR 6 and it should ensure that the same benchmarks apply to accredited employers. (See also Recommendation 6)
IPP/HIPR 7	No Recommendations made.
IPP/HIPR 8	In developing its response to this report and to its approach to its privacy management obligations, ACC should ensure that it has developed benchmarks for accuracy and that it addresses the risks to accuracy identified in this report or in other feedback from the review process. (See also Recommendation 6)
IPP/HIPR 9	ACC should review its practices in relation to the retention of personal information to ensure that: ■ Retaining identified client information for 75 years after the last interaction is appropriate. ■ Claimants and the community are aware of the practice. ■ It has identified and addressed the security risk in keeping personal information in identified form for such an extensive period. ■ It has in place strict governance and other arrangements to ensure that claimant information is only used for new purposes following detailed consideration including wide public consultation and that decisions are taken at least to Board or Executive level.
IPP/HIPR 10	In developing its response to this report and to its approach to its privacy management obligations, ACC should ensure that it considers the issues in relation to use of personal information identified in this report. (See also Recommendation 2 and 3)
IPP/HIPR 11	In developing its response to this report and to its approach to its privacy management obligations, ACC should ensure that it addresses the disclosure risks identified in this report, in particular, that it provides clear instructions and training to staff to ensure that only needed and appropriate information is disclosed in the context of claims processing. (See also Recommendation 2, 3 and 6)
IPP/HIPR 12	No recommendations made.

Appendix 1 – Review Terms of Reference

Independent Review of
ACC Privacy and
Security of Information

23 March 2012

Contents

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.

Appendix 2 – About ACC

ACC's role is to manage New Zealand's accident insurance scheme set up under the AC Act in a cost-effective, outcome-focused way that ensures the Scheme is financially sustainable for future generations. This role means that it engages with many New Zealanders as well as overseas claimants and that it handles very significant amounts of sensitive personal and health information.

In the July 2010 to June 2011 period, ACC processed 1.5 million new claims, managed 1.9 million existing claims and paid out a total of $2.2 billion[16]. During that period (2010 – 2011[17]) 60 complaints about ACC were received by the OPC.

This section provides an overview of ACC's management and organisational structure and key pieces of legislation and codes under which this review was conducted.

ACC's Board and Management

ACC is governed by a Board accountable to the Minister for ACC for the performance of the organisation. As noted earlier during the course of the Independent Review there has been movement in governance to the ACC Board. These include:

- The Chair, Deputy Chair and three other Board Members' first term (of three years) expired on 31 March 2012. The Minister asked, and all agreed to remain on the Board while the Minister considered the Membership of the Board as the Minister was only appointed as Minister for ACC on 12 December 2011.
- On 12 June 2012 the Minister decided to not reappoint the Chair, Deputy Chair and one other Member for a second term (of three years). The Minister asked, and all agreed to remain on the Board until 30 June 2012.
- The Minister also offered a second term on the Board to the two other Board Members' whose terms expired on 31 March 2012. One Board Member accepted the reappointment and the other Board Member tendered his resignation effective from 31 July 2012. The Minister accepted his resignation on 21 June 2012.
- On 13 June 2012, following the departure of the Chair, Deputy Chair and one other Board Member, the Chief Executive decided to step down. The Board accepted his resignation on 18 June 2012; however the Chief Executive departure date has not been agreed with the Board.
- In June 2012, the Minister for ACC and ACC signed a Service and Purchase Agreement 2012-2015 outlining the quality and quantity of services to be provided by ACC. The Agreement reflected the Government's priorities for ACC.

Under the previous ACC Board the following arrangements were in place:

- Three ACC Board sub-committees, the Audit and Risk Committee, Investment Committee and Remuneration Committee were established to assist the ACC Board to discharge its responsibilities.
- Day-to-day management of ACC is delegated to the Chief Executive. With Board oversight, the Chief Executive is responsible for providing leadership to the organisation, overseeing ACC's

[16] ACC Injury Statistics Tool accessed 23 July at http://www.acc.co.nz/about-acc/statistics/injury-statistics/index.htm#results

[17] *Annual Report of the Privacy Commissioner 2011* available at http://privacy.org.nz/annual-report-of-the-privacy-commissioner-2011/

systems and internal controls, monitoring operational and financial activities and ensuring the organisation achieves its business objectives, including risk management and ethical behaviour.

- Day-to-day operations are managed by ACC managers under the leadership of the Chief Executive.

ACC's priorities and strategic direction

The leadership team and Board are responsible for developing and implementing ACC's strategic and business plan, consistent with government priorities. In 2011 ACC began a process of renewing its strategic and business plan objectives to focus more on customer centricity and culture. This process, led by the Chief Executive, started in November 2011 and the Board approved the Plan in February 2012. This renewed focus on the customer is reflected in the government's key priorities for ACC.

Government's key priorities for ACC

ACC works under a Service and Purchase Agreement made with its Minister.

During the period under review, ACC was operating under the 2009-2012 Service and Purchase Agreement. Government's key priorities under this agreement included delivering value-for-money and demonstrating performance, with the following specific priorities for the ACC portfolio:

- Priority 1: To ensure the Scheme has a sustainable structure that will deliver affordable levies going forward.
- Priority 2: Undertake a stocktake of ACC Accounts and benchmark the Scheme against appropriate jurisdictions (to support the achievement of Priority 1).
- Priority 3: Provide advice on the legislative framework for accident compensation and rehabilitation, supported by monitoring and reporting on the performance of the Scheme and ACC's performance in administering it.

A new agreement came into effect on 1 July 2012, during the course of the Independent Review, which placed more emphasis on privacy. ACC's Minister said that the new agreement "represents a rebalance of the broader responsibilities ACC has to all New Zealanders" and that "ACC must achieve outcomes that are consistent with the letter and spirit of the legislation, while still preserving public trust and confidence"[18].

The Government's priorities for ACC as reflected in the Service and Purchase Agreement 2012-2015 between the Minister for ACC and ACC are:

- Priority 1: Improved trust and confidence.
- Priority 2: Improved management and security of private information.
- Priority 3: Maintain focus on levy stability and financial sustainability.
- Priority 4: Providing high quality services for clients.
- Priority 5: Ensuring early resolution of disputes.
- Priority 6: Reporting on the performance of the Accredited Employer Programme.

Included in the Service and Purchase Agreement are performance measures for each priority and are the ACC Board's accountability measures to the Minister.

[18] Minister Collins media release 28 June 2012 available at http://www.beehive.govt.nz/release/minister-sets-new-priorities-acc

ACC's stated outcomes

ACC sets out its key performance expectations in its Statement of Intent ("SOI") 2012-2015.[19] Its expected outcomes for the period are:

- Outcome 1: Rehabilitate injured people in New Zealand more effectively.
- Outcome 2: Delivering levy stability by achieving long-term financial sustainability.
- Outcome 3: Reducing the incidence and severity of injury where it is cost effective to do so.

These outcomes have been realigned to the key priorities as outlined above.

Programme of delivery

ACC is currently in a transition phase of affecting change through its programme of delivery as outlined in its strategy. The programme of delivery is categorised under five main areas and each is headed by an Executive and is supported by senior management. The main focus of the programme of delivery and the key result areas for each are outlined below:

- Programme of delivery 1: Quality results for the injured – improving return to work rates, enhancing quality of rehabilitation and increasing client service satisfaction.
- Programme of delivery 2: World class operating performance – reducing underlying levy rates, maintaining solvency track and improving returns from Insurance operations.
- Programme of delivery 3: Better support and service for levy payers – increasing levy payer satisfaction, enhancing service duration and quality and Improving self service capability.
- Programme of delivery 4: Improving health sector outcomes – ensuring provider quality, maximising health procurement savings and increasing provider satisfaction.
- Programme of delivery 5: Enterprise strategy development – developing ACC's capability and capacity.

ACC's staffing and organisational structure

ACC has approximately 2,800 staff members with the majority being case managers who facilitate the provision of the services required to help claimants recover from their injuries. Staff work in a variety of locations around New Zealand. These include a network of 26 branch offices, service centres, contact centres, specialised units and Corporate Office as follows:

- Inquiry Service Centre – experienced staff answer incoming phone queries from ACC clients, providers, employers and other key stakeholders.
- Contact Centres – staff manage claims of shorter duration (for example claims for clients with fewer than 70 days off work as a result of accident and/or fewer than 90 days of home-based rehabilitation).
- Service and Processing Centres – staff receive, register and assess injury claims cover. There are teams that calculate and process weekly compensation payments for clients. Service and processing centres also manage accidental death, hearing loss and dental claims, assess requests for rehabilitation entitlements and process claim-related invoices to service providers.

[19] ACC Statement of Intent 2012-2015 available at http://www.acc.co.nz/PRD_EXT_CSMP/groups/external_communications/documents/papers_plans/wpc112796.pdf

- Treatment Injury Centre – specialised staff assess and make decisions on claims that involve injuries from medical treatment. The centre also collects data from treatment injury claims.
- Sensitive Claims Unit – claims for physical and/or mental injury suffered as a result of sexual abuse or assault are managed by the Sensitive Claims Unit.
- National Serious Injury Service – specialises in working with people who have suffered serious injury such as spinal cord or traumatic brain injury.
- Recover Independence Service – manages claimants who have been receiving weekly compensation for a cumulative period of greater than 912 days.
- Business Service Centres – manages contacts with business clients. They assist levy payers to understand their ACC levies, manage payment options and resolve queries.
- Corporate Office – comprises of business groups that are responsible for managing ACC's corporate operations such as Governance, Policy & Research, Finance, Actuarial Services, People and Communications, Claims Management, Insurance & Prevention Services, Enterprise Planning and Information Technology.

ACC's legislative and regulatory framework

The key pieces of legislation and codes which apply to ACC and under which the review was conducted are as follows:

Accident Compensation Act 2001

Overview

In general terms, this Act is arranged as follows:

(a) Part 1 deals with preliminary matters such as the purpose of the Act and definitions.

(b) Part 2 determines whether a person has cover.

(c) Part 3 provides –

  (i) for the preparation and approval of a Code of ACC Claimants' Rights; and

  (ii) how to make a claim under this Act for cover and entitlements, and the process the Corporation must follow in deciding claims.

(d) Part 4 sets out what the entitlements are and Schedule 1 sets out the detail of the entitlements.

(e) Part 5 provides for the resolution of disputes about decisions.

(f) Part 6 provides for the management of the Scheme and for the setting and collection of levies.

(g) Part 7 continues the Accident Compensation Corporation and governs its operations.

(h) Part 8 relates to the management of injury-related information.

(i) Part 9 sets out miscellaneous provisions such as provisions about offences and penalties, and regulation-making powers.

(j) Part 10 provides for the continuation of an orderly transition from the competitive provision of workplace accident insurance.

(k) Part 11 provides transitional provisions for cover, entitlements, reviews and appeals, and financial matters relating to former Acts.

The following sections sets out the purposes for which ACC can collect information:

Section 279 - Purposes for which Corporation to collect information

1. The Corporation may collect information for the following purposes:
   a) to enable a comprehensive claims database to be maintained.
   b) to facilitate the monitoring of the operation of this Act.
   c) to monitor and evaluate the nature, incidence, severity, and consequences of injuries.
   d) injury prevention.
   e) the provision of appropriate rehabilitation and treatment.
   f) the provision of appropriate compensation.
   g) policy development under this Act.
   h) determining the cost to society of personal injury.
   i) levy setting.
   j) scheme management.
2. The Corporation must collect –
   a) such information as is prescribed for the purposes set out in subsection (1)(a) to (i) by regulations made under this Act.
   b) information for such of the purposes set out in section 287 that are prescribed by regulations made under this Act.
3. Information prescribed for the purpose set out in subsection (1)(a) must include information about the circumstances of the personal injury, the nature and severity of the personal injury, and its consequences.

Section 287 - Management of injury-related information

The purpose of this Part is –

a) to facilitate the achievement of the Government's overall injury management (including injury prevention) objectives, as determined from time to time, through information collection.
b) to facilitate the development and maintenance of a coherent set of statistics and indicators, and a research database on injury-related information.
c) to enable the analysis of such information to enhance policy development in both the government and private sectors.
d) to facilitate the dissemination of such information across all appropriate sectors (including the government and private sectors).
e) to enable the effectiveness of government agencies to be monitored in relation to the Government's overall injury management (including injury prevention) objectives.

ACC Claimants' Code of Rights imposes obligations on ACC regarding ACC's treatment of clients. Right 7 of the Code states that all claimants have the right to have their privacy respected, which includes compliance with legislation and granting all claimants access to their information in accordance with legislation.

The Official Information Act 1982 ("OIA")

The purpose of this legislation is:

- To increase the availability of official information to the people of New Zealand in order to promote more effective participation in the making and administration of laws and policies.
- To promote the accountability of Ministers of the Crown and government officials.

- To protect sensitive information where necessary in the public interest or to preserve personal privacy.

The Privacy Act 1993

The Privacy Act governs the collecting, using and the storing of personal information by agencies. The rules for the handling of personal information are set out in the twelve Information Privacy Principles ("IPPs"):

- IPPs 1-4 govern the collection of personal information. This includes the reasons why personal information may be collected, where it may be collected from, and how it is collected.
- IPP 5 governs the way personal information is stored. It is designed to protect personal information from unauthorised use or disclosure.
- IPP 6 gives individuals the right to access information about themselves.
- IPP 7 gives individuals the right to request correction of information about themselves.
- IPPs 8-11 place restrictions on how people and organisations can use or disclose personal information. These include ensuring information is accurate and up-to-date, and that it isn't improperly disclosed.
- IPP 12 governs how "unique identifiers" – such as IRD numbers, bank client numbers, drivers licence and passport numbers – can be used.

Section 23 of the Privacy Act provides that "*It shall be the responsibility of each agency to ensure that there are, within that agency, 1 or more individuals whose responsibilities include (a) the encouragement of compliance, by the agency, with the information privacy principles: (b) dealing with requests made to the agency pursuant to this Act: (c) working with the Commissioner in relation to investigations conducted pursuant to Part 8 in relation to the agency: (d) otherwise ensuring compliance by the agency with the provisions of this Act*".

The Health Information Privacy Code 1994

This code of practice recognises those expectations that health information should be treated differently. It applies specific rules – the Health Information Privacy Rules ("HIPRs") – to agencies in the health sector to better ensure the protection of individual privacy. With respect to health information collected, used, held and disclosed by health agencies, the code substitutes for the information privacy principles in the Privacy Act. ACC is considered to be an agency in the health sector and therefore must consider the HIPRs as well as the IPPs.

The rules in the Code are summarised as follows:

- Only collect health information if you really need it.
- Get it straight from the people concerned.
- Tell them what you're going to do with it.
- Be considerate when you're getting it.
- Take care of it once you've got it.
- People can see their health information if they want to.
- They can correct it if it's wrong.
- Make sure health information is correct before you use it.
- Get rid of it when you're done with it.
- Use it for the purpose you got it.
- Only disclose it if you have a good reason.

- Only assign unique identifiers where permitted.

The Public Health Act 1956

Section 22C subsections (1) & (3) Disclosure of Health Information:

(1) Any person (being an agency that provides services or arranges the provision of services) may disclose health information—

(a). if that information—

(i). is required by any person specified in subsection (2); and

(ii). is required (or, in the case of the purpose set out in paragraph (j) of that subsection, is essential) for the purpose set out in that subsection in relation to the person so specified; or

(b). if that disclosure is permitted—

(i). by or under a code of practice issued under section 46 of the Privacy Act 1993; or

(ii). if no such code of practice applies in relation to the information, by any of the information privacy principles set out in section 6 of that Act.

(3) For the purposes of principle 11(d) of the Privacy Act 1993, the disclosure of health information about an individual may be authorised—

(a). by that individual personally, if he or she has attained the age of 16 years; or

(b). by a representative of that individual.

Appendix 3 – Interviews conducted for the review

Below is the coverage of business areas and the number of staff interviewed throughout the Independent Review process:

Branches/ Location	Number of staff Interviewed	Number of Privacy Champions	Business area
Corporate Office - Wellington	85	3	■ ACC Board Members* ■ Accounts Payable ■ Actuarial Services ■ Assurance Services ■ Business and Programme Management ■ Business Improvement ■ Business Technology Group ■ Chief Executive's Office ■ Claims Management ■ Claims Processing & Specialist Services ■ Collections, Debt Management Unit ■ Communications External ■ Communications Internal ■ Data Management Services ■ Enterprise Planning & Information Technology ■ Executive Management ■ Governance, Policy & Research ■ Health & Safety ■ Insurance & Prevention Services ■ Learning & Development ■ Office of Complaints Investigator ■ Organisational Development, People Services ■ People and Communications
Sensitive Claims Unit - Wellington	10	2	■ Claims Management ■ Child & Adolescence
Christchurch Branch	4	0	■ Recover Independence Service
Counties Manukau Branch	19	2	■ Cultural Services ■ Front-line staff ■ National Serious Injury Service ■ Recover Independence Service ■ Relationship and Performance

Branches/ Location	Number of staff Interviewed	Number of Privacy Champions	Business area
Dunedin Branch	2	1	■ Front-line staff
Hastings Branch	7	2	■ Front-line staff ■ National Serious Injury Service ■ Recover Independence Service
Hamilton Branch	7	1	■ Customer Support Officer ■ Front-line staff ■ National Serious Injury Service ■ Recover Independence Service
Nelson Branch	6	1	■ Front-line staff ■ Recover Independence Service
Wellington Branch	5	1	■ Front-line staff ■ Recover Independence Service
Dunedin Service Centre	19	1	■ Cover Assessment ■ Elective Service Centre ■ Injury Service Centre ■ Lump Sum Unit ■ Registration Centre ■ Scanning Unit ■ Short Terms Claims Centre
Te Rapa Service Centre	14	2	■ Accidental Death ■ Administration ■ Claims Lodgement ■ Client Support Services ■ Inquiry Service Centre ■ Quality Assurance ■ Independent Review Team ■ Scanning Unit ■ Short Terms Claims Centre
TOTAL	**178**	**16**	

* Written statement provided.

Additionally we conducted interviews with the following parties external to ACC:

Stakeholders interviews	
■ A member of Parliament. ■ State Services Commission. ■ Office of the Privacy Commissioner. ■ Office of the Ombudsman. ■ ACC claimants/clients. ■ Claimant advocates. ■ ACClaim Otago. ■ New Zealand Orthopaedic Association. ■ New Zealand Council of Trade Unions.	■ Brain Injury Association of New Zealand. ■ Consumer. ■ Association of Psychotherapists. ■ Carers New Zealand. ■ Royal New Zealand Returned and Services Association. ■ Wellington Community Law Centre. ■ Business New Zealand. ■ Midwifery Council of New Zealand.

Appendix 4 – Chronology of events relating to the Breach

Date	Event
5 August 2011	The RIS Manager sent an email to the Client, inadvertently attached to the email was an internal ACC monthly management report containing limited personal information on 6,748 ACC clients.
16 August 2011	The Client emailed a response to the RIS Manager and copied the OPC and the Ombudsman's Office. The email thread contained the original email sent by the RIS Manager to the Client on 5 August 2011 but not the attachment.
14 September 2011	The Client met with an ACC Board member and raised a number of issues about ACC's handling of claims and managing personal information and specifically the Client's claim. The Board member sent the Chair an email passing on the concerns raised by the Client.
16 September 2011	The Chair forwarded the email he received from the Board Member to the Board and Corporate Secretary.
4 October 2011	The Board and Corporate Secretary asked the Acting National Manager Claims to organise a meeting with the Client. The purpose of the 1 December 2011 meeting was to listen to the Client's concerns regarding the Client's rehabilitation with the view to agreeing a way forward.
14 October 2011	The Client emailed the Board Member and copied the Chair and the Board and Corporate Secretary about her concerns with ACC not respecting client's rights and not complying with the Code.
26 October 2011	The Client forwarded the email received from the RIS Manager on 5 August 2011to the State Services Commission which included the Breach information.
1 December 2011	The Client met with two senior ACC Managers. At the meeting it was disclosed that the Client had received personal information relating to the Client "plus about six and a half thousand other claimants…" via email from ACC. The Client also gave the ACC Managers a list of 45 alleged breaches of legislation, guidelines or codes by ACC. The ACC Managers asked the Client whether ACC were aware of the Breach and whether the Client still had the Breach information. The National Manager Claims and the Board and Corporate Secretary were informed the meeting had taken place and that a list of alleged breaches of legislation, guidelines or codes by ACC had been received at the meeting. The manager who thought he was involved with releasing the personal information, resulting from an inference he made from what was said at the meeting, searched his own email communications with the Client to determine whether he had sent the information.
9 December 2011	ACC sent a letter to the Client responding to some of the issues raised by the Client in the meeting on 1 December 2011. In the letter ACC asked the Client to return the personal information to ACC.
16 December 2011	The Client's lawyer informed ACC the Client would not be contactable from 20 December 2012 to 20 February 2012.

Date	Event
21 December 2011	ACC received an email response from the Client's support person to ACC's letter sent on 9 December 2011.
22 December 2011	ACC responded via email to the email received from the Client's support person on 21 December 2011.
21 February 2012	The Client wrote a letter (via her lawyer) responding to ACC's email dated 21 December 2011.
22 February 2012	ACC responded via email to the letter received from the Client on 21 February 2012.
1 March 2012	The Client met with a reporter at the Dominion Post. A portion of the information related to the Breach, with all personal information redacted, was provided to this reporter.
9 March 2012	ACC received a query from the media about a story that it planned to run regarding a privacy breach.
13 March 2012	The media story regarding the Breach was made public. ACC identified the email containing the Breach information. The Client forwarded the email she received from the RIS Manager on 5 August 2011 to ACC's Manager, Legal Services. The Client assured ACC that the personal information in her possession had been destroyed.
14 March 2012	An independent IT specialist provided verification that the personal information had been removed from the Client's computer system via a certification of destruction.
16 March 2012	A situation report was prepared by the Chief Executive for the Minister of ACC.
23 March 2012	The OPC in conjunction with the ACC Board announced an independent inquiry into the privacy issues experienced by ACC and published the Terms of Reference of the inquiry.

Appendix 5 – The Breach information

An email sent by the RIS Manager to the Client on 5 August 2011 responding to a complaint regarding a medical advisor contained personal information about other ACC clients which resulted in the Breach. This email contained an attached email titled 'FW: Monthly review report'. The attached email contained an internal ACC management report. The management report was a three page Microsoft Word document that contained summary statistics about cases under review with DRSL. Embedded into the management report were two Microsoft Excel workbooks. The two workbooks contained the detailed statistical information which supported the information in the management report.

The first workbook contains one worksheet. Table 1 below is an excerpt showing all of the information contained in the worksheet for a sample of five ACC clients.

The worksheet contains personal information about ACC clients, which has been redacted for the purpose of this report. The worksheet identifies a client's name, claim number and the branch handling the claim. No further information is disclosed about client cases.

The second workbook contains ten worksheets. Three of these worksheets contain personal information. The other 7 worksheets do not contain information identifying ACC clients but do contain a claim number reference. Table 2, Table 3 and Table 4 below are excerpts from the three worksheets showing all of the information contained in the worksheets for a sample of five clients. All personal information has been redacted from the excerpts for the purpose of this report.

The worksheet in Table 2 identifies a client's name, claim number and review number. No further information is disclosed about client cases.

The worksheets in Table 3 and Table 4 identify a client's name, claim number, review number and the branch handling the claim. No further information is disclosed about client cases.

Table 1

Details of Reviews with Missing Outcome but Outcome Tasks Created
Data warehouse load current to : 30 July 2011
provided by ACC Data Warehousing and Business Intelligence

Region	Branch Number	Branch Name	task	Claim number	Surname	First name 1	Outcome	Outcome date	Review number	Lodgement date
Central Area	79	Wellington Branch	PRC REV: Record Review Outcome	Redacted	Redacted	Redacted		.	Redacted	12/01/10
Central Area	79	Wellington Branch	PRC REV: Record Review Outcome	Redacted	Redacted	Redacted		.	Redacted	13/01/10
Central Area	69	Palmerston North Branch	PRC REV: Record Review Outcome	Redacted	Redacted	Redacted		.	Redacted	19/01/10
Central Area	79	Wellington Branch	PRC REV: Record Review Outcome	Redacted	Redacted	Redacted		.	Redacted	26/01/10
Central Area	79	Wellington Branch	PRC REV: Record Review Outcome	Redacted	Redacted	Redacted		.	Redacted	03/02/10

Table 2

Claim number	Claimant name	Review number	Branch	Issue ID	Date received by DRSL	Lodgement Date	Issue code	Code 1	Code 2
Redacted	Redacted	Redacted	52	X2	.	30/06/2011	Cover	No date	Outstanding
Redacted	Redacted	Redacted	52	X2	.	30/06/2011	Cover	No date	Outstanding
Redacted	Redacted	Redacted	35	X29	11/07/2011	30/06/2011	Cover	12	X
Redacted	Redacted	Redacted	141	X2	13/07/2011	30/06/2011	Cover	Withdrawn	Withdrawn
Redacted	Redacted	Redacted	52	Y26	.	30/06/2011	IA, Lump Sums	No date	Outstanding

Table 3

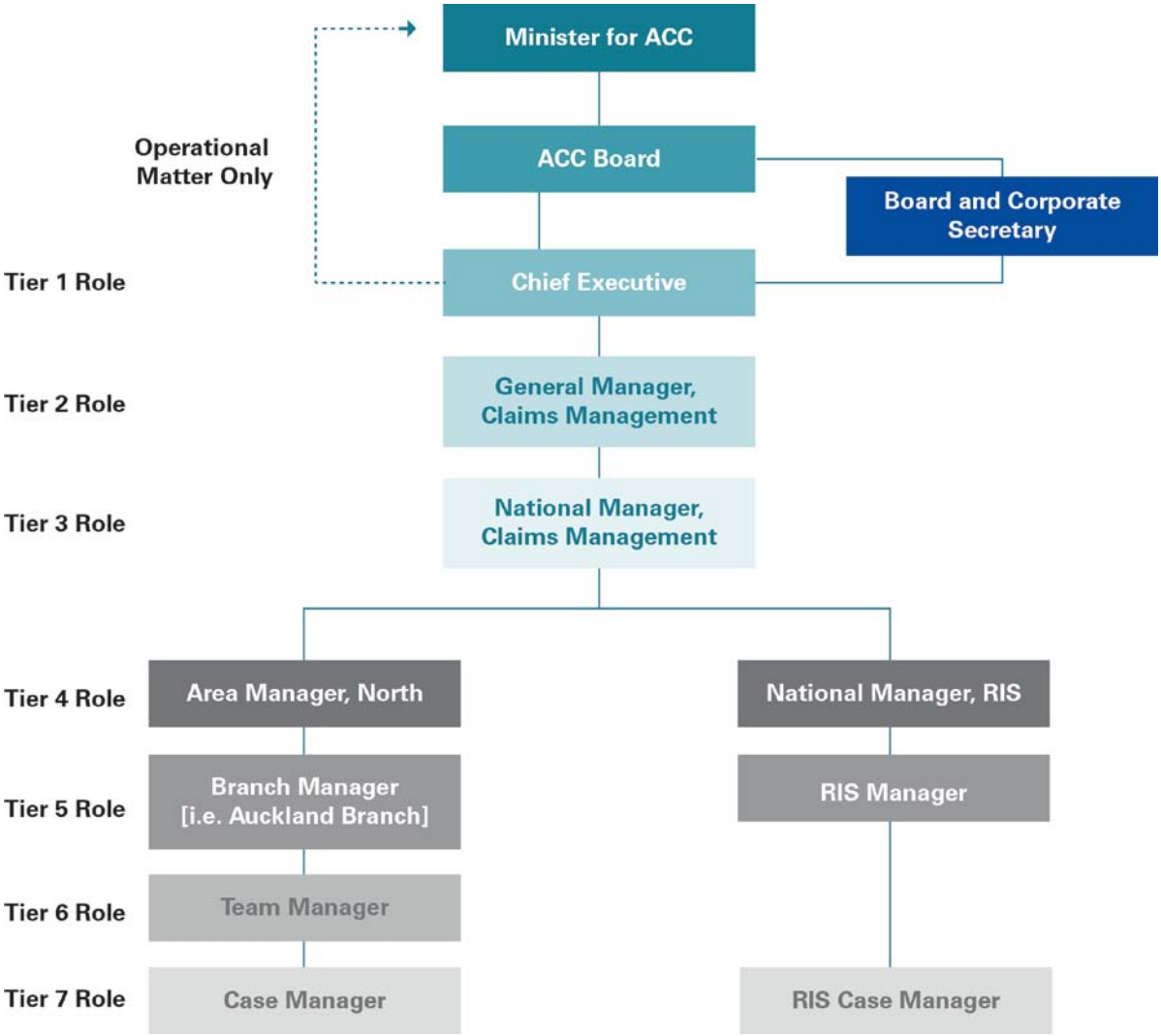
Review number	Claimant name	Claim number	Branch number	Branch name	Issue ID	Issue code	Date of outcome decision	Decision ID	Month of decision
Redacted	Redacted	Redacted	1	Office of Complaints	Z5	Jurisdiction	3/06/2011	O	1/06/2011
Redacted	Redacted	Redacted	1	Office of Complaints	Z5	Jurisdiction	12/01/2011	D	1/01/2011
Redacted	Redacted	Redacted	1	Office of Complaints	W8	The Code	7/12/2010	D	1/12/2010
Redacted	Redacted	Redacted	1	Office of Complaints	W8	The Code	19/01/2011	D	1/01/2011
Redacted	Redacted	Redacted	1	Office of Complaints	W8	The Code	9/06/2011	O	1/06/2011

Table 4

Review number	Claimant name	Claim number	Branch number	Branch name	Lodgement Date	Sent to DRSL?
Redacted	Redacted	Redacted	1	Office of Complaints	7/06/2011	N
Redacted	Redacted	Redacted	19	Sensitive Claims	7/06/2011	N
Redacted	Redacted	Redacted	23	Southern STCC	8/06/2011	N
Redacted	Redacted	Redacted	45	Henderson Branch	13/06/2011	N
Redacted	Redacted	Redacted	46	North Harbour Branch	16/06/2011	N

Appendix 6 – Organisational chart (extract)

The purpose of this organisational diagram is to provide details of the management structure of Claims Management, specifically focussing on the branches of Northern Area Claims Management and Recover Independence Service.



Glossary

Glossary term	Definition
Auckland Breach; "the Breach"	Refers to the unauthorised release of personal ACC claimant information by the RIS Manager on 5 August 2011.
AC Act	Accident Compensation Act 2001.
ACC 167	"Authority for the collection and disclosure of information" consent form signed by claimants being managed at branch level.
ACC 45	"Injury Claim Form" initially filled in by claimants or their health service providers when making a claim.
ACC; "the Corporation"	Accident Compensation Corporation.
ACC Managers	The two senior ACC Managers who attended the 1 December 2011 meeting with the Client, namely the Northern Area Manager and the National Manager RIS.
Accredited Employer Scheme	Employers who join this scheme take responsibility for their employees' work injury claims.
Action Remedy	The system used by Government Services and the Chief Executive's office to record privacy complaints.
BERT	Building Effective Relationships Training was implemented by ACC a few years ago to encourage resolution of issues with a client before they went to review.
Breach information; "the information"	In terms of the Breach refers to ACC internal management report containing two embedded spreadsheets containing personal ACC claimant information.
Board and Corporate Secretary	The Board and Corporate Secretary is the link between the Board and the Executive to ensure the effective and efficient management of the flow of business between the Board and the Executive.
Claim level	The level at which all information specific to the injury/claim is recorded in EOS.
Claimant	People who have lodged claims with ACC. Claimants are also referred to as clients – although normally not until cover has been accepted, except for areas like Sensitive Claims, Treatment Injury etc where the cover decision process takes a long time.
Code of Rights; "the Code"	Code of ACC Claimants' Rights established under Part 3 of the AC Act.
Copy File	The process of responding to a claimant's request for information under IPP/HIPR 6 or the Code of Rights.
DHB	District Health Board.
DRSL	Dispute Resolution Services Limited.
EOS	Electronic Claims Management System.

Glossary term	Definition
HIPC	Health Information Privacy Code.
HIPRs	Health Information Privacy Rules.
IIS	Information Integrity Solutions Pty Ltd.
InFact	ACC's reporting portal.
IPPs	Information Privacy Principles in the Privacy Act.
KPI	Key Performance Indicator.
National Manager RIS	The ACC manager who has national responsibility for RIS.
Northern Area Manager	Responsible for claims management of area branches and short-term claim centres for the northern areas of the North Island. The Northern Area Manager reports to the National Manager ACC Claims Management Network ("National Manager Claims"). During the month of October 2011, the Northern Area Manager stood in for National Manager Claims ("Acting National Manager Claims").
Near misses	Throughout ACC this is commonly defined as the discovery of a privacy breach before it is disclosed externally.
OIA	Official Information Act 1982.
OPC	Office of the Privacy Commissioner.
Party level	The level at which all general claimant information is recorded in EOS.
PbD	Privacy by Design.
PIA	Privacy Impact Assessment.
Privacy Act	Privacy Act 1993.
Privacy Breach [not "the Breach" but the term as used by ACC in its day-to day operations]	Throughout ACC this is commonly defined as the unintentional disclosure of personal information to a third party.
RIS	Recover Independence Services is the division of ACC whose responsibility it is to assist long-term claimants with their rehabilitation.
RIS Manager	In terms of the Breach, refers to the ACC staff member who released the information.
Security practices	Security practices relate to the processes and controls in place to manage the confidentiality, integrity and availability of the information systems and the data contained within them, and the physical security over ACC's information systems and premises.
SOI	Statement of Intent.
The Client	In terms of the Breach refers to the ACC claimant who received breach information.
The Scheme	New Zealand's accident insurance scheme set up under the AC Act.